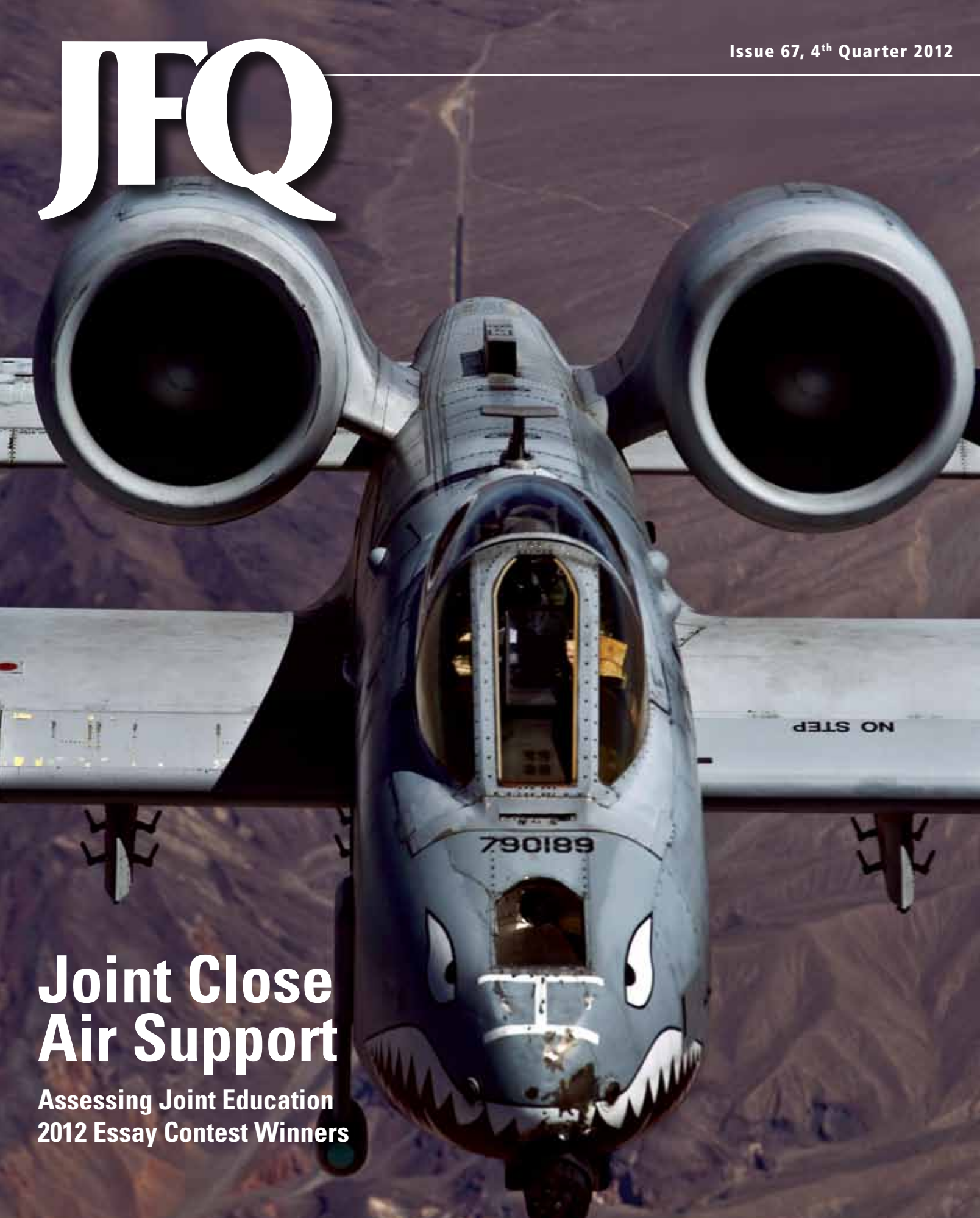
Issue 67, 4th Quarter 2012

JFQ



Joint Close Air Support

Assessing Joint Education
2012 Essay Contest Winners

Inside

Issue 67, 4th Quarter 2012

NDU Press is the National Defense University's cross-component, professional military and academic publishing house. It publishes books, journals, policy briefs, occasional papers, monographs, and special reports on national security strategy, defense policy, interagency cooperation, national military strategy, regional security affairs, and global strategic problems.

COMMUNICATIONS

Please visit NDU Press and *Joint Force Quarterly* online at ndupress.ndu.edu for more on upcoming issues, an electronic archive of *JFQ* articles, and access to many other useful NDU Press publications. Constructive comments and contributions are important to us. Please direct editorial communications to the link on the NDU Press Web site or write to:

Editor, *Joint Force Quarterly*
National Defense University Press
260 Fifth Avenue, S.W. (Building 64, Room 2504)
Fort Lesley J. McNair
Washington, DC 20319

Telephone: (202) 685-4220/DSN 325
FAX: (202) 685-4219/DSN 325
Email: JFQ1@ndu.edu
***JFQ* online: ndupress.ndu.edu**

4th Quarter, October 2012
ISSN 1070-0692

JFQ Dialogue

Forum

Essay Contests

Commentary

JFQ

Features

Recall

Book Reviews

Joint Doctrine

ABOUT THE COVERS

Front cover: Air Force A-10 Thunderbolt II aircraft assigned to 75th Fighter Squadron flies over National Training Center, Fort Irwin, California, August 2011, during exercise Green Flag–West 11-9 (U.S. Air Force/Daniel Hughes). Table of contents shows (left to right) MQ-1 Predator prepares for takeoff in Southwest Asia (U.S. Air Force/Julianne Showalter); coalition special operations forces wait for Army MH-47G Chinook helicopter during exercise Jackal Stone (U.S. Army/Eric J. Glassey); Marine teaches Police Station Security class for Afghan Uniformed Police Basic Training Course (U.S. Marine Corps/Orlando Perez); and Standard Missile 2 fired from USS *Gettysburg* (U.S. Navy/Kevin J. Steinberg).

CONTRIBUTIONS

Joint Force Quarterly welcomes submission of scholarly, independent research from members of the Armed Forces, security policymakers and shapers, defense analysts, academic specialists, and civilians from the United States and abroad. Submit articles for consideration to the address on the opposite page or by email to JFQ1@ndu.edu "Attention A&R Editor" in the subject line. For further information, see the guidelines on the NDU Press Web site at ndupress.ndu.edu.

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.

ndupress.ndu.edu

From the Chairman

Building Tomorrow's Leaders

Chairman speaks during National Defense University change of presidency

NDU (Katherine Lewis)

Military service is our nation's preeminent leadership experience. We need to keep it that way, and I need your help to do it. Doing so requires us to promote and emphasize the values that define our profession of arms. It includes leveraging technology, but not as a substitute for human interaction. It involves providing our men and women with the best education and training. It means asking them to lead in diverse and challenging contexts—to experience and recover from setbacks, unexpected events, and even chaos.

It also means embracing leadership as a personal responsibility. In this way, leadership is something that requires persistent study and constant reflection. With that in mind, I want to share some words to lead by.

Leader Development Is Job One

I have often said that in the face of change, the one thing we have to get right is the people. Our men and women are our greatest strength, and I firmly believe that developing them into tomorrow's great leaders is the best investment in our future.

Leadership is what will see us through when our organizational structure is not perfect, when technology comes up short, when training misses the mark, and when guidance is late to need.

Our nation needs innovative leaders who can think through complex problems and out-think our adversaries. We need professionals who can reconcile context, uncertainty, and surprise. We need to put a premium on those who seek and embrace adaptability as an imperative.

Leader development in these areas is our decisive edge. How we do that starts one person at a time, one engagement at a time. It is how we invest our own example, experience, and talents directly and personally in others.

It is essential that each of us—regardless of how many stars, bars, or stripes we wear—commits to mentor on an individual and consistent basis. This is one of the most fundamental ways that we can accelerate and reinforce the learning process.

Leaders Are Readers

We need leaders who are lifelong learners and creative thinkers. That is why I encourage our men and women to continue to study and develop a sense of perspective. It is also why I always have at least three books on my nightstand to stretch my views. Reading helps us to stay rooted in the past, understand the present, and have a vision for the future. Said another way, if you seek a new idea, find an old book.

Lifelong learning is more than reading. In fact, sometimes we need to put down the book, if only to think about what we have read. We have to continue broadening perspectives, challenging assumptions, and cultivating inquisitive minds. One of history's most creative minds, Albert Einstein, said, "I have no special talent. I am only passionately curious." I believe we have this passionate curiosity in our ranks today. We see it in our men and women striving to understand the context of current conflicts. Our task is to continue to nurture, build, and inspire this curiosity.

We have an opportunity to channel these attributes into innovative solutions to our biggest security challenges around the world. We cannot afford to stagnate or to accept failure of imagination. We should always seek to challenge ourselves and our minds, lest our enemies imagine a different, more dangerous future for us.

Lead Always, but Use Words Only When Absolutely Necessary

The future will be a difficult journey and one that we cannot take alone. Growing relationships is one of the tools in our leadership toolbox that we should reach for early and often. If we wait until a crisis, we risk being too late.

When leaders value, grow, and institutionalize relationships—between leaders and led, within the family, and on the international stage—the results are always better.

Words matter in every relationship, and in fact, I have found that the higher you climb the ladder, the more important it is to choose words carefully and with precision. Mark Twain once said, "The difference between the right word and the almost right word is the difference between lightning and a lightning bug."

Communicating is not limited to language. This is where deeds trump talk and actions speak over messages. This is where we have to work at it—consistently. We cannot just e-mail or phone these things in. We need to meet face to face. Most of us can start relationships, but we must also build and sustain them to be effective and meaningful.

Trust Is the Foundation of Our Profession

Ours is a profession that requires trust of the highest order—in each other, in the leaders appointed over us, and in our fellow citizens. Without it, our men and women would never leave their base camps, strap into a cockpit, man the deck of an aircraft carrier, or go beneath the waves.

From a broader perspective, trust is fundamental to operational success. This lesson of history has been reinforced in Iraq and Afghanistan. We are seeking to match this timeless insight to the changing character of warfare by rearticulating command and control as *mission command*.

Mission command is not a matter of rhetoric. As we decentralize authority, capability, and responsibility to the operational edge, we place a corresponding emphasis on mutual trust. Our paradigm for leader development also needs to prepare our men and women to accept this responsibility.

It is a charge that goes beyond the joint force to building teams among our interagency, intergovernmental, and multinational partners. Mutual trust does not work without their confidence that we are trustworthy teammates.

Trust also binds us with the American people we represent. They place great confidence in their armed forces. They—and those we lead—trust us to be leaders of character and consequence. It is up to each of us to honor their trust. It is up to all of us to commit to develop the leader after next. **JFQ**

MARTIN E. DEMPSEY
General, U.S. Army
Chairman of the
Joint Chiefs of Staff

Readiness and Resiliency Go Hand in Hand

By **BRYAN B. BATTAGLIA**

Meshed and intertwined into a Servicemember's behavior and in the daily rhythm of a command, resiliency is a needed ingredient to maintain individual and unit readiness.

A command will have a natural dive and peak pattern during its life cycle, so the "band of readiness" is a wavering line. How deep the dive is, and how steep the peak, depend on several factors in this ebb and flow in the readiness and resiliency of a command. From an enlisted perspective, I hope to show that one is needed to achieve the other.

It is fair to say that both readiness and resiliency are perishable items in the life cycle of the Servicemember and organization. Also, commands and organizations that lack active resiliency programs will struggle to accomplish their assigned missions and associated milestones. The goal, of course, is for the band to remain shallow in its dip and dive, thereby minimizing time, effort, and resources needed in returning units to a level of optimal performance and maintaining that posture. Keep in mind that the center of gravity in every command is its people, because they shape and perform the very tasks that accomplish the mission. While this list is not all-inclusive, here are a few observations from a senior enlisted lens as to the why in the dip and climb and some avoidance measures to keep a minimally wavering band.

Change in Command/Directorship

When a unit receives new leadership, there is an initial period during which the men and women adjust and adapt. Just as important, the new commander needs to make some adjustments and adaptations in his or her execution of duties. First, the departing commander may have set and shaped conditions over the course of the command tour in such a way that the unit remained operationally effective and in a high state of readiness. Any incoming commander (platoon through combatant command) would be fortunate to fall in on an outfit that lies in a high state of "ready, relevant, and capable." In such a case, the departing commander and his or her subordinate leaders set and maintained a healthy standard—a resilient climate to say the least. This is the kind of unit to which we all hope to be assigned. That said, setting a standard is one thing; how it is received and carried out is another. In this example, and barring the normal transfers and attrition of unit personnel, the new commander is essentially starting with a unit that is fit and proficient in both field and garrison. Therefore, the band of excellence and the band of readiness should remain shallow in dip and climb. As long as there are no major changes in the mission, the best thing an incoming commander can do is not to make any major rudder adjustments and allow the command to keep firing on its existing pistons. Sudden and significant modifications to a fit unit may be unnecessary and could cause underlying turbulence within the rank and file.

On the other hand, a commander may inherit a unit that has experienced disciplinary, proficiency, and ethical road bumps. The bands of readiness and excellence will obviously dip and dive more than they do in the previous example. Given a unit history of problems such as suicide, drug and alcohol use, sexual assault, or leader misconduct, the new commander may need to make some immediate changes to put the unit back on course and refocus its strengths and priorities.

Said another way, if a unit's center of gravity is off keel, sudden and immediate change is indeed needed. If problems are unattended to, the command will struggle simply to achieve its mission.

Command Climate and Unit Atmospherics

Readers of *Joint Force Quarterly* certainly understand that commanders are ultimately responsible for the success or failure of their commands. From the start, this includes establishing and maintaining a positive climate. But all the responsibility placed on the shoulders of the commander needs to be shared among midgrade officers and senior noncommissioned/petty officers, who are a significant part of the unit's center of gravity. These officers have the ability to influence and shape the unit more quickly than the commander. This is a good thing because a commander who empowers his or her subordinate leaders to execute intent and command philosophy—one who rewards effective performance yet holds his people accountable—marks a holistic leader who will promote a positive atmosphere.

As you can see, I am an advocate for commanders who place trust and confidence in their subordinate leadership, but I would

Sergeant Major Bryan B. Battaglia, USMC, is the Senior Enlisted Advisor to the Chairman of the Joint Chiefs of Staff and Senior Noncommissioned Officer of the U.S. Armed Forces.

SEAC meets with Air Force members at Ramstein Air Base, Germany

U.S. Air Force (Caitlin O'Neil-McKeown)

be remiss if I did not say that this trust is a two-way street; it must be reciprocated. The absence of a dual bond will negatively impact the command. This is where I believe that while the ultimate responsibility lies with the commander, he or she cannot do the job alone. Thus, every leader shoulders responsibility in setting and maintaining the command climate and sustaining readiness. In many ways, we are aligned and designed similar to an NFL team. I can only partially accept the premise that when the team is not making the playoffs, we have the tendency to put all responsibility on the coach: "Get rid of the coach and the problem will go away." As we peel back the onion, if I may mix metaphors, we see that we have only a linear assessment and inexact solution.

The climate that the commander initially sets will play a significant role in how far the band of readiness dips. A hostile work environment, a command atmosphere that does not promote good order and discipline, leadership by intimidation, and other negative practices will quickly change the band from readiness to read*imess*.

Modification of an Organization's Mission

Many of us have been assigned to a command that experienced a change in unit mission. Perhaps it was a change from a traditional command mission the unit was tasked with since its inception, or an interim mission change while the unit operationally supported a combatant command, or a complete unit deactivation. In each such case, deflection and elevation are experienced in the readiness band. Examples range from an existing unit whose traditional mission changes, such as 8th Army, U.S. Forces Korea, to a complete standup of a major organization such as U.S. Africa Command, to a total disestablishment of a four-star organization such U.S. Joint Forces Command. Changes in unit force structure, personnel/equipment, military occupational specialty, Air Force specialty code composition, core competencies, deadlines, dissipation of funding streams, and even geographical location all impact the bands of excellence and readiness for the command. These examples reinforce why individual and unit resiliency during a period of build, rebuild, or complete deactivation will help diffuse unnecessary turbulence and growing pains. Again, a unit and its members need resiliency embedded into daily rhythm and life cycle to achieve and sustain readiness.

Field vs. Garrison

The idea here is not to depict what our young force has come to see as the norm: the huge integration/reintegration phase of a major 6- or 12-month deployment we have seen time and time again. Rather, we must picture the Armed Forces in the absence of major combat operations when they are primarily living and operating out of a garrison setting at home base or home port.

A great number of senior leaders still in uniform grew up in a similar environment to my own. We were training for a war we never fought—the Cold War. While training, education, and development were in fact executed, the bottom line is that during the 1980s, I believe our military was extremely proficient in garrison survival, field exercises, and rotational peacetime deployments. Actually, I think that on the heels of the Vietnam War, the garrison life we maintained in the 1980s to mid-1990s paid significant dividends in preparation and readiness for our military to defend the Nation today. Garrison enabled us to rebuild upon a basic yet solid foundation through persistent repetition of what I would describe as key tenets of soldiering and military living. Over the course of time, these basics have developed and shaped a fighting force in affairs such as advanced tactics, law of land warfare, code of conduct, field and barracks sanitation, marching, weapons-handling, squad/section gear inspections, knee-to-knee counseling, physical fitness, professional development, and other fundamental areas—all of which are key ingredients to building relevancy, resiliency, proficiency, and good order and discipline.

Even if we never get the opportunity in our life cycle to return to a persistent garrison environment, we should still take every opportunity to implement some of the basic tenets throughout our commands, ships, bases, and formations. Part of maintaining unit readiness in the training life cycle may be packing up the unit to go to the field for 5 days or even for 2 weeks. It may be an Air Force squadron running expeditionary airfield operations from an adjacent base, or a Marine or Army infantry battalion on field maneuvers rehearsing raids and ambush techniques, or a Navy Seabee platoon training in refortification at a neighboring state's base.

My point is this: there are differences in maintaining proficiencies in a garrison setting compared to a field environment, and it is these differences that affect the bands. We should seek to keep the readiness and resiliency bands on a fairly level glide-slope. When moving from field to garrison and vice versa, good units can experience a slight variation in band wave with little adjustment in the ranks. Exceptional units can segue to either environment and not lose a drum beat. In any case, it is extremely important that no matter how long or short the field operation or sea trial may be, the transition from one to the other must be monitored by the leaders. **JFQ**

Executive Summary

Soldier directs AH-64 Apache attack helicopter strike on target at close combat attack lane during competition at U.S. Army Garrison Grafenwoehr, Germany

U.S. Army (Robert Hyatt)

As we go further into the time when finding ways to continue to meet mission with diminished resources, some have suggested that we consider the words of Nobel prize–winning chemist Sir Ernest Rutherford: "Gentlemen, we have run out of money, it is time to start thinking." In every corner of the United States and beyond, economic problems persist and are entering the fifth year since the 2008 Wall Street crisis. The U.S. military is not immune from the repercussions of these economic forces. The joint force will get smaller while formations large and small will be adjusted and made less costly, at least in the short run. The world of jointness is experiencing this pressure as well. One part of these readjustments for both budgetary and important mission considerations is the future of joint professional military education (JPME) and leadership development.

After so many years of combat operations, each of the Services to varying degrees has reached a point where the best of what we have learned needs to be made a part of what and how we train and educate succeeding military generations. You will find this and succeeding editions of *Joint Force Quarterly* increasingly filled with voices, especially those who are in JPME classrooms, seeking to provide the wisdom these authors have gained on a range of topics that are the keys to this evolution of the joint force's training and education. While budgetary pressures have begun to bite and units get smaller (even *JFQ* in recent issues), the mission will continue to get done and the force will, in the long run, be better trained and educated for the challenges ahead.

In the Forum, we offer two discussion topics: the futures of both security partnerships and professional military education. First, two authors with key insights discuss security cooperation and force assistance. From his perspective as director of plans at U.S. Africa Command, Charles Hooper reminds us that building partner capacity—an essential mission and an important component of the U.S. Government's approach to preventing and responding to crisis, conflict, and instability globally—should be seen as not just an "indulgence" but an enduring strategic imperative. Gene Germanovich then reviews Department of Defense (DOD) approaches to building partner capacity and offers a series of recommendations to better scope these efforts.

If you are a good observer of the writings of our 18th Chairman of the Joint Chiefs, General Martin Dempsey, you are aware of his white paper on JPME that he sent out earlier this year. This paper is crucial for a number of reasons, most importantly as a statement of where we are and where we need to go to support the Chairman's vision of the joint force in 2020. After many years of crisis and combat operations, combined with an increasingly austere fiscal environment, a serious review of the entire training and education system, Service and joint, is both needed and welcome. We are fortunate to be able to explore two other views on the mission of reinventing JPME to support the joint force in the next decade as the Chairman has asked us to do.

Fresh from leading the largest resident JPME course in DOD, Vince Bowhers examines a key issue, Service personnel management, that needs to be addressed in achieving success in joint education for the force. Often difficulties in getting the right student the right education at the right time can be found in the disconnects between how the Services manage the careers of their officers and the requirements of gaining appropriate joint experience and education. One promising means of achieving a wider exposure of the joint force to education and training is distance learning. In another persepective on delivering education, two seasoned veterans at the Air Command and Staff College, Kathleen Mahoney-Norris and John Ackerman, take us through how the college's distance learning experience is an increasingly accepted and valued form of delivering high-quality graduate military education to warriors around the world.

The judges of the 2012 Secretary of Defense and Chairman of the Joint Chiefs of Staff Essay Contests have selected another outstanding trio of winning papers from what they described as the best group of submissions in recent years. Having read every one of the more than 60 papers, I am certain they are correct in their judgment. In his first-place winning Secretary of Defense National Security Essay, Lieutenant Colonel Joseph Berger, USA, reviews the practice of placing uniformed Servicemembers under the control of the Central Intelligence Agency, using the raid that successfully killed Osama bin Laden as a framework for analysis. Lieutenant Colonel Andrew Foltz, USAF, won top honors

in the Chairman of the Joint Chiefs of Staff Strategic Research Paper Contest by effectively exploring when cyber operations constitute a prohibited use of force as defined by the United Nations Charter. Taking first place in the Chairman of the Joint Chiefs of Staff Strategy Article Contest, Gregory Macris from the Department of State argues that U.S. interests are supported best as we assist the government of the Republic of Korea in convincing as it works to convince its citizens that the immediate and short-run costs of reunification are actually important investments in the future of all Koreans.

Commentary brings a set of articles that mark a number of recent firsts, and we hope these will be followed in future editions by related discussions. Somewhat surprisingly given the amount of writing seen in other publications, Admiral (Ret.) Mark Fitzgerald has provided our first discussion on Air Sea Battle aside from General Norton Schwartz's answer in our interview several issues ago (*JFQ* 63). Admiral Fitzgerald argues that the approach to systems dedicated to making Air Sea Battle happen may be missing the mark but that the concept itself is sound. In another area related primarily to air and sea control, Lieutenant Colonel Pete Ohotnicky, USAF, Lieutenant Colonel Braden Hisey, USMC, and Jessica Todd argue that a renewed focus on the Arctic due to continuing ice melt and increased maritime activity is required with the reestablishment of a subunified command to protect U.S. interests there. From a recent research paper presented here at the National Defense University, Robert Butterworth provides an important discussion and context to the relationship between the medium of space and the joint warfighter. Seeing a way to continue to improve North Atlantic Treaty Organization (NATO) regional partnerships, Colonel (S) Arthur Davis, USAF, examines the newly formed NATO Special Operations Headquarters as a model for conducting operations to counter terrorism in defense of the Alliance.

Our forces sometimes find themselves forced to adapt in combat when a capability is used that doesn't fully match with our society's expectations or understanding, such as the atomic weapon in 1945 or the armed drone. History has also shown examples of how the task given to the military by its political masters may be in line with national interests but may also be at the limits of capabilities resident in the joint force. Our Features section offers some serious concepts to consider in the areas of new capabilities in need of some social adjustments as well as the way ahead on close air support, an area that seems to be relearned in each new war. Major Jeffrey S. Thurnher, USA, suggests that the deployment of lethal autonomous robots raises significant legal and ethical concerns for commanders and their political masters. Highlighting a likely Air Sea Battle related system of systems, George Galdorisi and John Morton report that the Aegis Ballistic Missile Defense is evolving into a global enterprise as the system migrates from U.S. to allied navies, in turn becoming the interoperable "glue" that binds the United States and its regional allies and partners into a credible combat force and, by extension, a credible deterrent. Colonel (S) John Schaefer III, USAF, describes the work behind reducing the response time for close air support in Afghanistan where aircraft arriving even a few seconds earlier can make the difference between life and death for our troops in contact with the enemy. Curtis Neal, Robert B. Green, and Troy Caraway offer the way ahead to institutionalize improvements in close air support response and integration for the joint force. They describe an emerging capability, the Joint Air Ground Integration Center, as a solution that takes advantage of existing organizational structures and 21st-century communications to conduct operations in a more efficient, linked, and situationally aware manner.

U.S. Marine Corps amphibious assault vehicle comes ashore during mechanized raid during exercise Cobra Gold 2012 in Hat Klad, Thailand

U.S. Marine Corps (Jonathan Wright)

In Recall, we are fortunate to have a returning *JFQ* contributor and expert to mark the passing of the 30th anniversary of an important crisis and combat far from any U.S. interests but between two of our friends at war in the Falklands. Brigadier General Raymond Bell, USA (Ret.), revisits the experiences of the British joint force operations and the logistics challenges of a short notice, long distance winter battlespace. As with every issue, we offer three significant book reviews and a review of current joint doctrine issues and events.

Given that there will be fewer resources but increasing challenges ahead, we offer the pages of *Joint Force Quarterly* as a means to help the joint force not only to "start thinking" but also to make sure the troops coming up behind today's force benefit from our collective wisdom. **JFQ**

—William T. Eliason, Editor

U.S. Air Force (Christine Clark)

Marine operations officer mentors students from Uganda and Kenya at International Peace Support Training Centre, Nairobi

Going Farther by Going Together

Building Partner Capacity in Africa

By CHARLES W. HOOPER

If you want to go quickly, go alone.
If you want to go far, go together.
—African proverb

Building partner capacity is an essential military mission and an important component of the U.S. Government's approach to preventing and responding to crisis, conflict, and instability. Demanding fiscal realities, the end of the Iraq War, the unfolding transition in Afghanistan, and a renewed focus on enduring interests in Asia and the Middle East are increasing the importance of burden-sharing. Secretary of Defense Leon Panetta's January 2012 strategic guidance, *Sustaining U.S. Global Leadership: Priorities for 21st Century Defense*, was clear on this point. Recognizing that building partnership capacity "remains important for sharing the costs and responsibilities of global leadership" with states that value "freedom, stability and

prosperity," Secretary Panetta directed that "whenever possible, we will develop innovative, low-cost, and small footprint approaches to achieve our security objectives, relying on exercises, rotational presence, and advisory capabilities."[1]

Some may argue that changes in the strategic environment diminish the value of building partner capacity as a component of our nation's overall defense strategy. It makes more sense, they say, to dedicate those scarce resources toward improving our own capabilities than to improve those of other partners. We disagree. Building the capacity of our willing and important partners is not a strategic indulgence but rather an enduring strategic imperative. We believe that a small investment now that enables our partners to address an emerging challenge is a bargain. This is exactly U.S. Africa Command's (USAFRICOM's) approach to the complex security challenges in its area of responsibility (AOR).

Threats, Challenges, and Opportunities

USAFRICOM's AOR is huge, diverse, and complex—and so are the security challenges we and our partners face. The command's AOR includes 53 African states, more than 800 ethnic groups, over 1,000 languages, and a diverse geography 3½ times the size of the continental United States, not to mention a diverse mix of political, economic, social, and security challenges. Djibouti, on the Horn of Africa, is a mere 20 miles across the Bab el-Mandeb waterway from Yemen and the Arabian Peninsula. Similarly, the eastern coastline of Africa is also the western shore of the Indian Ocean, sitting astride the sea lines of communication that link the continent and Europe to the rising powers of the Asia-Pacific region. In the north, Tunisia is less than 70 miles from Sicily, and only the Strait of Gibraltar separates Spain from Morocco. The point is that Africa is inextricably linked by geography, history, and commerce to not only the twin pillars of our new strategic guidance, but also to our enduring interests in Europe.

Africa's security challenges are daunting: terrorism and growing violent extremist organizations, piracy, and the illicit trafficking of arms, narcotics, and people. Poverty and corruption in many regions contribute to an insidious cycle of instability, conflict, environmental degradation, and disease that erodes Africans' confidence in national institutions and governing capacity. This, in turn, creates the conditions for a wide range of transnational security threats that can threaten America's homeland and its regional interests.

That said, the flawed, one-dimensional stereotype of Africa as a place where bad people rule and good people suffer the consequences is inaccurate. Once labeled by *The Economist* as "the hopeless continent," Africa now abounds with possibilities.[2] It is a continent of progress and potential.

The U.S. Agency for International Development's Chief Economist Steven Radelet identified 17 African countries with over a decade of sustained economic growth and falling poverty rates and further identified another half-dozen African states showing signs of similar progress.[3] Radelet tracked five fundamental changes common to these emerging states: the rise of accountable democratic governments, governments implementing sensible economic policies, the end of the African debt crisis, the spread of new technologies, and the emergence of a new generation of policymakers, activists, and business leaders.[4] These new leaders have a clear-eyed view of the stubborn economic and security challenges they face, what needs to be done, and how to do it. The United States is increasingly connected to these rising states and regional organizations through shared economic, political, and security interests, including commitments to consolidating the democratic and economic progress achieved in recent years. USAFRICOM's capacity-building efforts are an integral part of a unified U.S. Government approach to Africa and are fully in line with Secretary Panetta's January 2012 strategic guidance.

The foundation of USAFRICOM's theater strategy is building the security capacity of our African partners. The strategy is guided by two principles:

- A safe, secure, and stable Africa is in the U.S. national interest.
- Over the long run, it will be Africans who will best be able to address African security challenges, and USAFRICOM most effectively advances U.S. security interests through focused security engagement with African partners.

Building the capacity of willing partners is central to achieving our goals and objectives. To realize success in our mission we must prepare, in cooperation with our partners and allies, to respond to future crises and contingencies; prevent future conflicts by continuing to strengthen our partners' defense capabilities; and prevail in current and future operations.

Enabling our partners to meet common security challenges promotes the sharing of costs and responsibilities, supports our national interests, and—this is key—often provides a high return on modest investments. These capacity-building efforts are an integral part of a unified U.S. Government

U.S. Air Force (Joseph L. Swafford, Jr.)

Marine landing support specialist directs Navy air cushion landing craft during exercise near Camp Lemonier, Djibouti

Major General Charles W. Hooper, USA, is the Director of Strategy, Plans, and Programs for U.S. Africa Command.

approach that promotes America's overarching priorities in Africa: strengthening democratic institutions, spurring economic growth and investment, advancing peace and security, and promoting opportunity and development.[5]

The USAFRICOM Approach

The African proverb at the beginning of this article captures USAFRICOM's approach to building partner capacity: "If you want to go quickly, go alone. If you want to go far, go together." We at USAFRICOM choose to go together, with our African partners as well as our interagency partners, to better meet their security needs and to advance the interests of the United States.

Consistent with Secretary Panetta's 2012 strategic guidance, USAFRICOM operates, and out of necessity has always operated, with a light footprint. With no permanently assigned forces, the majority of our security cooperation activities are conducted by small teams led by our Army, Navy, Air Force, Marine, and special operations components focusing on building the capacity of our partners to address their own security challenges. African militaries are receptive to this approach, which allows us to cultivate the personal relationships that are so important to our efforts to deepen institutional partnerships and build self-sustaining security capacity.

These military engagements comprise a small but critical element of U.S. Government activities in Africa. To illustrate this, compare the Department of State and USAFRICOM spending in Africa. In fiscal year 2012 (FY12), the Department of State spent approximately $7 billion on the 53 countries in our AOR on a wide array of health, development, and security programs under its Title 22 authorities.[6] Approximately $3.3 billion of this $7 billion funded security-related programs such as peacekeeping, nonproliferation, antiterrorism, narcotics control and law enforcement, military education, and equipment financing.[7]

By contrast, USAFRICOM in FY12 controlled, influenced, and administered a modest $515 million in Title 22 and Title 10 security cooperation program dollars. The command directly controlled Department of Defense Title 10 programs such as the Combating Terrorism Fellowship Program, Military to Military Engagement, Air and Maritime Sector Development, and the Partner Military HIV/AIDS Program. USAFRICOM

Commander, Joint Special Operations Task Force–Trans Sahara, addresses Burkinabe soldiers prior to deployment to Mali during exercise Flintlock

U.S. Air Force (Jeremiah Erickson)

then supported and administered $130 million in traditional Department of State Title 22–funded programs such as Foreign Military Financing, International Military Education and Training, African Contingency Training and Assistance (ACOTA), Partnership for Regional East Africa Counterterrorism (PREACT), Trans-Sahara Counterterrorism Partnership (TSCP), and Africa Maritime Security Initiative.[8]

These numbers suggest three important points. First, they illustrate that USAFRICOM often plays a supporting role to broader U.S. Government efforts across Africa. Next, they demonstrate the requirement for our close collaboration with the State Department as well as other agencies. Finally, spending modest security cooperation dollars effectively across a complex AOR requires an analysis of the threats, prioritization of efforts, and an understanding of the willingness and capability of our partners.

Hard-nosed prioritization is an important aspect of our approach. The fact of the matter is that some regions and countries are more important than others. Current fiscal realities dictate that we prioritize regions in Africa to better focus our exercises, operations, and security cooperation activities. Our highest priority is the East Africa region, which is the nexus of terrorism and violent extremism that directly threatens our nation's security. In prioritizing engagement with individual states, USAFRICOM considers our common concerns, compelling U.S. national security interests, and each nation's role and capability in addressing these threats.

We conduct partnership capacity building along three interwoven lines of activity: fostering relationships, building operational capability, and developing institutional capacity.

Establishing and fostering security relationships built on mutual trust and respect is the foundation of our capacity-building efforts. The importance of the human dimension cannot be overstated. Senior leader engagements, conferences, exercises, workshops, education, the interactions of our junior leaders with their African counterparts, and the day-to-day work of Offices of Security Cooperation (OSC) all contribute to fostering lasting relationships. We build enduring and mutually beneficial relationships by acting as reliable partners. In short, we need to do what we promise and do it in a timely manner. Listening and learning skills are essential at every level of engagement. Impatience and a "we know best" attitude can stifle progress and trust.

Building operational capacity is about more than the number of troops and pieces of equipment. It is about aligning the right military capabilities—ground, maritime, and air—against a partner's unique mission requirements. Not all solutions are material. The doctrine, organization, training, materiel, leadership and education, personnel, and facilities model that we use in the U.S. Armed Forces to think through our own force development issues is useful when assessing operational capacity requirements with our partners.

Over time we have developed, along with our African partners, a deeper appreciation of the importance of focusing on institutional capacity. To support the building of institutional capacity, we focus on resource allocation, command and control, expanding combat multipliers such as intelligence and

engineers, and developing recruiting, training, and sustainment programs and policies. These functions help to ensure the readiness and independent sustainability of our partners' forces. An underlying premise of our institutional capacity-building efforts is that military forces must be subordinate to civil authority and accepted as legitimate members of a civil society based on the rule of law.

Building partnership capacity is not without hazards and challenges. First, trying to do too much too fast can undermine relationships. Strategic patience is not an American strength. However, building capable partner forces that willingly embrace democratic values takes time and patience. Each willing African state must ultimately find its own way to security, freedom, and prosperity. Therefore, the return on our efforts and investments will often not be immediately evident. That said, there are near-term intangible benefits—improved soldier/leader confidence, better discipline, increased unit esprit de corps and cohesion, reduced suspicion, and strengthened individual and collective national will—that, while difficult to measure, are, to quote the popular credit card commercial, "priceless."

Second, we must be prepared for setbacks. Many African governments remain fragile. The recent coup in Mali, despite significant multinational contributions to their armed forces and economic development, cannot be categorized in any other way than a huge setback. Finally, our outdated and often arcane partner-building capacity processes and policies create the risk that others, perhaps not those we would chose, may become the preferred security partners of African states.

Building Partner Capacity in Action

A prominent example of how building the security capacity of our African partners promotes the sharing of costs and responsibilities, supports our national interests, and provides a high return on modest investments is our sustained support to the African Union Mission in Somalia (AMISOM). Our direct and indirect efforts in USAFRICOM's highest priority region contribute to an African Union organization increasingly capable of securing ungoverned space, defeating al-Shabaab, and creating the conditions for a functioning state of Somalia.

AMISOM was initially authorized under a United Nations Security Council Chapter VII mandate in February 2007 to fill the security vacuum created by withdrawing Ethiopian troops.[9] The mandate was ambitious and wide-ranging and included ensuring the free movement and protection of those involved in the reconciliation process, protecting the institutions of the Transitional Federal Government (TFG), reestablishment and training of Somali security forces, and creating the conditions necessary for the provision of humanitarian assistance. The principal obstacle to success was al-Shabaab. In the chaotic aftermath of the Ethiopian invasion and overthrow of the Islamic Courts Union, al-Shabaab rapidly emerged as a dangerous al Qaeda affiliate that recruited foreign fighters, to include Americans. In 2007, Uganda and Burundi were the only two countries to contribute troops to AMISOM.[10] For the Ugandans, this marked their first deployment of a military force beyond their borders. Undermanned and inappropriately equipped and trained, AMISOM was not fully equal to the task.

Al-Shabaab employed improvised explosive devices (IED), suicide bombings, and ambushes against AMISOM and TFG forces within Somalia and demonstrated the capability to strike beyond Somalia's porous borders when it carried out twin suicide bombings in Kampala, Uganda, during the August 2010 World Cup.[11] This was a pivotal moment. The attack was intended to undermine the resolve of the primary AMISOM troop contributor, but it had the opposite result. Ugandan President Yoweri Museveni stood by his commitment to AMISOM and declared, "It would be a historic mistake to expect the war-weary Somali people to tame this global menace on their own."[12]

Al-Shabaab poses a direct threat to Americans and American interests. The scenario that keeps us up at night is an American with a U.S. passport receiving indoctrination, training, and support in East Africa and returning to an American city to conduct a terrorist attack. That would be mission failure. Therefore, one of our primary focuses is support to African nations that are willing and able to provide forces to AMISOM. We work extensively with Uganda and Burundi since they provide the majority of forces to AMISOM. If our efforts are successful, and we believe the trend line is improving, this will be an area where the United States would not have to commit sizable forces to address the security situation.

Our efforts are collaborative at every level. This collaboration starts with fostering productive relationships by listening and learning from deployed AMISOM forces about the threats they face and their assessments of training and equipment requirements. USAFRICOM works closely with the Department of State, Embassy Country Teams, and our OSCs to improve and adapt the Title 22 ACOTA programs to prepare AMISOM forces for the operating environment in Mogadishu. Over time, often applying hard-earned training and operational insights from Iraq and Afghanistan, and most importantly input from AMISOM forces, ACOTA training has expanded to include force protection, patrolling, convoy operations, cordon and search, base security, and counter-IED training. Finally, our USAFRICOM military mentors participate directly in ACOTA training alongside State Department–contracted trainers and continue to shape collective and individual training efforts at locations in Uganda and Burundi.

Section 1206 "Global Train and Equip" authorities allow USAFRICOM to complement and expeditiously reinforce ACOTA training and meet the operational requirements of AMISOM forces. For example, we use 1206 authority to fund 10-week combat engineer (sapper) training courses for deploying Ugandan engineer companies conducted by U.S. Marine Forces Africa's Special Purpose Marine Air Ground Task Force (SPMAGTF). Operating out of Sigonella, Italy, on a rotational basis, SPMAGTF is tailored to conduct small-footprint theater security cooperation engagements and consists of just fewer than 200 Marines organized in 5- to 14-man teams, with two KC-130 aircraft. This dual key funding authority has also allowed us to put small unmanned aircraft systems (UAS) in the hands of deployed Ugandan forces. These UAS have a direct positive impact on AMISOM's capacity to conduct operations in Somalia by targeting enemy locations, clearing routes, and identifying IEDs.

The new 1207(n) Global Security Contingency Fund (GSCF) Transitional Authorities provided in the fiscal year 2012 National Defense Authorization Act will allow us to reinforce AMISOM's success and focus on readiness and independent sustainability by enhancing intelligence, engineer, and sustainment functions.[13] We are collaborating closely with the Department of State and Embassy Country Teams to plan our activities and

Navy member of Combined Joint Task Force–Horn of Africa demonstrates knots to Tanzanian sailor

U.S. Air Force (Elizabeth Rissmiller)

programs to support not only AMISOM, but also the program goals and objectives for PREACT, which aims to defeat terrorist organizations by strengthening regional counterterrorism capabilities and enhancing and institutionalizing cooperation among the region's security forces.

AMISOM forces have driven al-Shabaab out of Mogadishu, creating space for Somalia's TFG to gain legitimacy and effectiveness. All this said, it is important not to overstate our contributions. Neither USAFRICOM nor the U.S. Government writ large is solely responsible for AMISOM's success. Nevertheless, USAFRICOM has been a supportive partner to willing and increasingly capable African countries meeting regional security challenges that have direct national security implications for the United States. Moreover, we are fostering enduring security relationships with willing partners in a dangerous and volatile corner of the world. This will serve us well in an uncertain future.

Building Capacity in the Sahel and in the Maritime and Air Domains

We follow a similar collaborative, regionally focused capacity-building model in combating other threats. For example, in North and West Africa, we focus our efforts against the terrorist organization al Qaeda in the Islamic Maghreb (AQIM). AQIM exploits the undergoverned spaces of the Sahel to plan and execute terrorist attacks. We work within the Department of State–led regional framework for combating AQIM, the Trans-Sahara Counterterrorism Partnership. Despite political uncertainty within some of our TSCTP partners, we have maintained a steady focus over time on building the regional counterterrorism capacity of our partners with small training teams, regional exercises, and our 1206 authorities. The results of these sustained efforts are states increasingly committed to and capable of combating extremism in the Sahel. That said, we all recognize that there is still much to be done.

In the maritime domain, we encourage regional approaches to transnational maritime security challenges such as piracy and illicit trafficking. Our partners have articulated their maritime needs, and USAFRICOM cooperates to help them meet their operational requirements. Our flagship maritime security engagement program is Africa Partnership Station, which provides sustained engagement with mobile training teams, interagency, and international trainers working from U.S. Navy, U.S. Coast Guard, and international partner nations' vessels. Participants include not only U.S. and African naval forces but also vessels from Europe and Brazil. This program improves tactical planning skills, maritime domain awareness, response capabilities, and multinational interoperability.

To enhance regional cooperation in the Gulf of Guinea, we have sponsored and supported, in conjunction with the Africa Center for Strategic Studies, two regional maritime security conferences between the Economic Community of Central African States (ECCAS) and the Economic Community of West African States (ECOWAS). The outcome of these ministerial-level conferences is a draft agreement that provides a firm basis for sustained and effective intra-African maritime cooperation in a region important not only to Africa but increasingly to the United States as well. We already see the beginnings of effective regional cooperation with Nigeria and Benin's joint maritime patrols and Cameroon, Sao Tome and Principe, Equatorial Guinea, and Gabon's participation in ECCAS-led patrols.

We approach air domain security challenges in a similar fashion with a new security cooperation program: Africa Partnership Flight, which features a light footprint, short duration, high impact, sustainability, and predictable engagement with our African partners. It will become the primary Air Force program for building partnership capacity

and will enable committed African states to enhance their aviation capabilities, foster greater regional cooperation, and increase air domain safety and security in Africa.

The Way Forward

Two new programs, the GSCF and the Army's Regionally Aligned Force (RAF), and the potential expansion of the existing National Guard State Partnership Program (SPP) will help USAFRICOM expand, focus, and sustain its efforts.

As already noted, the new GSCF provisions are promising innovations that we expect will facilitate interagency collaboration and unified action and provide a flexible and responsive capacity-building funding source. However, the GSCF is a prototype; it expires in 2015. So while we experiment with GSCF and potentially move toward its full implementation, the effective and well-understood 1206 authorities will expire in 2013. Therefore, it is important that we manage this transition in a manner that maintains continuity and allows us to meet our commitments to willing partners who are on the frontlines helping combat threats to our national security. As soon as practicable, it is essential that we move from temporary authorities and codify best practices and lessons learned into enduring statutes.

Army Chief of Staff Raymond T. Odierno, in his recent *Foreign Affairs* article, explained the concept of aligning Army brigades with regional combatant commands.[14] The RAF concept is an innovative approach consistent with USAFRICOM's emphasis on operating with small teams and maintaining a light footprint. Security cooperation engagements will be conducted primarily by small tailored units from within an aligned brigade. This alignment over time will allow staff and subordinate units to foster enduring security relationships and develop expanded regional knowledge as well as an understanding of our partners' unique security requirements. A RAF from the 2nd Brigade Combat Team, 1st Infantry Division, will begin working with USAFRICOM in FY13, and along with SPMAGTF will provide flexibility and continuity in our security partnerships.

In our efforts to strengthen the defense capabilities of African partners, the SPP assists USAFRICOM in establishing consistent, predictable long-term security partnerships. Currently, there are eight state partnerships in Africa (Botswana and North Carolina, Ghana and North Dakota, Liberia and Michigan, Morocco and Utah, Nigeria and California, Senegal and Vermont, South Africa and New York, and Tunisia and Wyoming). General Craig McKinley, chief of the National Guard Bureau, is actively considering adding two state partnerships as well as long-term possibilities for future growth.

The Security Partner of Choice

USAFRICOM's capacity-building efforts are an integral part of a U.S. Government approach to the threats, challenges, and emerging opportunities across Africa. Moreover, cultivating and nurturing effective security partners is a sound investment and hedge against an uncertain future. In Africa, we look forward to being the security partner of choice for rising nations by building lasting, beneficial partnerships. Our success depends on close collaboration with our interagency partners, Embassy Country Teams, African regional organizations, and African nations.

We believe that over the long run, it is Africans who should address African security challenges and that we most effectively advance U.S. security interests through focused and sustained engagement. In strengthening African defense capabilities and capacities, we enable states to take ownership of their challenges and strengthen their leadership roles. In the famous car maintenance commercial, the mechanic tell his customer, "You can pay me now"—pay a little to have a small but important repair done now—or "pay me later"—pay a lot to have the entire engine replaced later. If African states cannot meet their own security challenges, then the United States and the international community will continue to find themselves responding to crises and contingencies ranging from armed conflict to humanitarian disasters. We believe that for a relatively low cost, our programs are making a positive difference in a rising Africa and demonstrate the enduring value of building partner capacity to the security of the United States. While there are indeed many risks ahead, there is also great opportunity if we are willing to act now to work with our partners. **JFQ**

Richard Tracey and Caterina Dutto Fox, U.S. Africa Command, J5-9, contributed to the development of this article.

NOTES

[1] U.S. Department of Defense (DOD), *Sustaining U.S. Global Leadership: Priorities for 21st Century Defense* (Washington, DC: DOD, January 2012), 3.

[2] "Africa's Hopeful Economies: The Sun Shines Bright," *The Economist*, December 3, 2011, available at <www.economist.com/node/21541008?frsc=dg%7Ca>.

[3] Steven Radelet, *Emerging Africa: How 17 Countries Are Leading the Way* (Washington, DC: Center for Global Development, 2010), 9–25. The 17 countries are Botswana, Burkina Faso, Cape Verde, Ethiopia, Ghana, Lesotho, Mali, Mauritius, Mozambique, Namibia, Rwanda, Sao Tome and Principe, Seychelles, South Africa, Tanzania, Uganda, and Zambia. The six threshold countries are Benin, Kenya, Liberia, Malawi, Senegal, and Sierra Leone.

[4] Ibid.

[5] *U.S. Strategy Toward Sub-Saharan Africa* (Washington, DC: The White House, June 2012).

[6] *Congressional Budget Justification: Foreign Operations*—Annex A: Regional Perspectives, Fiscal Year 2013 (Washington DC: Department of State, 2012), 1–10, 56, 514, 559, and 575.

[7] Ibid.

[8] Ibid.

[9] "Security Council Authorizes African Union Somalia Mission for Further Six Months, Unanimously Adopting Resolution 1772 (2007)," United Nations Security Council, Department of Public Information Web site, available at <www.un.org/News/Press/docs/2007/sc9101.doc.htm>.

[10] "Statement by The Special Representative of the Chairperson of the African Union Commission for Somalia, Ambassador Boubacar Gaoussou Diarra, at the 21st meeting of the International Contact Group for Somalia (ICG-S)," African Union Mission to Somalia Web site, September 20, 2011, available at <http://amisom-au.org/2012/02/statement-by-the-special-representative-of-the-chairperson-of-the-african-union-commission-for-somalia-ambassador-boubacar-gaoussou-diarra-at-the-21st-meeting-of-the-international-contact-group-for/>.

[11] Lauren Ploch, *Countering Terrorism in East Africa: The U.S. Response* (Washington, DC: Congressional Research Service, November 3, 2010), 8, 12.

[12] Ibid, 29.

[13] National Defense Authorization Act for Fiscal Year 2012, Public Law 112-81-December 31, 2011, 125 STAT. 1625–1627, available at <www.gpo.gov/fdsys/pkg/PLAW-112publ81/pdf/PLAW-112publ81.pdf>.

[14] Raymond T. Odierno, "The U.S. Army in a Time of Transition: Building a Flexible Force," *Foreign Affairs* 91, no. 3 (May/June 2012), 10–11.

least get the education at an early stage of their joint tour, but the time investment would need to be supported by the joint commands, and the delivery method must be able to meet educational objectives based on preparing officers for joint responsibilities, not just increasing throughput. If satellite JPME programs are developed, joint educational standards need to be maintained for satellite locations through a curriculum and faculty development hub, such as JFSC, to prevent the education from becoming too regionally focused and limited in scope. Many future JPME concepts have merit, but only if approached with a clear view that the purpose of the education is to prepare officers for joint duty and not just to get them the joint qualification "check in the block."

There are some who say that recent joint operational experience has made the military sufficiently joint and there is no longer a need for JPME programs. This might be true for some at the tactical level, but shortfalls in joint staff and command performance at the operational level continue to be reported in studies, surveys, and leadership comments, showing that improvement is still needed.[13] The continuing importance of JPME is reflected in JCWS graduate surveys, in which well over 90 percent consistently rate the education as valuable to their job performance. It should also be noted that as current joint operations wind down, joint experience will become more limited, and the need for joint education, to prevent a return to parochial Service cultures and a lack of trust and understanding between the Services, will increase.

Improving JPME

Fixing the problems caused by a divided view of JPME's purpose requires a focus on the true purpose of JPME. The Joint Staff and Congress have conducted JPME studies over the past few years and have come to similar conclusions that JPME programs are sound, but need improvement. The studies confirmed that the purpose of JPME is to prepare officers for joint staff and command duties.[14] With this as the focus, we can examine current and future joint duty requirements and build JPME programs that prepare officers to fill these needs.

A first step is to determine which JDAL positions truly need JPME in preparation for duty. Past resistance to culling the JDAL could be overcome by weakening the link to promotion and strengthening the link to joint duty performance. It is an unintended consequence of the Goldwater-Nichols mandate for joint education and experience that the Services often take a check-in-the-block approach to JPME. Changing legislation to relieve the joint qualification promotion requirement would relieve Service pressure to keep JDAL billet numbers artificially high. This would have to be done carefully to prevent an exodus of officers back to Service assignments, where they see greater exposure to those who can help their careers. An alternative would be to encourage joint education and duty as career enhancing, but not mandatory for promotion. This would reduce the Service pressure to maintain JDAL billets just for promotion eligibility and joint assignments could be reduced to only those that involve in-depth joint matters. Only the best officers from the Services should qualify for the remaining joint assignments. To encourage a competitive nature in joint assignments, a requirement that officers with joint service be promoted at least at a rate proportional to the number of JDAL billets the Service holds must be ensured.

A second part of any legislative change should require completion of joint education prior to reporting for joint duty. This would prevent the Services from assigning officers to joint billets without investing in their preparation. Another concept to consider is to promote students upon graduation from JPME institutions, much like our Service academies commission new officers upon graduation. Promoting officers from O-3 to O-4 or O-4 to O-5 upon graduation from an appropriate JPME school would likely increase the level of competition to get into joint schools and billets, perhaps even requiring a screening board for acceptance.

Once the student timing and joint billet management problems are resolved, JPME programs can be shaped and resourced to meet throughput requirements and learning objectives that are focused on the purpose of preparing officers for joint command and staff duties. JPME programs will probably not need drastic change, but improvements in content, organization, and resources should all be considered.

Time is perhaps the most significant investment for JPME. Students must be allowed enough time to reach the educational objectives. The higher the expected level of learning, the more time is required for reading, writing, reflection, and critical thought. Compressing programs or trying to fit them into "free" time will reduce the value of the education and the performance of joint staff and command officers. These officers are being prepared for assignments in which they will be required to collect and analyze huge amounts of information, define complex problems, and concisely communicate comprehensive options and sound recommendations. We cannot take shortcuts in their education because of pressure to get personnel back to their units.

Joint professional military education is vital to U.S. national security. Today's complex environment is high risk and resource constrained. Senior decisionmakers cannot possibly see all the important factors influencing decisions and they need the help of the best prepared joint staff and command officers possible. The quality of the decisions made and the results of our military actions will depend on the quality of the advice provided by well-educated officers. **JFQ**

NOTES

[1] U.S. Congress, House of Representatives, Committee on Armed Services, Subcommittee on Oversight and Investigations, *Another Crossroads? Professional Military Education Two Decades After the Goldwater-Nichols Act and the Skelton Panel* (Washington, DC: U.S. Government Printing Office, April 2010), xiv.

[2] U.S. Congress, *Goldwater-Nichols Department of Defense Reorganization Act of 1986*, P.L. 99-433, October 1, 1986, Sec. 401, 100 Stat. 1025–1026.

[3] Ibid., 1029–1030.

[4] U.S. Congress, House of Representatives, Committee on Armed Services, *Report of the Panel on Military Education of the One Hundredth Congress*, 101st Cong., 1st sess. (Washington, DC: U.S. Government Printing Office, 1989), v.

[5] Ibid., 2–7.

[6] Chairman of the Joint Chiefs of Staff Instruction 1800.01D, *Officer Professional Military Education Policy (OPMEP)*, July 15, 2009, Change 1, December 15, 2011, A-A-4.

[7] Ibid., A-A-5.

[8] Ibid.

[9] *OPMEP*, A-A-6.

[10] Ibid., 7.

[11] *Another Crossroads?* 20.

[12] Joint Staff J7/Joint Training Division, *"The Joint Staff Officer Project,"* Final Report (Washington, DC: Joint Staff, April 2008), 65.

[13] Ibid., 5–7. Also see *Another Crossroads*, xii–xiii.

[14] Ibid., xi. Also see *"The Joint Staff Officer Project,"* 5.

SECURITY FORCE ASSISTANCE
in a Time of Austerity

Special operations Marines observe Armed Forces of the Philippines soldiers during jungle movement

U.S. Navy (Troy Latham)

By **GENE GERMANOVICH**

The Nation's debt and the nearly inevitable decline in the U.S. defense budget have unleashed a debate on exactly what military capabilities and missions require reduction or elimination. To date, the public dialogue has centered largely on cuts to big-ticket procurement and modernization programs (for example, the Joint Strike Fighter) and overseas defense posture (for example, Army brigades in Europe). Defense commentators have yet to sufficiently address how budgetary pressures will limit the military's ability to conduct the wide array of security cooperation activities central to advancing strategic objectives as outlined in national-level documents and combatant command campaign plans. Arguably the most resource-intensive and fiscally complex type of security cooperation is security force assistance (SFA), which is focused on training, equipping, and advising foreign security forces in order to increase their capacities and capabilities. Since this set of activities is continuously highlighted as a key national security tool in strategy documents and policy issuances, a closer examination of SFA in a time of austerity is appropriate.

Although SFA is often an effective tool that limits the possibility of regional conflict, its costs—some apparent and others hidden—are likely to prohibit the Department of Defense (DOD) from continuing to build, at current levels, the capacity of many dozens of foreign security forces around the globe. A more focused approach is needed to target limited resources at long-term, enduring SFA efforts with key nations in each strategically important region. Limited SFA missions may continue as economy of force ventures, but scarce resources should be carefully allocated to those critical partners in each geographic combatant command's (GCC) area of responsibility that can provide the greatest return on the U.S. Government's dollar. Defense leaders have a choice: conduct SFA in many places and risk spreading resources (time, money, and forces) ineffectively, or focus on fewer high-priority nations.

This article begins with an overview of SFA as a national security tool and provides a broad accounting of SFA costs, both apparent and hidden. The conclusion offers recommendations to scope the global SFA effort through stricter prioritization of missions and more creative use of defense resources. An important assumption is that DOD funding for the global SFA effort will remain constant or decrease marginally in an increasingly challenging fiscal environment—as implied by DOD strategic guidance issued by the President and Secretary of Defense in January 2012: "Whenever possible, we will develop innovative, low-cost, and small-footprint approaches to achieve our security objectives, relying on exercises, rotational presence, and advisory capabilities."[1]

This guidance reaffirmed the 2010 National Security Strategy and reinforced the importance of working with allies and partners to build their capacities. What is new is an overt focus on selecting a limited, more efficient set of defense tools, including SFA, to advance strategic objectives.

SFA as a National Security Tool

Over the last decade, building the security capacity of allies and partners has become a pillar of U.S. national security strategy. The U.S. Government, with the Department of State and DOD at the forefront,

Gene Germanovich is a Strategy and Policy Consultant at Booz Allen Hamilton. Over the last 6 years, he has advised U.S. Government clients on national security strategy, defense policy, and security cooperation issues.

has made a strategic investment in training foreign security forces, providing arms, and mentoring rising leaders and organizations. Defense doctrine and policy refer to this set of activities as Security Force Assistance. What distinguishes SFA from other forms of security cooperation is that "SFA activities must directly increase the capacity or capability of a foreign security force or its supporting institutions."[2] While many engagements with foreign security forces contribute tangentially to a partner's capacity or capability (for example, multinational exercises or intelligence-sharing), it is DOD policy that only activities whose "clear and express" purpose is building capacity or capability are considered SFA.[3] DOD Instruction 5000.68, "Security Force Assistance (SFA)," outlines the desired outcome:

SFA activities shall be conducted primarily to assist host countries to defend against internal and transnational threats to stability. However, the Department of Defense may also conduct SFA to assist host countries to defend effectively against external threats; contribute to coalition operations; or organize, train, equip, and advise another country's security forces or supporting institutions.[4]

The intent behind SFA is that by assisting its partners in establishing competent, responsible, and effective security forces, DOD contributes to U.S. Government efforts to prevent regional conflict that threatens American interests and potentially requires U.S. intervention. For example, starting in 2002, the U.S. military has assisted the Philippine armed forces in enhancing their counterterrorism capacity through the provision of training and equipment, thus obviating the possibility that Washington would need to conduct a large-scale counterinsurgency effort to fight al Qaeda–affiliated groups in the southern Philippines.[5] The Secretary of Defense's theater-level guidance directs many similar SFA efforts in each of the GCC's areas of responsibility. By law and policy, GCCs are to plan and execute capacity-building activities in coordination with or under the auspices of State Department programs.

Although previous and current U.S. administrations have held opposing views on a number of policy issues, SFA was adopted as a strategic tool by the George W. Bush administration and wholly endorsed and continued by President Barack Obama's national security apparatus. In its National Security Strategy, the Obama administration states:

Our strategy goes beyond meeting the challenges of today, and includes preventing the challenges and seizing the opportunities of tomorrow. This requires investing now in the capable partners of the future. . . . These kinds of measures will help us diminish military risk, act before crises and conflicts erupt, and ensure that governments are better able to serve their people.[6]

The case of the Philippines demonstrates the promise of SFA. Though they still exist and have a capacity to disrupt, Abu Sayef and other terrorist organizations based in the southern Philippines no longer pose an immediate threat to Southeast Asian allies or U.S. interests. In early 2012, the Philippine air force conducted an air strike that killed 15 militants, including one of the group's leaders. This operational success was made possible in large part by American training and advice over the last decade, which has led to the continual improvement in the intelligence capabilities of the Philippine armed forces.[7]

The Apparent Costs of SFA

In a noncombat environment, SFA is theoretically inexpensive—especially when compared against the cost of U.S. intervention: billions of dollars, casualties, and domestic and international political ramifications. SFA missions are funded through a variety of programs administered by the Department of State or DOD, often through a patchwork of funding streams with associated legislative authorities. For example, consider DOD's primary authority and funding source to provide training and equipment to a foreign security force for the purposes of counterterrorism, known as Section 1206. Fiscal year 2011 cases totaled $247 million, ranging from $300,000 to train Albanian forces for a deployment to Afghanistan to a $44 million package to prepare troops from Uganda and Burundi for counterterrorism missions in Somalia.[8] Compared to the cost of military intervention, or even other portions of the defense budget, capacity-building of a foreign security force seems fairly low cost.

Other DOD funding sources for SFA efforts include operations and maintenance accounts for limited purposes only as explicitly authorized by law, such as deploying civilians to advise ministries of defense and training foreign militaries in support of counterdrug missions. Much broader in scope, State Department programs include Foreign Military Financing and the Global Peace Operations Initiative.

SFA-related funding sources account for the monetary cost of equipment transfers and the operational cost of advise-and-assist missions. Despite a plethora of complex legislative authorities and funding streams, capacity-building dollars are well-tracked by the State Department, Office of the Secretary of Defense (OSD), Defense Security Cooperation Agency, and GCCs.

The Hidden Costs of SFA

While in-theater operational costs are apparent, the more difficult accounting relates to hidden costs, some monetary and others not. Many of these hidden costs are incurred by U.S. Special Operations Command (USSOCOM) and the military Services, which are tasked with organizing, training, equipping, and deploying an array of units and forces to conduct SFA in support of the GCCs.

Congress essentially mandated an improvement in joint education and experience, using promotion as the leverage

Institutional Costs of USSOCOM. Although USSOCOM's most publicized mission is to synchronize planning of global operations against terrorist networks, special operations forces (SOF) have partaken in what is known as "the indirect approach" for many decades, primarily training and advising foreign security forces to counter internal security threats. These SFA efforts have generally been long-term engagements that require instructors with highly specialized advising skills, fluency in one or more foreign languages, and well-honed knowledge of the culture and history of a particular region or country. The institutional costs of providing such specialized forces include investing in years of language training, procuring SOF-particular equipment such as nonstandard aviation platforms, developing doctrine, and including SFA curriculum at institutions such as the Joint Special Operations University.

Recall the case of the Philippines, a mission primarily executed by SOF. While this ongoing operation itself has had a manageable cost, the SOF personnel who led it took years to develop the skill set required to execute the mission effectively.

As a result of intense requirements associated with Afghanistan, Iraq, and the global counterterrorism mission, SOF continues to conduct SFA globally but focuses on nonpermissive environments compelling a small American footprint. With national guidance documents emphasizing SFA, defense leadership has turned to its general purpose forces (GPF) to cover down on a significant portion of SFA requirements around the globe.

Infrastructure for General Purpose Forces. Although generally not as immersive as SOF, GPF advise-and-assist missions still require familiarity with methods of instruction, cultural sensitivity, and at least minimal knowledge of a particular country, in addition to the functional skill set being taught. While DOD has made increasing investments in Foreign Area Officers who possess these skills, GPF by definition remains a broadly qualified force without in-depth expertise in any one area such as SFA.

A common approach to preparing GPF for SFA missions is to send U.S. personnel through an institution that provides a predeployment training program centered on basic advising skills. For example, when a team of helicopter pilots is assigned a mission to train a partner nation's air force, it may prepare by attending the Air Force's Air Advisor Academy to learn how to provide instruction to a less developed air force. The rationale behind this method, utilized similarly by each of the military Services (as shown in the table), is that the Air Force cannot afford to create an entire unit of helicopter trainers, but it can provide GPF pilots with a requisite level of cultural knowledge and familiarity with methods of instruction.

The more SFA missions conducted, and the more diverse they are in purpose, the greater the required throughput and associated cost of preparing U.S. forces. While 1206, Foreign Military Financing, or Global Peace Operations Initiative funds may account for the cost of using helicopter pilot trainers once in theater, they do not cover the salaries, domestic travel, facilities, and curriculum development efforts of the Air Advisor Academy.

Table 1. Military Service Organizations That Train Advisors

Service	Organization	Mission Summary
Army	162nd Brigade, Fort Polk, LA	Provide training to U.S. personnel in advisor skills, combat skills, and SFA skills
Navy	Maritime Civil Affairs and Security Training Command	Prepare U.S. forces to execute civilian-to-military operations and military-to-military training in support of security cooperation and security assistance requirements
Marine Corps	Marine Corps Security Cooperation Group	Conduct assessments, planning, related education, and training for U.S. personnel, and advisory support to ensure unity of effort in building partner nation security forces
Air Force	Air Advisor Academy	Provide U.S. advisors with predeployment training that includes mission training, culture training, and combat skills
Coast Guard	U.S. Coast Guard Training Center Yorktown International Mobile Training Branch	Provide Coast Guard personnel training in counterterrorism, force protection, survival skills, and advanced training in their specialty fields to prepare them for technical training and consulting with partner nations

Larger scale SFA efforts with standard military units (as opposed to small, highly tailored teams of advisors) also have associated posture costs. If implemented, the U.S. Army's envisioned Regionally Aligned Brigade—a sizeable force construct used to service dozens of SFA requirements in each of the GCC's areas of responsibility—will require significant expenditures on facilities, particularly if based in theater. The Marine Corps's Special Purpose Marine Air Ground Task Force (SPMAGTF) for Security Cooperation construct is already in place, an example being the SPMAGTF operating out of Naval Air Station Sigonella in Italy. This SPMAGTF for Security Cooperation is a rotational force of hundreds of Marines who train African security forces in peacekeeping and counterterrorism. Individual training activities conducted by SPMAGTF are funded through the GCC, State Department, and partner nation funding sources. The cost of deploying the force and basing it in Italy, however, is borne by the Marine Corps.

An additional institutional cost is OSD and Joint Staff funding and manpower for organizations such as the Joint Center for International Security Force Assistance, which serves as a source of SFA expertise and captures and disseminates lessons learned from SFA missions.

The Planning Penalty. One of SFA's unique features is the diverse set of missions, with examples including training pilots for functions associated with a Federal Aviation Administration–like organization, providing night vision goggles to enhance the capabilities of an elite counternarcotics unit, and advising a ministry of defense in how to build a personnel payment system. Making the planning effort more complex is the milieu of legislative authorities and funding streams, which is unlikely to change due to congressional resistance to a simpler legal framework. Thus, unlike a more standard deployment (for example, a carrier battlegroup), GCCs spend considerable resources to justify, plan, fund, and assess individual efforts. Military Services incur the same planning penalty as they organize, train, equip, and deploy GPF forces to conduct SFA.

Furthermore, an insufficient number of Security Cooperation Officers (SCOs) at many Embassy Country Teams increases the planning burden on GCCs and their Service components. SCOs serve as the primary interlocutor among GCCs, the State Department, and host nations. Without an adequate

Airman interviews graduate of Air Advisor Course in Iraq to ensure school is meeting operational needs

U.S. Air Force (Randy Redman)

SCO structure (some Country Teams have only one), GCCs risk conducting activities unlinked to State Department objectives, and must dedicate more time and effort to administrative issues such as obtaining visas. On many occasions, staffs are stressed to a point where planning time for logistics and funding precludes attention to optimizing the nature of the training, equipment transfer, or advisory support itself.

Stressing the Force for Leadership. SFA's least visible cost—and arguably the most taxing one—is not one measured in dollars. Working with foreign security forces requires a level of maturity, experience, and skills most frequently found in the senior ranks of officers and staff noncommissioned officers. Difficult to cultivate in mass and capped by legislation, mid- to senior-level leaders are a treasured resource. To provide a disproportionate level of senior leadership for SFA missions, the Services routinely pull leaders from nondeployed units that are in predeployment training for another mission. To illustrate, consider a Marine Corps infantry battalion. The Marine Corps routinely sends captains (O-3) and above from U.S. home stations to train foreign security forces. In their absence, a nondeployed unit's leadership is degraded, with potential consequences to morale, safety, and preparedness. In the worst case, the infantry battalion could be called to respond to a crisis while its key leaders scramble to return from their temporary SFA assignments.

Scoping the Security Force Assistance Effort

The following recommendations are designed as specific policy prescriptions that adhere to the spirit of recent DOD strategic guidance by more appropriately scoping DOD's global SFA efforts. In addition to stricter prioritization at the theater level, decisionmakers should emphasize several emerging SFA concepts that will result in more efficient and effective use of defense resources.

Refine Theater-level Guidance. An inadvertent consequence of defense leadership's continual focus on SFA has been an undue amount of GCC concentration—some of it directed by OSD and some self-generated—on capacity-building in countries where other forms of military-to-military engagement are sufficient for achieving strategic objectives. To supplement broad strategic guidance, OSD should issue more detailed theater-specific guidance that precisely conveys where U.S. forces will engage with allies and partners, and for what purpose. To date, this type of guidance has generally entailed an all-of-the-above approach to working with a large set of critical partners in each GCC's area of responsibility.

Given budgetary pressures, it is becoming imperative to provide greater specificity to GCCs on where they should focus on enduring capacity-building efforts versus maintaining more routine military-to-military ties. Criteria for determining where SFA is a plausible course of action that will promote U.S. national security interests includes linkages to high priority war plans, host nation appetite, the ability to harness limited interagency resources, and sustainability. Absent these necessities, the focus should remain on security cooperation efforts short of capacity-building.

Synchronize Efforts of Special Operations and General Purpose Forces. To optimize division of labor, GCCs and their Service components should increase coordination and synchronization of efforts with the GCC's theater special operations commands. The military Services lack SOF institutional legacy of working with foreign security forces, and GPF are by nature less adept at this mission set than

U.S. Army (Peter D. Lawlor)

Navy technician and Uruguayan EOD robot operator engaged in training coordinated by Maritime Civil Affairs and Security Training Command

USSOCOM-trained advisors. But the global demand for SOF, who will be the last forces to leave Afghanistan and are required for the counterterrorism fight into the foreseeable future, necessitates that GPF partake in DOD global SFA efforts.

A promising construct for SOF-GPF collaboration is one whereby GPF train partners in basic skills and, when the foreign security force has matured, hand the effort over to SOF to conduct advanced individual and small unit training. In some cases, once SOF has concluded the advanced training, the partner nation's military may be ready for sustainment training via large-scale multinational exercises shepherded by U.S. GPF. A continuing SOF-GPF dialogue is beneficial throughout the capacity-building process.

SOF-GPF synchronization and an explicit division of labor, where warranted, reduces the amount of time and level of effort the Services need to dedicate for training U.S. personnel for SFA missions, while mitigating the worldwide demand for SOF. This integrated approach also provides the foreign security force with the most suitable trainers at each stage of capability development.

Focus on Regional Security Organizations. Assistance to regional security organizations, currently emphasized to various degrees by each of the GCCs, has continuing merit and financial advantages. For example, the State Department–funded Africa Contingency Operations Training and Assistance program involves U.S. forces training African partner nation militaries and providing the equipment needed to support peacekeeping operations and counterterrorism efforts in the Horn of Africa region. Another variation of this model, often referred to as the "train-the-trainer" approach, is the Colombian Marine Corps Regional Training Center in Covenas, Colombia. Originally a venue for U.S. Marines to train with Colombian marines, the training center is now a regional destination for Latin American naval infantry forces, with Colombia in the lead. Over several decades, this center has nurtured regional cooperation among historically suspicious neighbors while enhancing the capacity of foreign security forces to conduct counterdrug operations.

Investing in regional training organizations presents several fiscal benefits. At multinational training centers, the United States can train more foreign security forces in the course of one deployment. Working with multiple foreign security forces at one location reduces predeployment training requirements, intra- and inter-theater travel, and operational costs on the ground. Where feasible, the train-the-trainer approach serves as an SFA force multiplier: the United States can slowly reduce its SFA level of effort while one or more mature partners take the lead for training security forces. Finally, U.S. foreign policy benefits when the security forces of a region develop collective solutions based on interoperability and trust.

Send Qualified Security Cooperation Officers to the Right Countries. To alleviate the burdensome planning requirements associated with SFA missions, OSD should work with the State Department to engineer a modest increase in the number of SCO personnel at U.S. Embassy Country Teams. Many defense analysts have suggested increasing SCO presence worldwide, particularly in African nations where the gap is most acute, but to date little action has been taken due to the associated manpower and funding costs. A more manageable solution is to increase SCO presence only in each GCC's high-priority countries where DOD leader-

ship determines the SFA effort should be most comprehensive. Some positions could be realigned from Europe, where the SCO presence remains relatively strong as a result of the Cold War's legacy of security assistance.

Among planners and commanders, SCOs are recognized as a pivotal component of the U.S. Government's effort to enhance the capabilities of foreign security forces. Given their location at American Embassies, SCOs are in an optimal position to synchronize a GCC's vast array of U.S.-led security cooperation activities, including capacity-building efforts, which are ongoing in many partner nations. Recognition of the SCO as a central coordinator for SFA missions is a positive development that has led to a growing emphasis on improving SCO training prior to their tours at Country Teams. In addition to adding a modestly higher number of SCOs in high-priority nations, the Defense Security Cooperation Agency and military Services should continue to improve training available to these key individuals.

Conclusion

There are two counterarguments to the case for more carefully scoping the DOD worldwide SFA effort. First, SFA is an effective lever in the defense and foreign policy toolkit. Combatant commands provide training, equipment, and advice to foreign security forces in order to curb the need for direct U.S. intervention, develop future coalition partners, enhance operational access and posture, and support diplomatic objectives. Scaling back on the number of SFA efforts may entail operational risk. This counterargument has merit but should be considered in a broader context: DOD conducts myriad security cooperation activities beyond SFA. The defense toolkit also includes multinational exercises, intelligence cooperation, senior leader engagement, and many similar shaping activities. These military-to-military interactions also serve both defense objectives and diplomatic endeavors and should be continued to the extent possible. Additionally, scaling back on the number of SFA efforts would result in a qualitative enhancement of the highest priority missions.

The second and related counterargument posits that the cost of SFA—even considering the institutional commitments by USSOCOM and the Services—is lower than those of regional conflict or unchecked transnational threats that risk forcing the Nation to engage in combat operations. While this perspective also has appeal, today's fiscal pressures necessitate reductions in nearly every area of the defense budget with precious few exceptions such as cyberspace capabilities and ballistic missile defense. Without stricter prioritization and more creative utilization of resources dedicated to SFA, policymakers risk spreading resources (time, money, and forces) ineffectively.

In a world where weak states and transnational actors pose a threat to U.S. interests and several regional powers are emerging as competitors, DOD's global SFA mission, if properly integrated into broader U.S. Government efforts, is a wise strategic endeavor that is generally cost-effective. But if GCCs lack the guidance to scope their SFA efforts, the inevitable endstate is a high number of suboptimal SFA missions—with USSOCOM and the Services scrambling to prepare U.S. forces for an overly diverse set of advise-and-assist requirements in a difficult budgetary environment. A better result would be focused high-priority efforts in each region of the world that have a chance to deliver the same kinds of results witnessed in the Philippines. In today's age of austerity, tough choices must be made and lower-cost, innovative concepts must be adopted. **JFQ**

NOTES

[1] The White House, *Sustaining U.S. Global Leadership: Priorities for 21st Century Defense* (Washington, DC: The White House, January 2012), 3. Emphasis in original.

[2] DOD Instruction 5000.68, "Security Force Assistance (SFA)," October 27, 2010, 2.

[3] Ibid.

[4] Ibid.

[5] Department of Defense (DOD) *Quadrennial Defense Review Report* (Washington, DC: DOD, February 2010), 28.

[6] *National Security Strategy* (Washington, DC, The White House, May 2010), 27.

[7] Simone Orendain, "10-Year US Counterterror Support Paying Off: Philippine Military," *Voice of America*, February 16, 2012, available at <www.voanews.com/english/news/asia/10-Year-US-Counterterror-Support-Paying-Off-Philippine-Military-139434983.html>.

[8] Nina M. Serafino, *Security Assistance Reform: "Section 1206" Background and Issues for Congress* (Washington, DC: Congressional Research Service, 2012), 20–26.

PME and Online Education in the Air Force

Raising the Game

By KATHLEEN A. MAHONEY-NORRIS *and* JOHN ACKERMAN

The U.S. House of Representative's 2010 assessment of professional military education (PME)—*Another Crossroads? Professional Military Education Two Decades After the Goldwater-Nichols Act and the Skelton Panel*—was clearly intended to present a comprehensive evaluation of education for U.S. military officers, and in many ways, the report accomplishes that goal admirably.[1] However, Another Crossroads does not assess the area of distance learning in much depth or detail. In fact, the 238-page report contains only nine brief comments or references to distance learning. This lack of detailed consideration of nonresident education was certainly understandable in 1989 when the U.S. House Armed Services Committee issued its first critical assessment of PME in the well-known Skelton Report.[2] After all, that was still the era of the traditional correspondence or "box of books" distance learning method for those who did not attend a PME school in residence.

But the lack of sustained consideration of distance education programs is more problematic today for at least two major reasons. First, a large percentage of U.S. field grade officers receive at least some, if not all, of their required intermediate- and senior-level joint and Service-specific professional military education via flexible, adaptable distance education methods. Equally important, many of the online learning programs are increasingly high quality, employing interactive technologies and fostering critical thinking, research, and writing skills.

Both of these factors are particularly relevant when considering PME for U.S. Air Force officers, especially at the intermediate level. While the Air Command and Staff College (ACSC) at Maxwell Air Force Base typically educates some 500 majors and equivalent ranks in residence each academic year—awarding them joint PME Phase I (JPME I) credit, their Air Force intermediate developmental education, and a Master's degree—that number pales beside the 3,869 graduates who received their JPME Phase I and intermediate developmental education through ACSC's self-paced distance learning ("correspondence") program in 2011.[3] In fact, at any given point, some 10,000 students are enrolled in the ACSC non-Master's distance education program to attain their required PME. Additionally, for academic year 2012, ACSC's relatively new online Master's degree program (implemented in 2007) awarded JPME I credit and the same Master's degree as the residence program to 488 graduates. The online program now typically enrolls from 1,000 to 1,200 students in each of the six 8-week terms held each year. Comparing these distance education student numbers to resident program student numbers, it is evident that no more than 20 percent of Air Force majors complete their PME via residence methods.

Thus, while granting that the House Subcommittee was correct in assuming in its 2010 report that in-residence education for officers would provide the optimal education, clearly this opportunity cannot realistically be made available to the majority of (Air Force) officers. Limitations such as repetitive operational deployments, the not-inconsiderable costs of educating students in residence (especially in an austere budgetary era), and other resource constraints—such as deficiencies in institutional infrastructure and numbers of faculty—all tend to militate against substantially increasing the numbers of in-residence students.

Some observers would not be as concerned about this situation, perhaps partly because of the perspective that it is legitimate to focus educational efforts on "the best and brightest" officers, who are usually competitively selected to attend PME in residence. Yet it is increasingly difficult to deny that all officers need to be well educated in today's globalized age of complex and continuous military operations—including those in the Reserve Components, who unfortunately are least likely to attend PME in residence. The context of irregular/asymmetric warfare and continuing stabilization and reconstruction missions that require diplomatic, political, economic, and specific military skills means that even the most junior officers are faced with time-sensitive decisions that may have important consequences. In the information age, the misstep of just one military member or small unit can have major political and strategic consequences, as incidents from Abu Ghraib

ACSC

Air Force officer en route home from Iraq receives Master's degree at ACSC

to accidental civilian deaths during military operations in Afghanistan demonstrate.

Furthermore, it is vital that officers be culturally sensitive and attuned to work effectively together within an interagency and coalition environment. And with more and more U.S. military members involved in security cooperation activities, the necessity for rigorous and substantive education of U.S. officers so they can better serve as effective role models and mentors in the critical task of educating and training other militaries is even more apparent, as highlighted by *Another Crossroads*. Congress could scarcely have been more explicit in underscoring the importance of quality education today for producing competent officers and leaders:

The primary purpose of PME is to develop military officers, throughout their careers, for the rigorous intellectual demands of complex contingencies and major conflicts. The United States cannot afford to be complacent when it comes to producing leaders capable of meeting significant challenges, whether at the tactical, operational, or strategic levels of warfare. Military officers must think critically, communicate well, conduct themselves with integrity, and lead others to perform strenuous tasks in difficult and often dangerous situations. As a matter of national security, the country's continuing investment in the PME system must be wisely made.[4]

The authors contend that ensuring a quality educational opportunity for a much larger percentage of field grade officers via challenging, quality online learning programs would be a wise investment for U.S. national security—one that may also prove cost-effective in an increasingly constrained budgetary environment. To support that contention, this article first provides a short assessment of the increased growth and quality of distance education and online learning programs in the United States. The bulk of the article then details the ongoing Air Force experience with distance education and online learning, making comparisons between the online Master's degree program and ACSC resident education as applicable. Finally, some conclusions and projections are offered based upon the Air Force experience to date.

Expansion and Quality of Online Learning

The apparent congressional lack of focus on distance education in PME is puzzling in light of the rapidly accelerating growth of online education at military and especially civilian institutions—and this growth trend is shared by Ivy League universities and community colleges alike. A recent assessment of online education in the United States by the respected Sloan Consortium noted the following data points which underscore the substantial growth:

- Over 6.1 million students were taking at least one online course during the fall 2010 term—an increase of 560,000 students over the number reported the previous year.
- The 10 percent growth rate for online enrollments far exceeds the less than 1 percent growth of the overall higher education student population.
- Thirty-one percent of higher education students now take at least one course online.[5]

Of course, the quality of online education is crucially important, and in that regard the Sloan report has recorded increasingly favorable opinions in surveys taken since 2003 of top educators who compared learning outcomes for online versus resident (face-to-face) education. The Department of Education's own extensive meta-analysis and review of numerous empirical studies comparing online, resident, and blended learning approaches concluded in 2010:

In recent experimental and quasi-experimental studies contrasting blends of online and face-to-face instruction with conventional face-to-face classes, blended instruction has been more effective, providing a rationale for the effort required to design and implement blended approaches. When used by itself, online learning appears to be as effective as conventional classroom instruction, but not more so.[6]

Whether used in conjunction with residence teaching methods or on its own, online learning is poised to make valuable contributions to expanding and deepening military educational efforts.

ACSC: Residence and Online Education Programs

Originally called the Air Command Staff School, the Air Command and Staff College began its residence program for majors in 1946 and has produced over 38,000 graduates, so it has some 60 years of educational experience to draw upon compared to the relatively new online Master's program described below. Nevertheless, the basic components of ACSC's residence and online programs mirror one another; it is commonly stated that ACSC actually has one program with two delivery methods—residence and online. Both the residence and online programs have been certified by the Chairman of the Joint Chiefs of Staff to award JPME I credit (and by the Air Force to fulfill its intermediate-level PME requirements), and both programs are accredited by the Southern Association of Colleges and Schools to award a Master's of Military Operational Art and

Dr. Kathleen A. Mahoney-Norris is Professor of National Security Studies at the Air Command and Staff College. Lieutenant Colonel John Ackerman, USAF (Ret.), Ph.D., taught at the Air Command and Staff College for 10 years and currently teaches and develops curriculum for several universities online.

Science degree. Since ACSC is an intermediate-level PME school, the curriculum is centered on the operational level of war and consists of 11 courses (33 credit hours) with the same learning outcomes for both programs in areas ranging from security and culture studies to strategy to leadership to joint warfighting and research. The in-residence degree program takes approximately 10 months of full-time study to complete, and students go through a structured program. They do have some flexibility when it comes to the research/electives program throughout the year, and they may participate in several other special educational programs.

In 2006, Air Force leadership directed ACSC to develop an online Master's degree equivalent to the resident program, underscoring the increasing need for a flexible approach. This flexibility was required in light of continuing high operations tempo and multiple deployments for Air Force members, balanced against joint/Service PME requirements, and growing expectations that officers should earn an advanced degree. In the summer of 2007, majors who had not yet completed JPME I were offered the option of receiving their JPME, their Air Force PME, and an accredited Master's degree through the Online Master's Degree program (OLMP), administered via a Web-based learning management system. The program expanded in 2010 when senior Air Force captains who had completed their initial PME through Squadron Officer School were offered the option to receive their Master's degree online, too, through a modified curriculum track within the OLMP. Then, in 2011, graduates of the Fighter Weapons School were provided the opportunity to receive a Master's degree through a unique blended combination of courses taken online (via the OLMP) and in-residence coursework at the Fighter Weapons School at Nellis Air Force Base, Nevada. As captains obviously do not receive JPME I credit along with their Master's degree, the remainder of this article focuses on majors who complete JPME in the ACSC program.

In contrast to the 10-month residence program, online students would normally expect to complete their PME and degree on a part-time basis in 2 years (although they can take up to 5 years). Flexibility in this program is a priority, as students decide for the most part in what order they wish to take their 11 courses, what number of courses they wish to take during each 8-week term (although no more than two courses per term is normally considered appropriate), and whether they wish to take a term or two off from pursuing courses. This is possible because all courses are offered during every one of the six yearly terms, and it is student demand that drives the number of sections scheduled for each course. Another advantage of this flexible delivery method is that students can choose courses based upon upcoming assignments. For example, a student selected for command may decide to take the Leadership and Command course just prior to taking command, or a student being deployed to work with other Services may take the joint courses. However, the online program is less flexible than the residence program in the sense that students in the online program do not have a choice of electives—all of them must complete the Research I and II courses. On the other hand, within some limits, they can pursue a research topic of their own choice.

ACSC OLMP student participates in National Security Studies Course Online Discussion Group

ACSC

The OLMP is constantly evolving and adapting; it can quickly respond to increased enrollments in the overall program and/or demands for more sections of particular courses. It is extremely flexible in terms of balancing individual professional and family concerns. Many more officers now have the opportunity to complete their intermediate-level PME requirements and a Master's degree tailored to meet the demands of educating members of the Department of Defense in relevant national security, regional-cultural, strategy, leadership, and joint and coalition warfare topics. As a representative comment from one graduate noted in 2011 (all students are invited to complete an anonymous exit survey upon graduation from the OLMP):

The ACSC OLMP courses immediately benefitted me while I was deployed in a joint billet. As I was taking many of the joint warfare courses during my deployment, I was able to immediately utilize the information I gained from the classes in my job. . . . Overall, the courses in leadership, joint operations and planning, and cultural studies have made me a much better officer and leader in my career field.

However, even conceding that the OLMP has these benefits, such advantages do not demonstrate that the online program would meet the type of rigorous, demanding quality education required by Congress for PME colleges. To assess the quality of ACSC online education, this article next addresses two of the four areas identified by the original Skelton Report as crucial to quality PME: faculty and pedagogy.[7]

Assessing Quality

The Skelton Panel in 1989 and Congressional Subcommittee in 2010 were particularly concerned with ensuring the quality of both PME faculty and pedagogy. In their view, one of the hallmarks of an effective faculty lay in subject matter expertise and scholarly and critical thinking ability as reflected in terminal degrees. *Another Crossroads* singled

out the move to accreditation of graduate degree programs by almost all intermediate- and senior-level PME colleges as one specific factor that had "helped the schools attract higher-quality faculty members thereby improving the PME curricula and quality of teaching."[8] In fact, the enhancement of qualifications among faculty at ACSC from 1989 to 2012 is striking. While in 1989 there were no civilian faculty members, by academic year 2012 the teaching faculty consisted of 38 civilian and 91 military members.[9] All military faculty members have completed at least intermediate-level PME, as have some civilians (often retired military or with some military background), although not necessarily all have done so in residence. Even more telling is the fact that 39 faculty members have doctoral degrees, 26 of whom are civilian faculty and 13 military. Almost all Ph.D.s of the ACSC faculty are in curriculum-relevant areas including political science, international relations, military history, public policy, leadership, and education.

The assumption is that the increased number of civilians improves the faculty's diversity and depth as does the expansion of terminal degrees among both civilian and military faculty. Presumably these trends have led to better education, which was an explicit presumption contained in the congressional reports on PME. The fact that both the residence and online programs have met the criteria for graduate education standards is also evident in ACSC accreditation by the Southern Association of Colleges and Schools, while Joint Staff evaluations continue to certify that intermediate-level PME requirements are being met.[10]

When specifically assessing the credentials and quality of ACSC online faculty, it would be extremely misleading to survey only the numbers of full-time faculty assigned to ACSC's Distance Learning Directorate (DL). In fact, most of the 24 full-time DLC faculty—16 military (3 with Ph.D.s) and 8 civilian (5 with Ph.D.s)—are categorized as "course directors" who are responsible for the development and oversight of the online curriculum, in addition to monitoring the quality of the assigned sections of their particular course during each term. These faculty members/course directors commonly teach online courses at least once a year and teach the in-residence versions of the courses (and often an elective) each year. Naturally, they cannot also teach the 8 to 11 online sections of the courses (each with 13–20 students depending on student demand) that may be scheduled per term. Thus, the OLMP depends on credentialed adjunct faculty who are competitively chosen and centrally managed through a contract administrator (a Ph.D. with many years of relevant professional and online educational experience) in residence at ACSC.

Examining the composition of the geographically dispersed adjunct faculty who teach online, out of a pool of some 90 civilian and military members, 38 hold Ph.D.s or equivalent terminal degrees, with several faculty members in the process of completing their doctoral studies. The number of times faculty members teach varies according to their own professional situations and student demand for courses each term. A typical term would feature 52 online faculty teaching with the following characteristics: 22 with Ph.D.s; 28 with prior resident PME teaching experience; 10 sister-Service members; 18 current/former joint officer qualified; 30 with command experience; and 21 of 0-6 rank (Active duty and retired), plus 1 general officer. The fact that so many individuals with varied military backgrounds are drawn to teaching military officers is probably not surprising, but it certainly adds to the value and relevance of the program.

it is possible to argue that the overall quality of the ACSC online faculty is comparable to that of the in-residence faculty

An online faculty member's teaching performance is continuously assessed each and every term—weekly if not daily—by the contract administrator, course directors, and other staff at ACSC, along with the students. The very nature of the open online environment means that each online faculty member receives many more evaluations than in-residence faculty. It is quite easy to remove unsatisfactory teachers in this competitive system; thus, the adjunct faculty roster is an impressive list of seasoned senior teachers with appropriate subject matter, scholarly, and professional expertise. Adjunct faculty members have also proven themselves adept at teaching online, a methodology that is not automatically or easily mastered by those who teach in brick-and-mortar classrooms.

Based on the type of qualifications and faculty management processes summarized above, it is possible to argue that the overall quality of the ACSC online faculty is comparable to that of the ACSC in-residence faculty. In fact, as the authors can attest, student course evaluations and program exit surveys consistently praise the outstanding caliber and professionalism of the experienced, diverse instructors they encounter online. This particular point has been underscored by focus group discussions held in the last 2 academic years with students in the resident program who had previously completed the online Master's degree or had at least taken more than one of the online courses prior to attending ACSC in residence. Student comments from these discussions were nearly unanimous in comparing online faculty very favorably to resident faculty, emphasizing in particular the subject matter expertise and strong teaching skills of their online instructors.

While the above discussion provides some perspective on the quality of online faculty, it is equally important to assess pedagogy. In this regard, Congress's 2010 report noted approvingly that "PME institutions have generally implemented the Skelton Panel recommendations on improving teaching practices and have adopted more demanding standards. Student-centered seminar discussion groups are the core means of instruction at the in-residence schools."[11] At this point, online education as offered via the ACSC OLMP cannot replicate the seminar-based, active learning (Socratic dialectic) of in-residence education. Nonetheless, student-centered and instructor-facilitated discussion groups are the core means of instruction in the OLMP (along with essay and paper assignments and some group exercises).

In the typical course, students are assigned to one of several seminar discussion groups, and for each week's lesson, they are required to address one or two questions related to the lesson readings and objectives, posting their written responses online. Students must additionally respond to at least two other students' postings each week. In this way, an asynchronous running "discussion thread" is carried throughout the week (the online program was designed to be asynchronous to accommodate military officers assigned and deployed in many loca-

tions and time zones). Many instructors find student responses to be quite thoughtful, well researched, and informed when they have time to reflect upon a response. Faculty members also note that, unlike face-to-face education, the "discussion" online includes all students and tends not to be dominated by one student or group of several students. In fact, individual course evaluations and exit surveys completed by students as they graduate reveal almost universally favorable comments about the high-quality interaction and learning that take place through these online discussions. Significantly, by a large majority, the ACSC students who took part in the focus groups noted above rated the quality of academic interaction, discussion, and learning between the residence and online programs as comparable (although networking and getting to know other students on a personal level were recognized as clearly superior in the residence program).

Another important pedagogical area involves nurturing critical thinking, research, and writing skills, which are considered essential for the professional development of officers. In that regard, students in the online Master's program usually write considerably more than in the residence program because all of their discussion postings (and assignments) are written, not presented verbally as in a residence seminar room. Exit surveys often single out the extensive writing required as improving their research, communication, and thinking skills. One student who had first taken ACSC online courses and then attended in residence during academic year 2012 concluded in the focus group discussions, "I can now say that the OLMP challenged me in a much more cerebral way. All correspondence relied upon the written word that you were forced to support with evidence."

Furthermore, all OLMP students research and write a substantive paper through a two-course sequence as a degree requirement, whereas residence students have several writing options available other than a long research paper to fulfill their requirements. Again, in exit surveys, online students often cite completing their research project as one of the highlights of the program in terms of its lasting value for improving their research, writing, and critical thinking skills. One data point demonstrating the quality of research conducted in the online program is that the online students' research papers compete equally with resident student papers for yearly awards sponsored by external organizations such as the Defense Intelligence Agency and the Armed Forces Communications and Electronics Association. For both academic years 2011 and 2012, online students won 8 out of 18 of these externally sponsored research awards.

Regardless of the many favorable aspects that may accrue to an online program, clearly a brick-and-mortar program cannot be fully replicated online, and student experiences will differ in a residence versus a distance education program. To state the obvious, students in a residence program such as at ACSC have the leisure to study and reflect on the curriculum on a full-time basis, all while interacting professionally and socially with fellow officers from various Services and countries. The OLMP as currently structured does not offer that opportunity (although the presence of sister Service and joint qualified officers on the online faculty offers some compensation). Additionally, the OLMP is pursued on a part-time basis (each course requiring 10–15 hours of work per week) as students juggle work and personal commitments. These two factors constitute probably the greatest weaknesses of the online program, but the alternative for the majority of midgrade Air Force officers is to earn what is often viewed as a "square-filler" advanced degree of perhaps dubious quality, primarily with only civilian classmates, and to take required PME via traditional correspondence methods. Fortunately, even this latter, much criticized method of earning PME is being challenged by planned upgrades at Air Command and Staff College as described in the next section.

if all military members and most civilian members need professional military educational programs, then alternatives beyond the constraints of residence programs need to be seriously examined

Transforming PME through Online Learning

Looking to the future, it seems undeniable that technological advances will make online education ever more flexible, responsive, and interactive (and presumably cheaper, which seems likely to become an increasingly important factor). In fact, ACSC's online Master's program is experimenting with incorporating new social media tools into some of its courseware, from blogs to personal journals to group Wikis, to assess how these new methods may enhance learning.

But it is equally worth considering whether, and how, online tools may help improve in-residence teaching via what is commonly termed "blended learning." As one example, for the past 3 academic years the authors have experimented with teaching the first truly blended learning, year-long research elective course at ACSC. Students in the unique Future Trends elective begin their consideration of trends that may affect national security and methodological approaches through face-to-face seminar discussions in the fall semester, while also building their initial research proposal via an online seminar discussion group with their fellow students. In the spring semester, they focus on conducting necessary research to support their papers, while regularly posting sections of their papers online in a discussion group. Thus, as students build first their proposals and then their papers, they post these products on a regular weekly/biweekly schedule, receiving constant detailed feedback online from fellow students and faculty on each segment of their proposals/papers.

All faculty observations and student evaluations of the blended learning approach in this ACSC course have been overwhelmingly positive in terms of assessing the amount of learning and collaboration that occurs. As one student put it in the anonymous Future Trends course evaluation for academic year 2012: "An outstanding elective that fosters critical thinking and takes advantage of peer critiques/support through the blended course environment (classroom, blackboard [online learning management system], and self-paced research). Gives students unprecedented leeway in selecting a research topic that is relevant." This mixed approach has potentially enormous benefits as studies measuring learning outcomes in higher education continue to conclude that a blend of face-to-face and online teaching methods seems to be the most effective instructional method of all.[12]

While to date these online-associated efforts are quite promising, of greatest significance in terms of the number of officers

affected is the concerted effort under way to move the 10,000 students enrolled at any one time in ACSC's non-Master's PME correspondence methods to the next generation of a fully online learning environment. (Notably, this effort resonates beyond the Air Force as 17 percent of enrollees are U.S. Navy officers; other Services and civilians are also well represented.) By the fall of 2012, all seven ACSC courses required to fulfill JPME I certification and Air Force intermediate-level PME objectives will be Web-based and accessed through the Blackboard learning management system—the same system used in the OLMP.

Within the self-paced portions of each course, students will first complete a variety of computer-based interactive learning activities—lesson checks, critical thinking activities, and exercises. In one unique component, students will deepen their understanding of national security themes by completing an individualized, self-paced National Security Decision Making simulation where students act as junior staff members assigned to the National Security Council staff. (This simulation has already been successfully beta-tested, generating extremely positive student feedback.) Additionally, at three different points within the new program, students will be placed into cohort groups to complete 2 to 3 week seminars that feature peer-to-peer interaction and instructor facilitation, concluding the program with a Joint Warfare phase. This structure, with its enhanced technology, will help to address the student demands consistently revealed in PME correspondence program surveys for greater interaction with fellow students and faculty and a more stimulating learning experience. It seems safe to say that the new program will foster enhanced levels of learning and, ultimately, critical thinking.

As noted above, the congressional 2010 assessment of PME did not consider distance education to any great extent. Yet online learning has moved far beyond those traditional distance learning correspondence programs that were not interactive, let alone intellectually rigorous. The capability now exists to provide many more officers with carefully designed, intellectually challenging programs that take advantage of highly interactive online technologies. The assessment provided here of ACSC's online Master's program presumably provides some evidence for the contention that online programs can provide high-quality graduate and required military education for officers, although clearly more systematic empirical studies are required to substantiate this conclusion. In any case, the ongoing transformation of ACSC's non-Master's program should prove to be immensely valuable for enhancing JPME I and Air Force intermediate developmental education for exponentially greater numbers of officers and civilian employees of the Department of Defense.

If, as has been argued here, all officers (indeed, one could argue all military members and most civilian members of the Department of Defense) need professional military educational programs that help them to better understand and support national security needs in today's complex threat environment, then alternatives beyond the constraints of residence programs need to be seriously examined. Furthermore, online learning can also provide the opportunity for lifelong learning and study so necessary for nurturing critical thinkers and strategists. Indeed, as pointed out by John Nagl and Brian Burton in their insightful comprehensive study *Revitalizing America's Military Officer Corps*, "distance learning and self-directed online education can provide important and flexible education program [sic] for officers. Although the face-to-face interaction available at 'brick-and-mortar' schools is preferable, current technology makes the establishment of a continuous PME program more practical than ever."[13] **JFQ**

NOTES

[1] U.S. Congress, House of Representatives, Committee on Armed Services, Subcommittee on Oversight and Investigations, *Another Crossroads? Professional Military Education Two Decades After the Goldwater-Nichols Act and the Skelton Panel* (Washington, DC: U.S. Government Printing Office, April 2010).

[2] U.S. Congress, House of Representatives, Committee on Armed Services, *Report of the Panel on Military Education of the One Hundredth Congress*, 101st Cong., 1st sess. (Washington, DC: U.S. Government Printing Office, 1989). The report is often referred to as the Skelton Report as Congressman Ike Skelton (D-MO) chaired the Panel on Military Education.

[3] While for simplicity's sake the term *Air Force officers* is used, the residence and distance education programs for the Air Command and Staff College (ACSC) enroll a certain percentage of officers from other Services, international officers, and some Air Force civilian employees.

[4] *Another Crossroads?* vii. Emphasis added.

[5] I. Elaine Allen and Jeff Seaman, *Going the Distance: Online Education in the United States, 2011* (Newburyport, MA: Sloan Consortium, November 2011), 5, available at <http://sloanconsortium.org/publications/survey/going_distance_2011>.

[6] U.S. Department of Education Office of Planning, Evaluation, and Policy Development, *Evaluation of Evidence-Based Practices in Online Learning: A Meta-Analysis and Review of Online Learning Studies* (Washington, DC: Department of Education, September 2010), xviii, available at <www2.ed.gov/rschstat/eval/tech/evidence-based-practices/finalreport.pdf>.

[7] The Skelton Report considered students, faculty, pedagogy, and leadership to be the "bedrock" areas of quality requiring assessment within professional military education (PME). As senior leadership for all ACSC programs is the same and this article has made the case that all officers need quality PME, the assessment here keys on faculty and pedagogy.

[8] *Another Crossroads?* 70.

[9] ACSC Mission Briefing, February 2012.

[10] For details, consult *The Air University Catalog, Academic Year 2011–2012* (Maxwell Air Force Base, AL: Air University, October 2011), available at <www.au.af.mil/au/catalogs.asp>.

[11] *Another Crossroads?* xv.

[12] U.S. Department of Education, xv.

[13] John A. Nagl and Brian M. Burton, eds., *Keeping the Edge: Revitalizing America's Military Officer Corps* (Washington, DC: Center for a New American Security, February 2010), 70.

Joint and Combined Warfighting School students participate in joint exercise at Joint Forces Staff College

JFSC (Susan Milton)

MANAGE OR EDUCATE

Fulfilling the Purpose of Joint Professional Military Education

By VINCENT C. BOWHERS

This disconnect between JPME* [joint professional military education] *and joint duty assignments has become a common practice, disregarding a fundamental purpose of JPME, which by law and policy, is preparation for those assignments.

—U.S. Congress, *Another Crossroads?*[1]

Any educational program that loses sight of its purpose will likely fail to achieve that purpose. This might seem obvious and easy to avoid, but it is exactly how we are falling short in fulfilling the purpose of joint professional military education (JPME). The purpose of JPME is currently seen differently from the officer management perspective than it is from the joint education perspective, and this difference is degrading officer performance on joint staffs and resulting in less than optimal joint operational planning and execution. Without a single clear purpose, JPME requirements are difficult to focus, and the vision of having well-prepared officers performing joint staff and command duties is not being completely fulfilled. The good news is that recovering JPME from this shortfall will not be difficult. We simply need to reestablish a clear purpose, update the requirements to that purpose, and reshape JPME programs based on the results.

Development of the JPME System

Although there were efforts to educate officers from the different Services together before World War II, the original purpose of JPME is frequently traced back to a need identified by General Dwight D. Eisenhower, Admiral Chester W. Nimitz, and General Henry H. Arnold for more inter-Service trust and understanding in the officer corps during World War II. The issue was not that the Allied forces did not succeed in their efforts, but that they could have done a better job if they had more officers who understood the challenges and opportunities of using land, sea, and air forces together in joint operations. Educational programs at the Army-Navy Staff College, National War College, and Armed Forces Staff College were established to bring together officers from all the Services to learn joint perspectives in preparation for joint command and staff duties. The purpose clearly was to prepare officers for service at the joint command and staff levels and thus improve planning and execution of coordinated land, sea, and air operations.

In the 1970s and 1980s, joint operational problems, such as the 1980 failed attempt to rescue American hostages in Iran, led to the establishment of joint officer management (JOM) policies as part of the Goldwater-Nichols Department of Defense Reorganization Act of 1986. Goldwater-Nichols gave specific guidance for preparing joint specialty officers, including the requirement to complete a JPME school followed by a joint duty assignment in order to become joint qualified.[2] The purpose was to provide select officers with *education and experience in joint matters*, defined as "matters relating to the integrated employment of land, sea, and air forces, including . . . (1) national military strategy; (2) strategic planning and contingency planning; and (3) command and control of combat operations under unified command."[3] Goldwater-Nichols linked joint qualification to promotion rates and required joint duty for promotion to flag or general rank. Congress essentially mandated an improvement in joint education and experience, using promotion as the leverage.

In 1987, Representative Les Aspin, Chairman of the House Committee on Armed Services (HASC), appointed the Panel on Military Education to be led by Representative Ike Skelton. The Skelton Panel was charged with reviewing "Department of Defense plans for implementing the joint professional military education requirements of the Goldwater-Nichols Act with a view toward assuring that this education provides the proper linkage between the Service com-

Captain Vincent C. Bowhers, USN, is the Chief of Staff for Commander, Task Force Individual Augmentee, and has served as a faculty member of the Joint Forces Staff College.

petent officer and the competent joint officer." The panel was also instructed to "assess the ability of the Department of Defense military education system to develop professional military strategists, joint warfighters and tacticians" and to report recommendations as appropriate.[4] Again, this HASC chairman's tasking focused the purpose of JPME on joint command and staff competence.

The Skelton Panel made nine key recommendations for significant JPME improvements. In summary, they were:

- establish a professional military education (PME) framework with primary education objectives for flag/general, senior, intermediate, and primary PME levels
- improve the quality of faculty through hiring civilian faculty and assigning high-quality military faculty
- establish a two-phase joint specialty officer education process with Phase I taught at the Service colleges and Phase II taught at the Armed Forces Staff College (now the Joint Forces Staff College
- convert the National War College into a National Center for Strategic Studies, which provides both research and education programs
- make national military strategy the primary focus and increase the Service mix at the senior Service colleges
- implement a substantive Capstone course that includes national security strategy and national military strategy
- determine if Navy military education should include attendance at both intermediate and senior colleges
- establish a Director of Military Education on the Joint Staff
- require an essay-type examination and writing of a paper at intermediate and senior PME schools.[5]

These recommendations were used to design the JPME system we have today.

JPME program guidance is provided by the Chairman of the Joint Chiefs of Staff in the Officer Professional Military Education Policy (OPMEP). The policy calls for five military education levels:

- precommissioning
- primary (O-1 to O-3)
- intermediate (O-4)
- senior (O-5 to O-6)
- general/flag officer.

Chairman addresses graduates at NDU

NDU (Katherine Lewis)

The first two levels have a Service and tactical focus with limited joint exposure. The intermediate level of PME has two phases focused on operational art for the purpose of expanding the understanding of "joint force deployment and employment at the operational and tactical levels of war" as well as "joint and service perspectives."[6] Intermediate-level JPME Phase I (JPME I) is taught via resident and nonresident programs at the Service colleges. Intermediate-level JPME Phase II (JPME II) is taught via a resident program at the Joint and Combined Warfighting School (JCWS) at Joint Forces Staff College (JFSC). There is a similar program available via a blended online and resident delivery for Reserve Component and National Guard officers at the Joint Continuing Distance Education School at JFSC. Senior-level JPME programs are focused on "strategic leadership and advisement," including "national security strategy, theater strategy and campaigning, joint planning processes and systems, and joint, interagency, intergovernmental, and multinational capabilities and integration."[7] Senior-level JPME I is available via nonresident programs offered by the Service colleges, and senior-level JPME II is taught in resident programs at the Service colleges, JCWS, Joint Advanced Warfighting School at JFSC, and the National War College and Dwight D. Eisenhower School for National Security and Resource Strategy (formerly the Industrial College of the Armed Forces) at National Defense University (NDU). The general/flag officer level program is focused on preparing senior officers for "high-level joint, interagency, intergovernmental, and multinational responsibilities"[8] and is taught in the Capstone program at NDU.

The Management-Education Disconnect

So what is the purpose of JPME today? The OPMEP states that it is "designed to fulfill the educational requirements for joint officer management as mandated by the Goldwater-Nichols Act."[9] Goldwater-Nichols and the Skelton Panel report indicate JPME should prepare officers for joint staff and command duty. But when we examine the current practice of sending officers to JPME whenever it fits in their career path, with apparent disregard for providing the education before joint duty, it is clear that the Services feel the purpose is to qualify officers for promotion under JOM policy, not to prepare them for joint duty. The management perspective and the education perspective of the purpose of JPME are disconnected, and this is degrading officer preparation for joint staff and command duties and hurting our overall joint operational performance. This disconnect has resulted in two specific problems that have a negative impact on JOM and JPME: first, officers are not getting the JPME when they need it; and second, JPME programs are being managed to provide throughput in support of promotion eligibility instead of being designed to improve joint duty performance.

The first problem is evident by looking at when in their career paths officers complete JPME II. If the purpose of JPME is to prepare officers for joint staff or command duty, then they should complete the education before they are assigned to a joint position. In reality, over half of the intermediate-level officers serving in joint-designated billets receive their JPME II after at least 1 year in the joint duty assignment, and many of them get the education at the end of or after their joint

tour. JPME II students frequently comment that they wish they had the education before they started their joint tour. Staff officers frequently check into their joint assignment without completing joint education and are tasked with duties that they do not fully understand and are not prepared for.

In the absence of JPME II, new staff officers must learn through on-the-job training (OJT) and rely on assistance from the few educated and experienced staff members who understand joint planning, deployment, and employment. This method of learning joint staff processes and perspectives takes valuable time from the experienced staff and reduces the overall staff effectiveness. Staff officers report that the OJT learning process takes from 7 months to 2 years for an officer to become joint proficient, depending on prior experience and position responsibilities.[10] Then, after a year or two of OJT, when staff officers have learned joint basics the "hard way" and can effectively perform their duties without assistance from more experienced staff officers, they are frequently sent to JCWS for the 10-week JPME II curriculum and become unavailable to do staff work. The one benefit of this timing is that it brings more experience to classroom discussions, but this is outweighed by the overall decline in staff performance in the experienced officer's absence. It becomes obvious that these officers are being sent to the school so they can be fully joint qualified and promoted under Goldwater-Nichols, not because it is preparing them for joint duty.

The second problem caused by a divided understanding of the purpose of JPME is that joint education program decisions are frequently made for the wrong reasons. Without a clear purpose, it is difficult to determine how many officers need the education and what they need to learn. If the purpose of JPME is to prepare officers for joint staff and command duties, then the program throughput, length, and content should be based on the number of joint staff and command positions and the type of duties involved.

Currently, the distribution of student seats for JCWS is based proportionally on the number of joint billets each Service is assigned on the Joint Duty Assignment List (JDAL). JDAL billets are intended to be only those billets that involve significant exposure to joint matters, but research shows that they basically include any O-4 and above billet on a joint staff.[11] Efforts to refine the JDAL to only billets with significant joint exposure are resisted by those who see the purpose of those billets as filling a promotion requirement under Goldwater-Nichols. As a result, there are over 12,000 JDAL billets requiring JPME support. If one assumes an average tour length of 3 years, with some shorter tours being countered by repeat joint tours, the JPME requirement to meet joint assignments is about 4,000 graduates a year. JCWS, the primary source of intermediate-level JPME II graduates, teaches four classes of about 255 students each year. When we subtract the number of international students from the total, JFSC graduates fewer than 1,000 Phase II–educated officers a year. JPME II programs at the Service colleges, National War College, and Eisenhower School graduate about 1,000 additional U.S. military officers a year. This leaves a shortfall of about 2,000 JPME II graduates per year, but it is a shortfall that is based on maximizing Goldwater-Nichols promotion qualifiers, not improving joint staff and command competence. Pressure to meet the excess demand has been driving JPME program changes that are based on the wrong purpose.

For example, one change that resulted from this pressure to increase throughput was the reduction of JCWS from a 12-week to a 10-week curriculum so it could support four classes a year instead of three and meet a quota of about 1,000 graduates. This change increased the throughput, but only the length of the course was reduced, not the educational requirements. As a result, the curriculum was compressed and both student and faculty reading and reflection time was reduced at the same time when the need for critical thinking to address complex problems in the joint operating environment was gaining emphasis. Throughput pressure also led to expanding JPME II certified programs to include resident senior Service schools. Again, this change was made with an eye toward increasing throughput for Goldwater-Nichols promotion eligibility and not because the Service schools had JPME II–equivalent programs. In fact, the student and faculty Service mix requirement at the senior Service colleges is not as joint as the other JPME II schools, limiting the joint experience and exposure to other Service cultures in the classroom.

Throughput pressure is also driving a current proposal to move JPME II toward online education, or a blended online and resident education with a shortened resident portion. This approach needs to be evaluated based on the educational purpose of JPME and not just throughput for promotion under Goldwater-Nichols. Careful consideration is needed to determine if the learning objectives, particularly those in the affective domain dealing with attitudes and values, can be achieved with these delivery methods. It should also be noted that officers surveyed, regardless of rank or age, show a strong preference for classroom education and cite interaction with members of the other Services as the most valuable aspect of JPME.[12] Are the Services willing to invest time toward joint education or are they trying to add this requirement on to the officers' "free" time, lowering the quality of life and learning for officers working long hours and having to study JPME at home? There is also a pilot program to expand JPME II to satellite campuses at locations with concentrations of joint billets. This could improve the chances that staff officers who did not get JPME prior to arrival at their joint duty station could at

Chairman speaks with Joint Staff Army interns and Air Force fellows

U.S. Army (Sun L. Vega)

The NDU Foundation Congratulates the Winners of the 2012 Writing Competitions

Secretary of Defense National Security Essay Competition

In 2012, the 6th annual competition was intended to stimulate new approaches to coordinated civilian and military action from a broad spectrum of civilian and military students. Essays were to address U.S. Government structure, policies, capabilities, resources, and/or practices and to provide creative, feasible ideas on how best to orchestrate the core competencies of our national security institutions. The NDU Foundation awarded the first place winner a generous gift certificate from Amazon.com.

FIRST PLACE
LTC Joseph B. Berger III, USA
National War College
"Covert Action: Title 10, Title 50, and the Chain of Command

SECOND PLACE
Maj Ryan P. Allen, USMC
Marine Command and Staff College
"The 600-Pound Gorilla: Why a Smaller Department of Defense Is in the Best Interest of the United States"

THIRD PLACE
LTC Lawrence T. Brown, USA
U.S. Army War College
"Restoring the 'Unwritten Alliance': Brazil-U.S. Relations"

Chairman of the Joint Chiefs of Staff Strategic Essay Competition

This annual competition, in its 31st year in 2012, challenges students at the Nation's joint professional military education institutions to write research papers or articles about significant aspects of national security strategy to stimulate strategic thinking, promote well-written research, and contribute to a broader security debate among professionals. The first place winners in each category received a generous Amazon.com gift certificate courtesy of the NDU Foundation.

Strategic Research Paper

FIRST PLACE
Lt Col Andrew C. Foltz, USAF
Air War College
"Stuxnet, Schmitt Analysis, and the Cyber 'Use-of-Force' Debate"

SECOND PLACE
Mr. Marc Koehler, Department of State
National War College
"The Effects of 9/11 on China's Strategic Environment: Illusive Gains and Tangible Setbacks"

THIRD PLACE
Maj Eric Dill, USMC
Marine Command and Staff College
"Lashkar-e-Taiba: A Global Threat Today, A Threat to Pakistan Tomorrow"

Strategy Article

FIRST PLACE
Mr. Gregory Macris, Department of State
National War College
"A Focus on Costs, Not Benefits, Dampens Koreans' Desire for Reunification"

SECOND PLACE
Lt Col Houston R. Cantwell, USAF
National War College
"Controversial Contrails: The Costs of Remotely Piloted Foreign Policy"

THIRD PLACE
COL Diana M. Holland, USA
U.S. Army War College
"Democracy Promotion in Oman"

The NDU Foundation is proud to support the annual Secretary of Defense, Chairman of the Joint Chiefs of Staff, and *Joint Force Quarterly* writing competitions. NDU Press hosted the final round of judging on May 15–16, 2012, during which 22 faculty judges from 15 participating professional military education institutions selected the best entries in each category. The First Place winners in each of the three categories are published in the following pages.

Joint Force Quarterly Kiley Awards

Each year, judges select the most influential articles from the previous year's four issues of *JFQ*. Three outstanding articles were singled out for the Kiley Awards, named in honor of Dr. Frederick Kiley, former director, NDU Press:

Best Forum Article
"Whose COIN?"
Amitai Etzioni, The George Washington University

Best Feature Article
"Why Unmanned"
Paul Scharre, Office of the Secretary of Defense

Best Recall Article
"Decisiveness in War"
Colonel Phillip S. Meilinger, U.S. Air Force (Ret.)

Distinguished Judges

Twenty-three senior faculty members from the 15 participating PME institutions took time out of their busy schedules to serve as judges. Their personal dedication and professional excellence ensured a strong and credible competition.

Photo: Tara Parekh

Left to right: Dr. Bill Eliason, Editor, *Joint Force Quarterly*; Dr. Donna Connolly, Naval War College; Dr. Peter Thompson, College of International Security Affairs; CAPT Bill Marlowe, USN (Ret.), Joint Forces Staff College; Professor Douglas Hime, Naval War College; Dr. John M. Schuessler, Air War College; Dr. Nathan W. Toronto, Army Command and General Staff College; CDR Youssef Aboul-Enein, USN, Industrial College of the Armed Forces; Dr. Richard L. DiNardo, Marine Corps Command and Staff College; Dr. James A. Mowbray, Air War College; Lt Col Dennis Adams, USAF, Air Command and Staff College; Dr. Benjamin (Frank) Cooling, Industrial College of the Armed Forces; Dr. Kathleen Mahoney-Norris, Air Command and Staff College; Professor Colton Campbell, National War College; COL Greg Cantwell, USA, U.S. Army War College; Dr. Wray Johnson, Marine Corps School of Advanced Warfighting; Dr. Larry D. Miller, U.S. Army War College; Col John Paul, USAF, Joint Forces Staff College; COL Vince Dreyer, National War College; Professor Charles C. Chadbourn III, Naval War College; and Dr. Nicholas E. Sarantakes, Naval War College

Not shown: Dr. David A. Anderson, Army Command and General Staff College; Dr. James Lacey, Marine Corps War College; and Dr. John Sheldon, School of Advanced Air and Space Studies

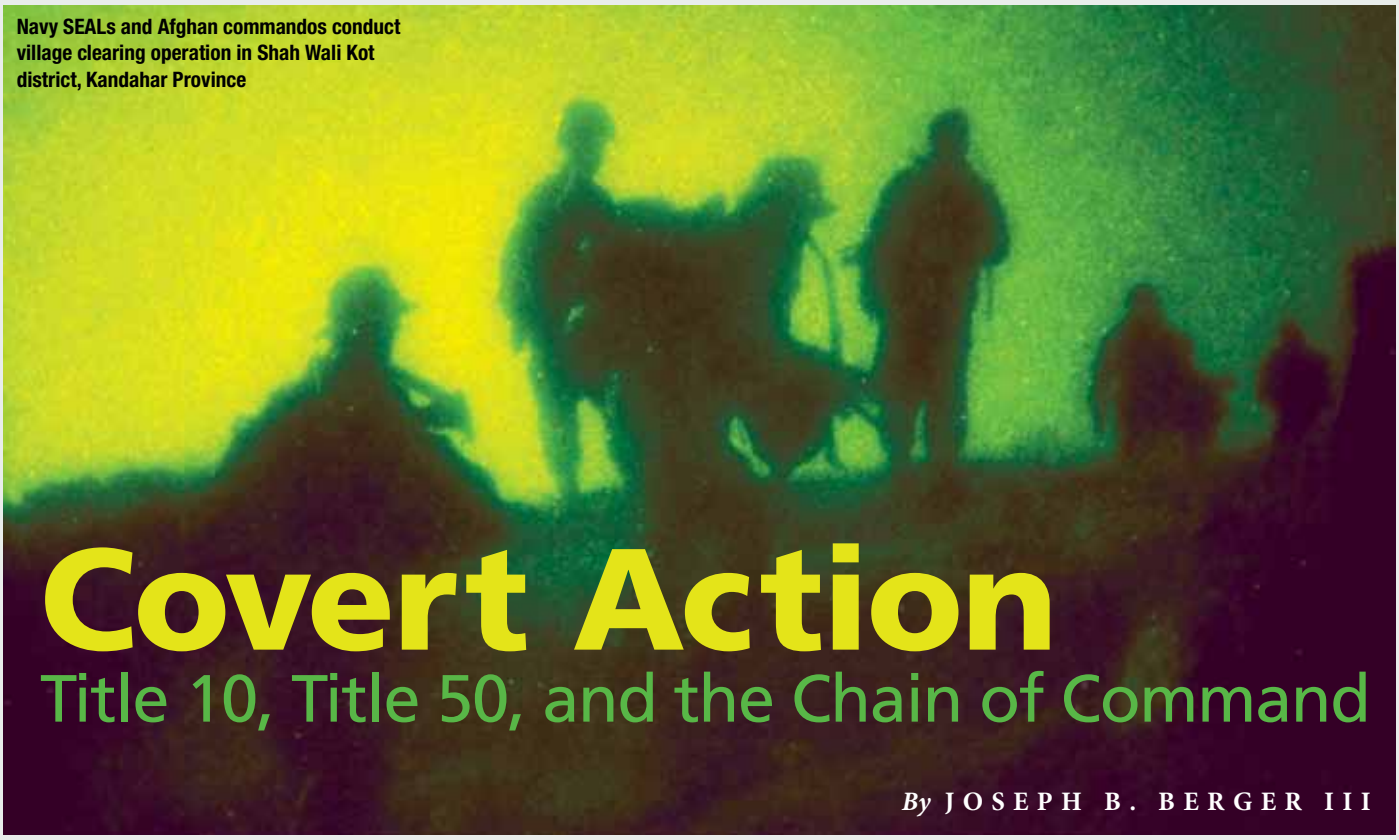
NDU Foundation

The NDU Foundation is a nonprofit 501(c)(3) organization established in 1982 to support and enhance the mission and goals of the National Defense University, America's preeminent institution for military, civilian, and diplomatic national security education, research, outreach, and strategic studies. The Foundation promotes excellence and innovation in education by nurturing high standards of scholarship, leadership, and professionalism. It brings together dedicated individuals, corporations, organizations, and groups that are committed to advancing America's national security and defense capabilities through the National Defense University. The Foundation provides NDU with privately funded resources for:

- Education, Research, Library, and Teaching Activities
- Academic Chairs, Faculty Fellowships, and Student Awards
- Endowments, Honoraria, Seminars, and Conferences
- Multicultural, International, and Inter-agency Programs
- National Security and Homeland Defense Outreach

Keep informed about NDU Foundation activities by visiting online at:

www.nduf.org



Navy SEALs and Afghan commandos conduct village clearing operation in Shah Wali Kot district, Kandahar Province

U.S. Army (Daniel P. Shook)

Covert Action

Title 10, Title 50, and the Chain of Command

By JOSEPH B. BERGER III

Recent media reports have Pentagon officials considering "putting elite special operations troops under CIA [Central Intelligence Agency] control in Afghanistan after 2014, *just as they were during last year's raid on* [Osama bin Laden's] *compound*."[1] This shell game would allow Afghan and U.S. officials to deny the presence of American troops in Afghanistan because once "assigned to CIA control, *even temporarily*, they become spies."[2] Nearly simultaneously, Department of Defense (DOD) leaders were warned to "be vigilant in ensuring military personnel are not inappropriately utilized" in performing "new, expanding, or existing missions," ensuring the force is aligned against strategic choices "supported by rigorous analysis."[3] Placing Servicemembers—uniformed members of the Army, Navy, Marine Corps, and Air Force—under CIA control demands such rigorous analysis. The raid on bin Laden's compound provides a framework.

In his May 1, 2011, televised address, President Barack Obama reported "to the American people and to the world that the United States ha[d] conducted an operation that killed Osama bin Laden."[4] President Obama initially detailed little beyond noting that he had directed "the[n] Director of the CIA [Leon Panetta], to make the killing or capture of bin Laden the top priority of our war against al Qaeda" and that the operation, carried out by a "small team of Americans" was done "at [his] direction [as President]." In the following days, senior executive branch officials garrulously provided explicit details, from the now-iconic White House Situation Room photograph to intricate diagrams of the Abbottabad compound and the assault force's composition. Most noteworthy was Panetta's unequivocal assertion the raid was a covert action:

Since this was what's called a "Title 50" operation, which is a covert operation, and it comes directly from the president of the United States who made the decision to conduct this operation in a covert way, that direction goes to me. And then, I am, you know, the person who then commands the mission. But having said that, I have to tell you that the real commander was Admiral [William] *McRaven because he was on site, and he was actually in charge of the military operation that went in and got bin Laden.*[5]

Despite his self-effacing trumpeting of Vice Admiral McRaven's role, Panetta's comment highlights that critical confusion exists among even the most senior U.S. leaders about the chain of command and the appropriate classification of such operations.

Openly describing the raid as both a "covert operation" and "military operation," Panetta asserted he was the "commander," describing a chain of "command" that went from the President to Panetta to McRaven. Panetta's public comments are problematic, as is describing a chain of command that excludes the Secretary of Defense and purports to route *command* authority through the CIA director. Title 50 is clear:

The term "covert action" means an activity or activities of the United States Government to influence political, economic, or military conditions abroad, where it is intended that the role of the United States Government will

Lieutenant Colonel Joseph B. Berger III, USA, wrote this essay while a student at the National War College. It won the 2012 Secretary of Defense National Security Essay Competition.

not be apparent or acknowledged publicly, but does not include . . . (2) traditional . . . military activities *or routine support to such activities*.[6]

The administration did the opposite, making patently clear the raid's nature and, in exhaustive detail, the precise role of the United States. Instead of categorizing it as a covert action under the director's "command," the President could have conducted the raid as a covert action under the Secretary of Defense instead of the CIA director, or under his own constitutional authority as Commander in Chief and the Secretary's statutory authorities, classifying it as a traditional military activity and excepting it from the statute's coverage. As a traditional military activity, there would have been no legal limits on subsequent public discussion. Alternatively, conducting the raid as a covert action within a *military* chain of command removes the issues the director raised in asserting *command* authority over Servicemembers. The decisionmaking process remains shrouded, but conducting a raid into a sovereign country targeting a nonstate actor using military personnel and equipment under the "command" of the CIA director and classifying it as a covert action raises significant legal and policy questions. Such decisions threaten the legitimacy and moral authority of future U.S. actions and demand a rigorous examination of those associated risks.

The Abbottabad raid illustrates the post-9/11 security environment convergence of DOD military and CIA intelligence operations.[7] While dead terrorists attest to this arrangement's efficacy, many directly challenge the legal and policy framework behind current DOD-CIA cooperation. The discourse focuses largely on distinctions between Title 10 and Title 50 and the legal basis for conducting apparently overlapping military and intelligence operations beyond the battlefields of Iraq and Afghanistan. Notwithstanding the potentially misleadingly simple labels of Title 10 and Title 50, these complex issues lack clear answers. Many argue the legacy structure ill equips the President to effectively combat the threat. But tweaking that structure carries risk. Thus, correctly classifying and structuring our actions within that framework are critical. The law of war is designed to protect our nation's military forces when they are engaged in traditional military activities under a military chain of command; spies conducting intelligence activities under executive authority have no such protections. This distinction rests on a constitutional, statutory, treaty, and doctrinal framework underpinning the military concept of command authority.

U.S. power relies on moral and legal legitimacy. Exclusive state control over the legitimate use of armed force remains viable domestically and internationally *only* where exercised within an accepted framework. Thus, employing DOD forces in a nontraditional manner entails significant risk. The policy implications of classification and structure are neither semantic nor inconsequential, and must be understood by senior decisionmakers; likewise, individual Servicemembers must understand the practical effects. A rigorous risk analysis should therefore inform any deviation, however permissible under domestic law.

This article focuses on the risks associated with both using military personnel to conduct kinetic covert action and using them without a military chain of command. Those risks inform the recommendation to change practice, but not the law. Specifically, the author rejects melding distinct operational military (Title 10) and intelligence (Title 50) authorities into the often mentioned Title 60. Properly classifying actions—either *under* the statute as a covert action or *exempted* from the statute as a traditional military activity—ensures the correct command structure is in place.[8] Ultimately, the analysis argues for revisiting the previously rejected 9/11 Commission recommendation to place paramilitary covert action under DOD control.[9]

U.S. power relies on moral and legal legitimacy

This article first outlines current and likely future threats and then explains the critical terms of art related to covert action and, against that lingua franca, examines why kinetic military operations should be either classified as traditional military activities or kept under a military chain of command. Analyzing the relevant constitutional, statutory, treaty, and doctrinal elements of command, this article illustrates that a raid conducted like the Abbottabad raid, while legally permissible, is best conducted as a traditional military activity.

Changed Character of the Battlefield and Enemy

In the decade since 9/11, DOD and CIA elements have become "operationally synthesi[zed]."[10] A senior intelligence official recently noted that "the two proud groups of American secret warriors had been 'deconflicted and basically integrated'—finally—10 years after 9/11."[11] The direct outgrowth is the increased reliance on special operations forces (SOF) to achieve national objectives against a "nimble and determined" enemy who "cannot be underestimated."[12] While the United States fought wars on geographically defined battlefields in Iraq and Afghanistan and beyond, the underlying legal structure remained constant. In the wars' background, leaders, advisors, academics, and others argued about the structure of the appropriate legal and policy framework. Post-Iraq and post-Afghanistan, the United States must still address other threats, including those that al Qaeda and their associated forces present.

The threats have migrated beyond a battlefield defined by sovereign nations' borders. When asked recently in "how many countries we are currently engaged in a shooting war," Secretary of Defense Panetta laughed, responding, "That's a good question. I have to stop and think about that . . . we're going after al Qaeda wherever they're at. . . clearly, we're confronting al Qaeda in Pakistan, Yemen, Somalia, [and] North Africa."[13] The unresolved legal and policy challenges will likely increase in complexity on this geographically unconstrained battlefield. Remaining rooted in enduring principles is critical. DOD conduct of kinetic operations beyond traditionally recognized battlefields raises significant legal and policy concerns, especially where the U.S. Government conducts them without knowledge or consent of the host nation, as apparently happened with the Abbottabad operation.[14] Properly categorizing and structuring these operations, while vexing for policymakers and their lawyers, carries much greater stakes for the Servicemembers executing them.

The Need for a Lingua Franca

Colloquial usage refers to DOD authorities as Title 10, and the CIA's as Title 50. That is technically inaccurate and misleading since DOD routinely operates under *both* Titles 10 and 50.[15] Instead of Title 10, this article uses the term *military operations*; instead of Title 50, it uses *CIA operations* or the more

President delivers statement on successful special operations raid on Osama bin Laden compound in Pakistan

White House (Pete Souza)

specific *covert action*. All three terms require clarification.

CIA operations are all CIA activities except covert action. Covert action is the narrow, statutory subset of Presidentially approved, CIA-led activities.[16] Unfortunately, colloquially, covert action "is frequently used to describe *any* activity the government wants concealed from the public."[17] That common usage ignores the fact that a traditional military activity, notwithstanding how "secretly" it is executed, is by statute *not* a covert action. DOD defines a *covert operation* as one "planned and executed as to conceal the identity of or permit plausible denial by the sponsor," where "emphasis is placed on concealment of the identity of the sponsor rather than on concealment of the operation."[18] While not in conflict with the statutory definition, the DOD definition is incomplete; it fails to recognize the President's role and ignores the exception of traditional military activities.[19] Practitioners should use the statutory definition.

The concept of clandestine operations further blurs colloquial and doctrinal imprecision.[20] DOD activities "may be both covert and clandestine . . . focus[ing] equally on operational considerations and intelligence-related activities."[21] Appropriately, DOD officials assert that, absent a Presidential covert action finding, they "conduct only 'clandestine activities.'" [22] They characterize *clandestine activities* as those "conducted in secret but which constitute 'passive' intelligence information gathering."[23] Interchanging the terms and mixing them with intelligence functions is inaccurate and dangerous; practitioners must draw clear distinctions. The sponsorship of a covert action is hidden, not the act itself. The specific acts of the U.S. Government in influencing a foreign election (for example, posters, marches, election results, and so forth) would be visible, but not the covert sponsorship of those acts. For clandestine acts, the act itself (for example, intercepting a phone call) must remain hidden. The CIA and DOD can conduct clandestine operations without Presidential approval, whereas covert action triggers statutory requirements for a Presidential finding and congressional notification. Some have argued DOD's "activities should be limited to clandestine" activities, as this would ensure military personnel are protected by the law of war,[24] a critical point examined in detail later.

Military operations are DOD activities conducted under Title 10, including activities intended or likely to involve kinetic action. Pursuant to an order issued by the Secretary of Defense, they are conducted by military personnel under DOD command and in accordance with the law of war. They specifically exclude DOD's intelligence activities (for example, the Joint Military Intelligence Program); like the CIA's, those intelligence activities are conducted pursuant to Title 50.

Statutorily assigned responsibility helps distinguish between CIA operations and military operations. Although the President can designate which department, agency, or entity of the U.S. Government will *participate* in the covert action, the statute implicitly tasks the CIA as the default *lead* agency: "Any employee . . . of the [U.S.] Government other than the [CIA] directed to participate in any way in a covert action shall be subject either to the policies and regulations of the [CIA], or to

written policies or regulations adopted . . . to govern such participation.[25]

Executive order 12333 (EO 12333) makes that default tasking explicit:

The Director of the [CIA] *shall . . . conduct covert action activities approved by the President. No agency* except the [CIA] *(or the Armed Forces of the United States in time of war declared by the Congress or during any period covered by a report from the President to the Congress consistent with the War Powers Resolution. . . .) may conduct any covert action activity unless the President determines that another agency is more likely to achieve a particular objective.*[26]

The statute, coupled with EO 12333, unequivocally places all covert action squarely under the CIA's control; the narrow exception for DOD is currently inapplicable. While the Executive order expressly tasks the director with conducting covert action, it does not task the Secretary of Defense.[27] Default CIA primacy and the absence of statutory specificity in defining traditional military activities create risk when DOD conducts kinetic covert action.

The Unique Nature of Traditional Military Activities

One practitioner described traditional military activities' exclusion from covert action's definition as "the exception that swallows the rule."[28] But while DOD-CIA operational convergence blurs the issue, the exception need not swallow the rule. Functionally, anything done by a uniformed member of a nation's armed forces is a "military" activity; the nuanced requirement is to understand which are *traditional* military activities. That definition can be consequential, functional, or historical—or a combination of some or all three approaches. The statute's legislative history provides the best clarification, noting the conferees intended that:

"Traditional military activities" include activities by military personnel under the direction and control of a United States military commander *(whether or not the U.S. sponsorship of such activities is apparent or later to be acknowledged) . . . where the fact of the U.S. role in the overall operation is apparent or to be acknowledged publicly.* In this regard, the conferees intend to draw a line between activities that are and are not under the direction and control of the military commander. Activities that are not under the direction and control of a military commander should not be considered as "traditional military activities."[29]

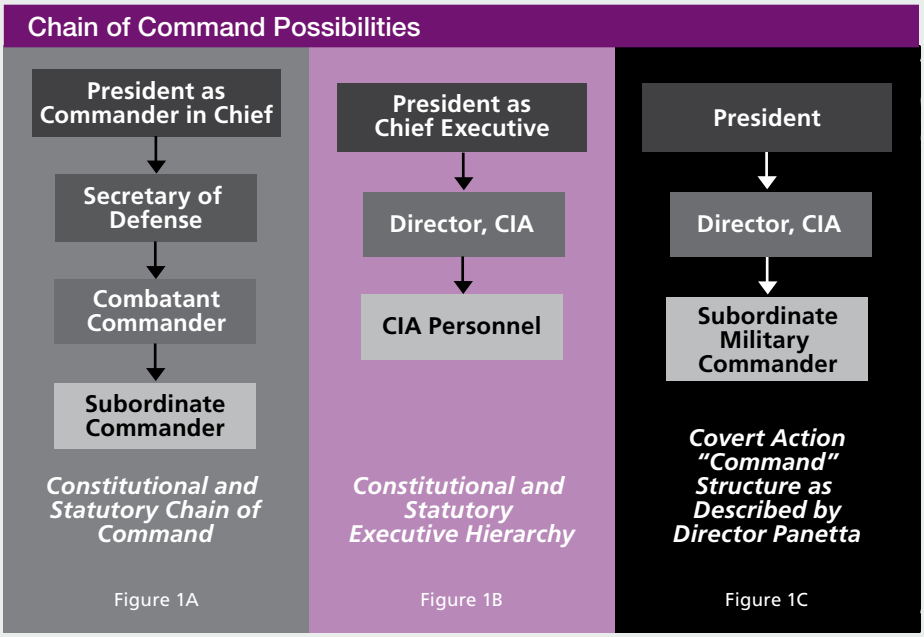
That nonstatutory definition frames the follow-on analysis. That functional and historical definition turns on who is in charge.

Activities under the "direction and control of a military commander" meet the requirement to be excepted from the statute; those with a different command and control arrangement are *not* traditional military activities. "Command" is unique to the military and the definition appears to draw a bright line rule; but the CIA director blurred the line by asserting "command" over a DOD element.[30] The confusion questions the necessary nature and scope of leadership by a "military commander." What level or rank of command is required? Must the chain of command from that military commander run *directly* back to the Commander in Chief *solely* through military channels? *Must* it run through the Secretary of Defense? *Can* it run through the director if there is a military commander below him? Given Goldwater-Nichols,[31] what about the geographic combatant commander? In short, what does the wiring diagram look like? These questions highlight three baseline possibilities as depicted in the figure below.

Part 1A of the figure reflects DOD's Title 10 chain of command, illustrating the broadest historical, functional, and consequential definition of traditional military activity. The clear chain is rooted in the uniquely military concept of *command* and the President's constitutionally defined role as Commander in Chief. It clarifies congressional oversight responsibility, results in unquestioned jurisdiction, and forms the basis of the strongest legal argument for combatant immunity. Part 1B represents the President as chief executive, exercising oversight and control of the CIA under Title 50. This hierarchy lacks the legal command authority exercised over military personnel in 1A. Finally, part 1C represents the paradox created by the covert action statute's attempts to overlap the parallel structures of 1A and 1B; it is often described as Title 60.

The current Congressional Authorization for the Use of Military Force allows the President to "use all necessary and appropriate force" to prevent "future acts of international terrorism against the United States."[32] This statutory grant of power creates the paradox: here, where the Senate vote was 98 to 0 and the House vote was 420 to 1, the President's executive authority (as Commander in Chief *and* chief executive) is greatest,[33] the exercise of those powers blurs the clear lines of parts 1A and 1B of the illustration. Merging the two, although permissible under the covert action statute, creates risk.

Consequently, questions about the nature and structure of the chain of command demand rigorous scrutiny and cannot be left to ad hoc arrangements. Defining military command determines whether or not the activity is a traditional military activity *and* therefore not under the



ambit of the statute. The criticality of this categorization is twofold: it is the core of the state's monopoly on the legitimate use of force and cloaks Servicemembers in the legal armor of combatant immunity.

Chain of Command, or Control?

Since George Washington's Presidency, the Secretary of War (later Defense) has served without interruption as a Cabinet member. The President's role, enshrined in the Constitution, is clear: "The President shall be Commander-in-Chief of the Army and Navy of the United States."[34] With the Secretary of Defense, this embodies the Founders' vision of civilian control of the military. The Secretary of Defense's appointment requires the "Advice and Consent of the Senate."[35] While the President *can relieve* him and replace him with an inferior officer (that is, the Deputy Secretary of Defense), Senate-confirmed executive branch officials are not fungible. He *cannot interchange* officials individually confirmed to fulfill separate and unique duties—something James Madison warned about in *Federalist 51*.[36]

Longstanding U.S. practice is an unbroken chain of command from the President, through his Secretary of Defense, to a subordinate uniformed commander. Even Goldwater-Nichols's[37] streamlining the military warfighting chain of command to run from the President through the Secretary and directly to the unified combatant commanders did not alter that fundamental practice.[38] Combatant commanders simply replace Service chiefs. The civilian leader *between* the Commander in Chief and his senior uniformed commander remains unchanged—a specific individual confirmed by the Senate to execute statutory duties. The inviolate concept of civilian control of the military and the Senate's Advice and Consent requirement make assertion of any executive authority to "trade out" duties between Cabinet officials implausible. The President can place military personnel under CIA *control*, but *control* is not *command*.

Command is the inherently military "privilege" that is "exercised by virtue of office and the special assignment of members of the US Armed Forces holding military grade."[39] In fact, under the Army regulation, "A civilian, other than the President as Commander-in-Chief . . . may *not* exercise command."[40] Goldwater-Nichols allows the President to exercise command through his Secretary of Defense. Command rests on constitutional and statutory authority (including the Uniform Code of Military Justice) and the customs and practices of the Service. Removing military personnel from that hierarchy—illustrated in part 1C of the figure—changes their fundamental nature. This is Panetta's assertion: he was in "command" [41] of the raid on Osama bin Laden's compound.

Titles 10 and 50 define the specific duties of the Secretary of Defense[42] and Title 50 the CIA director's.[43] The duties are neither identical nor interchangeable. In Title 50, Congress explicitly states that DOD shall function "under the direction, authority, and control of the Secretary of Defense" in order to "provide for their unified direction under civilian control."[44] Placing the Services under the Secretary of Defense is necessary to "provide for the establishment of [a] clear and direct line of *command*."[45] Congress is equally clear in Title 10, granting the Secretary complete authority over DOD: "there shall be a Secretary of Defense, who is the head of the [Department], appointed . . . by the President, by and with the advice and consent of the Senate."[46] The statute allows the Secretary to "perform any of his functions or duties, or [to] exercise any of his powers through" other persons, but only persons from within DOD.[47]

Goldwater-Nichols codifies geographic combatant commanders' nearly inviolable command authority

Two caveats exist to the Secretary of Defense's "authority, direction, and control": the Secretary's authority is "subject to the direction of the President" and the 1947 National Security Act.[48] The latter covers DOD personnel within the National Foreign Intelligence Program (NFIP). The former appears to be an exception that swallows the rule. But even in empowering the President to limit his Secretary's authority, Congress did not specifically authorize any change to the fundamental *command* of military forces. Likewise, in defining the director's *limited* authorities over military personnel, Congress maintained the *military command* structure over military operations.

Congress neither allows the director command nor control of DOD operational assets, nor did it grant the President a caveat like that with the Secretary of Defense's authority.[49] Although the director's duties include the transfer of "personnel within the NFIP," which includes DOD personnel, such transfers are limited to personnel within DOD's Joint Military Intelligence Program (JMIP).[50] SOF are not part of the JMIP. When DOD does transfer *any* JMIP personnel to the CIA, the director must "promptly" report that transfer to both the intelligence oversight and Armed Services Committees of both houses.[51] Transfers between other executive branch elements trigger no such requirements. Congress only intended CIA control over DOD *intelligence* assets and was clearly concerned about even that. Goldwater-Nichols reinforces this analysis.

Goldwater-Nichols codifies geographic combatant commanders' nearly inviolable *command* authority: "*all* forces operating within the geographic area assigned to a unified combatant command *shall* be assigned to, *and under*" his command.[52] Two exceptions supplant that authority. Servicemembers assigned to U.S. Embassies (for example, the Defense Attaché) are under the Ambassador's *control* and the Defense Intelligence Agency's *command*. For those Servicemembers, diplomatic protections have replaced law of war protections, but the Secretary of Defense remains in the chain of command. The second exception, carved from Goldwater-Nichols's "unless otherwise directed by the President" language, covers DOD participation in covert action.[53] Goldwater-Nichols's silence on the Secretary of Defense remaining in the chain of command indicates Congress did not intend to change the default hierarchy. DOD recognized that point by defining *combatant command* as being "under a single commander" and running "*through the Secretary of Defense*."[54] All these say nothing about covert action.

The statute and EO 12333 put the director "in charge" of the conduct of covert actions.[55] CIA "ownership" means any non-CIA employee supporting a covert action "belongs" to the CIA. However, the CIA lacks DOD's legal command structure and no CIA official possesses the *command* authority inherent in an officer's commission.[56] The CIA can only be in charge, not in command. The director cannot give a lawful *order* that would be legally binding on Servicemembers. The Constitution unequivocally grants Congress the authority to "make Rules for

Special operations forces use fast-rope insertion technique during assault and secure building training

U.S. Army (Jason Cauley)

the Government and Regulation of the land and naval Forces."[57] Those rules, the Uniform Code of Military Justice, never contemplated CIA personnel exercising command authority over Servicemembers. The CIA's ownership of covert action is limited. Exclusive CIA control fails elsewhere; the statute authorizes the President to task "departments, agencies, or entities"[58] to conduct covert action. The implication is that DOD can conduct a covert action exclusively. EO 12333 specifically envisions that.[59] Placing DOD elements under CIA control to conduct a kinetic operation is arguably unnecessary.

This chain of command is constitutionally enshrined, codified, and ratified through longstanding practice; even if Congress had explicitly authorized the President to reroute it, doing so creates risk. First, it removes the law of war's protections upon which Servicemembers conducting kinetic operations rely. In such an event, Servicemembers must be made aware they are no longer protected. Second, as a state practice, realigning military personnel under a nonmilitary framework to conduct kinetic activities creates precedential risk for U.S. allies. Such a decision must be fully informed at all levels.

Chain of Command: International Law Context

National armies engaged against each other have, throughout modern history, been cloaked in the law of war's combatant immunity. Absent that immunity, a captured individual is subject to *criminal* prosecution for his wartime conduct. His deliberately targeting and killing others become nonmilitary and therefore criminal. In World War II's aftermath, widespread acceptance of what constituted an "army" rendered a definition unnecessary: "Individuals composing the national forces" automatically enjoyed combatant immunity.[60] However, for those *outside* their nation's military hierarchy, specificity was necessary. The Third Geneva Convention grants prisoner of war status—which confers combatant immunity—to those who are subordinate to a responsible *commander*, wear a fixed, distinctive insignia recognizable at a distance, carry their arms openly, and conduct their operations in accordance with the laws and customs of war.[61]

The command requirement stems from the "dual principle of responsible command and its corollary command responsibility."[62] The Hague Convention required that a commander be "responsible for his subordinates."[63] The Geneva Convention recognized "*no* part of [an] army . . . is not subordinated to a *military commander*," applying this "from the Commander-in-Chief down to the common soldier."[64] The later protocols "could not conceive" of a hierarchy "without the persons who make up the command structure being familiar with the law applicable in armed conflict."[65] This is DOD's unchallenged area of expertise.[66] Like Congress's definition of traditional military activity,[67] the commentary's definition, when coupled with the requirements for those *not* considered part of the Nation's army, is the parallel to Servicemembers conducting kinetic covert action under CIA control. Combatant immunity necessitates prisoner of war status; for those not acting as part of the army, that status requires a *military* chain of command. Replacing the Secretary of Defense with the CIA director eviscerates this.

U.S. history records a fundamental belief in the rules for combatant immunity.[68] First, to codify these requirements, the 1863 Lieber Code defined *prisoner of war* as including "all soldiers."[69] The code noted noncompliance with the rules meant no combatant immunity: spies were "punishable with death by hanging by the neck."[70] "Armed prowlers . . . who steal within the lines of the hostile army for the purpose of . . . killing . . . are not entitled to the privileges of the prisoner of war."[71] The code's noteworthy purpose was *not* to regulate conduct *between* nations, but for application in a non-international armed conflict and maintaining the moral high ground necessary to facilitate reconciliation with and reintegration of the confederate states.

The law of war's efficacy rests on the principle of reciprocity. One party provides the protections to its prisoners believing and hoping its enemies will respond in kind. Commendable German and U.S. treatment of each other's prisoners during World War II exemplifies this principle; Japanese treatment of U.S prisoners at Bataan proves its imperfections. Regardless, maintaining the moral

Special Operations Task Force West Marines investigate Taliban presence in Zanghlav, Herat Province

U.S. Army (Kimberly K. Fritz)

high ground is critical. Had Abbottabad gone poorly, the United States would have asserted that U.S. personnel in Pakistani custody were entitled to the high standards of prisoner of war treatment. That would have required those Soldiers and Sailors to be in compliance with the law of war. The nonmilitary chain of command may have been problematic in making that assertion.

Conclusion

"From its inception . . . America has venerated the rule of law."[72] Traditional military activities occur against a rich fabric of domestic and international law. Covert action, while uniquely codified, presents multiple dilemmas. Although permissible under U.S. domestic law, covert action is generally illegal in the target country.[73] Again, maintaining the moral high ground is critical.

Although inimical to covert action's fundamental premise, overt executive branch commentary following the Abbottabad raid highlighted the legal risk associated with policy decisions. Placing Servicemembers under CIA command threatens to undermine the protections they rely on when conducting kinetic military operations, especially where the activity is more accurately classified as a traditional military activity.

The risk can—and should—be mitigated by first properly classifying the activity. Classifying a traditional military activity as anything else undermines the very categorization and its inherent law of war protections. DOD can undoubtedly conduct secretive (that is, clandestine and/or unacknowledged) actions as traditional military activities and enjoy the full body of the law of war's protections. The current framework neither envisions nor facilitates placing Servicemembers under CIA control and preserving the command relationships necessary to cloak them in combatant immunity. The Abbottabad raid utilized this risk-laden approach.

This is not to assert that conducting the raid as a covert action was illegal. There were three likely outcomes: success, failure, or something in between (that is, aborting the mission). Neither success nor failure required covert action's plausible deniability. The United States immediately publicly acknowledged killing of "public enemy number one"; regardless, the crashed helicopter disclosed the U.S. role. A noncatastrophic driven decision to abort (for example, Pakistani detection of violation of their sovereign airspace) provides the sole outcome where the United States would likely have hidden behind the statute's shield, disavowing all. The covert action classification provided an insurance policy, yet the cost of allowing that policy to "lapse" through post-success disclosures undermines the plausibility of such "insurance" in the future.

Compare the Abbottabad covert action with the recent rescue of a U.S. citizen in Somalia, conducted secretively, but not covertly, by "a small number of joint combat-equipped U.S. forces."[74] This comparison illustrates that such activities can be conducted as traditional military activities, maintaining secrecy and preserving individual Servicemember protections. The need for continued distinction between covert action and traditional military activities and, where covert, the need for DOD-conducted operations to maintain a military chain of command, drive these recommendations. The United States should revisit the rejection of the 9/11 Commission's recommendation that DOD assume responsibility for paramilitary covert operations.[75]

Where DOD participation is necessary and primary, the operation should be conducted as an unacknowledged traditional military activity. If the risk analysis drives a decision to conduct the operation as a covert action, the President should maintain the military chain of command. This ensures Servicemembers going in harm's way have *every* protection the Nation they serve can provide them—or a clearer understanding of the additional risks they are assuming on behalf of their Nation. **JFQ**

NOTES

[1] Kimberly Dozier, "AP Sources: CIA-Led Force May Speed Afghan Exit," *ABC News Online*, March 3, 2012, available at <http://abcnews.go.com/Politics/wireStory/ap-sources-cia-led-force-speed-afghan-exit-15840357>. Emphasis added.

[2] Ibid. Emphasis added.

[3] Memorandum from Acting Under Secretary of Defense for Personnel and Readiness for Secretaries of the Military Departments et al., SUBJECT: Guidance related to Utilization of Military Manpower to Perform Certain Functions, March 2, 2012.

[4] Remarks by President Barack Obama, delivered from the East Room of the White House, May 1, 2001, available at <www.whitehouse.gov/blog/2011/05/02/osama-bin-laden-dead>.

[5] Interview of Leon Panetta by Jim Lehrer on *PBS Newshour*, "CIA Chief Panetta: Obama Made 'Gutsy' Decision on Bin Laden Raid," May 3, 2011, video of interview available at <www.pbs.org/newshour/bb/ terrorism/jan-june11/panetta_05-03.html>.

[6] 50 U.S.C. §413b(e). Emphasis added.

[7] Jeff Mustin and Harvey Rishikof, "Projecting Force in the 21st Century—Legitimacy and the Rule of Law: Title 50, Title 10, Title 18, and Art. 75," *Rutgers Law Review*, vol. 63 (Summer 2011), 1235.

[8] 50 U.S.C. §413b(e)(2).

[9] National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report*, July 2004, 415, available at <www.9-11commission.gov/report/911Report.pdf>. See also Richard A. Best, Jr., *Covert Action: Legislative Background and Possible Policy Questions* (Washington,

DC: Congressional Research Service, 2011), available at <www.fas.org/sgp/crs/intel/ RL33715.pdf>.

[10] Mustin and Rishikof, 1236.

[11] Mark Ambinder, "The Secret Team That Killed bin Laden," *National Journal Online*, May 3, 2011, available at <http://nationaljournal.com/whitehouse/the-secret-team-that-killed-bin-lawden-20110502>.

[12] Remarks as prepared for delivery by Attorney General Eric Holder at Northwestern University School of Law, March 5, 2012, available at <www.justice.gov/iso/opa/ag/speeches/2012/ag-speech-1203051.html>.

[13] Interview of Leon Panetta by Scott Pelley, *60 Minutes*, January 29, 2012, available at <www.cbsnews.com/video/watch/?id=7396828n&tag=contentMain;contentAux>.

[14] See, for example, Adam Levin, "Bin Laden raid was humiliating to Pakistanis, Gates and Mullen say," *CNN Online*, May 18, 2011, available at <http://articles.cnn.com/2011-05-18/us/pakistan.bin.laden_1_gates-and-mullen-bin-pakistanis?_s=PM:US>.

[15] See generally Andru E. Wall, "Demystifying the Title 10-Title 50 Debate: Distinguishing Military Operations, Intelligence Activities, and Covert Action," *Harvard National Security Journal* 85, no. 3 (2011).

[16] 50 U.S.C. §413b(e).

[17] Mustin and Rishikof, 1240.

[18] Joint Publication (JP) 1-02, *Department of Defense Dictionary of Military and Associated Terms* (Washington, DC: The Joint Staff, November 8, 2010, as amended through November 15, 2011), 81, available at <www.dtic.mil/doctrine/ new_pubs/jp1_02.pdf>.

[19] For a more thorough discussion of what have been categorized as "unacknowledged special operations," see Richard C. Gross, "Different Worlds: Unacknowledged Special Operations and Covert Action," unpublished monograph, U.S. Army War College, 2009.

[20] See Greg Miller, "CIA Is in Baghdad, Kabul for Long Haul: Large Covert Presence Part of U.S. Plan to Exert Power More Surgically," *The Washington Post*, February 8, 2012, A1.

[21] JP 1-02, 53.

[22] 50 U.S.C. §413b(a)(1) through (5) for the requirements for Presidential findings.

[23] Best.

[24] Ibid. See also William Safire, "Covert Operation, or Clandestine?" *The New York Times*, February 14, 2005, available at <www.nytimes.com/2005/02/13/arts/13iht-saf14.html>.

[25] 50 U.S.C. §413b(a). Emphasis added.

[26] Executive order 12333, *United States Intelligence Activities* (As amended by Executive Orders 13284 [2003], 13355 [2004], and 13470 [2008]), para. 1.7(a)(4), available at <www.fas.org/irp/offdocs/eo/eo-12333-2008.pdf>. Emphasis added.

[27] Ibid., para 1.10(a) through (l).

[28] Gross, 7.

[29] H.R. Rep. No. 102-115, at 5898 (1991) (Conf. Rep.). Emphasis added.

[30] Panetta interview by Lehrer.

[31] The Goldwater-Nichols Department of Defense Reorganization Act of 1986 (P.L. 99-433; 100 Stat. 992), October 1, 1986.

[32] P.L. 107-40 [S. J. RES. 23, 107th Congress], September 18, 2001. The act authorized the President "to use all necessary and appropriate force against those nations, organizations, or persons he determines planned, authorized, committed, or aided the terrorist attacks that occurred on September 11, 2001, or harbored such organizations or persons, in order to prevent any future acts of international terrorism against the United States by such nations, organizations, or persons."

[33] See *Youngstown Sheet & Tube Co. v. Sawyer*, 343 U.S. 579 (1952).

[34] U.S. Constitution, Article 2.

[35] Ibid.

[36] *The Federalist Papers, No. 51* (James Madison arguing for the need for established institutions vice reliance on the good will of incumbent leaders).

[37] Goldwater-Nichols, note 32.

[38] 10 U.S.C. §162, and the following.

[39] See, for example, Department of the Army Regulation 600-20, *Army Command Policy*, March 18, 2008, para. 1-5(a), 1.

[40] Ibid.

[41] Panetta interview by Lehrer; see also figure 1C.

[42] 10 U.S.C. §113 and 50 U.S.C. §403-5 (defining the Secretary's specific duties with respect to the National Foreign Intelligence Program).

[43] 50 U.S.C. §403-4.

[44] 50 U.S.C. §401.

[45] Ibid. Emphasis added.

[46] 10 U.S.C. §113(a).

[47] 10 U.S.C. §113(d).

[48] 10 U.S.C. §113(b).

[49] "Authorities of the Director of Central Intelligence," 50 U.S.C. §403, and the following.

[50] Ibid.

[51] 50 U.S.C. §403(d)(5).

[52] 10 U.S.C. §162(a), and the following.

[53] 10 U.S.C. §162, and the following.

[54] JP 1-02, 57. Emphasis added.

[55] Executive order 12333; see also 50 U.S.C. §413(b)(a)(3).

[56] 5 U.S.C. § 3331.

[57] U.S. Constitution, Article 1, sec. 8.

[58] 50 U.S.C. §413(b).

[59] Executive order 12333.

[60] See, for example, Herbert C. Fooks, *Prisoners of War* (Federalsburg, MD: J.W. Stowell Printing, 1924), 25. See also Geneva Convention Relative to the Treatment of Prisoners of War, August 12, 1949, 6 U.S.T. 3316, 75 U.N.T.S. 135, art. 4.A.(3).

[61] Ibid., art. 4 (A)(2)(a)-(d). Emphasis added.

[62] Elihu Lauterpacht et al., *International Law Reports*, 133 (Cambridge; Cambridge University Press, 2008), 62.

[63] Regulations Respecting the Laws and Customs of War on Land, annex to Convention (no. IV) Respecting the Laws and Customs of War on Land, October 18, 1907, art. 1, 36 Stat. 2277.

[64] Yves Sandoz, Christophe Swinarki, and Bruno Zimmerman, eds., *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949* (Geneva: Martinus Nijhoff Publishers, 1987), para. 3553. Emphasis added.

[65] Ibid., art. 43, para. 1672.

[66] See, for example, Protocol additional to the Geneva Conventions of August 12, 1949, and relating to the protection of victims of international armed conflicts (Protocol I) Art. 82, June 10, 1977, 1125 U.N.T.S. 3; see also *Commentary on the Additional Protocols*, art. 82, paras. 3340–3345.

[67] H.R. Rep. No. 102-115.

[68] Statement of Hon. Wilber M. Brucker, General Counsel, Department of Defense, *Hearing before the Committee on Foreign Relations, United States Senate*, 84th Cong., 1st sess. Brucker notes during 1955 hearing on the Geneva Conventions before the Senate Committee on Foreign Relations that the U.S. "Armed Forces have always attempted to comply scrupulously" with these laws of armed conflict and their underlying principles.

[69] General Orders Number 100, *Instructions for the Government of the Armies of the United States in the Field*, April 1863, arts. 48–80, available at <http://avalon.law.yale.edu/19th_ century/lieber.asp>. Emphasis added.

[70] Ibid., art. 88.

[71] Ibid., art. 84.

[72] United States War Department, *The 1863 Laws of War* (Mechanicsburg, PA: Stackpole, 2005), xi.

[73] See, for example, Richard A. Clarke, *Against All Enemies: Inside America's War on Terror* (New York: Free Press, 2004), quoting former Vice President Al Gore: "Of course it's a violation of international law, that's why it's a *covert* action."

[74] Letter from President Barack Obama to Hon. John Boehner, Speaker of the House of Representatives, entitled "Notification of Special Forces Operation" (Washington, DC: Government Printing Office, 2012). The President noted the letter was sent "consistent with the War Powers Resolution." See 50 U.S.C. §1541, and following (P.L. 93-148).

[75] See, for example, Richard A. Best, Jr., and Andrew Feickert, *Special Operations Forces (SOF) and CIA Paramilitary Operations: Issues for Congress* (Washington, DC: Congressional Research Service, updated 2006).

Members of International Telecommunications Union and UN Institute for Training and Research confer on cyber security

UN (Jean-Marc Ferré)

Stuxnet, Schmitt Analysis, and the Cyber "Use-of-Force" Debate

By ANDREW C. FOLTZ

All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations.

—Article 2(4), Charter of the United Nations[1]

One of the many seemingly intractable legal issues surrounding cyberspace involves whether and when peacetime cyber operations constitute a prohibited use of force under Article 2(4) of the United Nations (UN) Charter. Notwithstanding a significant body of scholarly work on this topic and extensive real-world examples from which to draw, there is no internationally recognized definition of a use of force.[2] Rather, what has emerged is a general consensus that *some* cyber operations will constitute a use of force, but that it may not be possible to identify in advance the specific criteria states will use in making such determinations.

As discussed in this article, several analytic frameworks have been developed to help assess when cyber operations constitute a use of force.[3] One conclusion these frameworks share is that cyber operations resulting in physical damage or injury will almost always be regarded as a use of force. When these frameworks were developed, however, there were few, if any, examples of peacetime, state-sponsored cyber coercion. More importantly, the prospect of cyber attacks causing physical damage was largely theoretical.[4] Beginning

Lieutenant Colonel Andrew C. Foltz, USAF, wrote this essay while a student at the Air War College. It won the Strategic Research Paper category of the 2012 Chairman of the Joint Chiefs of Staff Strategic Essay Competition.

in 2007, however, a string of cyber operations—including the 2007 Distributed Denial of Service (DDoS) attack on Estonia, the 2008 DDoS attack on Georgia, and the 2008 discovery that the U.S. Government's most sensitive networks had been compromised—hinted at increased use of the cyber domain by states and their proxies for peacetime coercion. Then, with the discovery of the Stuxnet worm in 2010, which damaged uranium enrichment equipment at a nuclear facility in Iran, theory became reality.

Although Stuxnet has been described as a watershed event, there has been little academic discussion on whether it constituted a use of force.[5] Perhaps this is because it caused physical damage and, therefore, clearly constitutes a use of force under prevailing analytic frameworks. This appears to be the emerging consensus.[6] Although I generally agree with this conclusion, I also believe that by looking beyond the physical damage, Stuxnet provides a unique opportunity to assess the adequacy and continued relevancy of these frameworks.

As a first step toward such an assessment, this article tests one of the more robust frameworks, known as the Schmitt Analysis, by applying it to Stuxnet. Developed in 1999 by Professor Michael Schmitt, it is one of the most academically rigorous and frequently cited frameworks for characterizing cyber operations. The Schmitt Analysis consists of seven factors that states are likely to consider when characterizing cyber activities: severity, immediacy, directness, invasiveness, measurability, presumptive legitimacy, and responsibility. A key feature of the framework is that it remains faithful to Article 2(4) of the UN Charter while at the same time effectively bridging key elements of competing analytic frameworks that do not exhibit such fidelity to the Charter. By focusing this evaluation on Schmitt's model, I expect the results will have implications for the use-of-force debate more generally.

The article begins with a discussion of why, as a practical matter, discerning a peacetime use-of-force threshold in cyberspace is important. Next, I detail the Article 2(4) prohibition on the use of force and the difficulty applying it in the cyber context. I then review Schmitt's model and perform a Schmitt Analysis of Stuxnet. Finally, I examine what the analysis of Stuxnet reveals about the framework's continued utility and relevance. Overall, I find that Schmitt's underlying analytical approach remains sound—that is, the best way to characterize the lawfulness of peacetime cyber operations is to predict how states will characterize them. That said, the Stuxnet analysis reveals several limitations with Schmitt's framework, while also highlighting opportunities to broaden it. More importantly, I conclude that the time has come to relax the model's strict adherence to the UN Charter because Article 2(4) is just one of several factors that states are likely to consider when characterizing the lawfulness of cyber operations.

the need for clarity has taken on greater importance now that the United States and many of its allies treat cyberspace as a military operational domain

Why the Use-of-Force Threshold Matters

Cyberspace represents a strategic vulnerability for many states because it is inextricably tied in to their economies, critical infrastructures, and even their national security apparatus. Compounding these concerns is the fact that a wide range of actors have proven adept at exploiting these vulnerabilities. Cybercrime, for example, is now estimated to exceed $1 trillion globally per year.[7] Even the most secure U.S. defense networks are not immune.[8] The scope of the problem has become so great that some claim the United States is engaged in a cyber war, and that it is losing.[9] The *National Security Strategy* of 2010 notes that "cybersecurity threats represent one of the most serious national security, public safety, and economic challenges we face as a nation."[10] The White House's *International Strategy for Cyberspace* of 2011 goes further by proclaiming: "When warranted, the United States will respond to hostile acts in cyberspace as we would to any other threat to our country," to include a military response.[11]

Against this backdrop, discerning a cyber use-of-force threshold becomes important for a number of reasons. Foremost is that characterizing cyber operations is a precondition to determining which legal regime governs state behavior.[12] If state-sponsored cyber activities constitute a use of force, then international law governing the use of force (jus ad bellum) and the Law of Armed Conflict (jus in bello) apply. In appropriate circumstances, this could trigger a state's right to self-defense and thereby permit a forceful, perhaps even armed response. In contrast, non-state-sponsored cyber operations and operations not amounting to a use of force are traditionally governed by more constrained law enforcement regimes.[13]

The need for clarity has taken on greater importance now that the United States and many of its allies treat cyberspace as a military operational domain.[14] Accordingly, discerning a use-of-force threshold would seem to be necessary for a wide range of peacetime military activities, such as defining the spectrum of permissible peacetime cyber operations, such as computer network exploitation; developing peacetime cyber rules of engagement; identifying appropriate approval authorities; assigning appropriate agency responsibilities and resources; signaling adversaries and allies as part of a deterrence strategy; recognizing when treaty obligations have been triggered; and determining whether UN Security Council authorization is required to conduct certain operations.

The Use of Force in Cyberspace

Notwithstanding the need for clarity discussed above, there is no international consensus on what constitutes a use of force in cyberspace, nor does it appear a mechanical rule is likely to emerge any time soon.[15] This section describes why ambiguity persists and the various solutions that have been proposed to resolve it. After summarizing the relevant law governing the use of force in international relations, I highlight the technical, legal, and political challenges of applying existing norms within cyberspace.

Use of Force Under the UN Charter. Jus ad bellum[16] describes the law governing the transition from peace to armed conflict. Though grounded in customary international law, the black letter principles of jus ad bellum are now contained in Article 2(4) of the UN Charter, which prohibits states from the "threat or use of force" in their international relations. Several features of this prohibition are problematic in the cyber context. First, Article 2(4) only pertains to international relations between sovereign states—it does not proscribe the conduct of nonstate actors,

who appear to be the source of most malicious cyber activity. Also, as noted above, the Charter does not define the phrase *use of force*. Finally, Article 2(4) does not provide any exceptions to the prohibition on the unilateral use of force, nor does it prescribe remedies for unauthorized uses of force. Such exceptions and remedies are found in chapter VII of the Charter which, unlike Article 2(4), is not limited to relations between states and employs thresholds quite distinct from the use-of-force standard.[17] Importantly, it is not the use of force, but rather an "armed attack" that triggers a state's right to use force in self-defense.[18]

Although use of force is not defined, an approximate threshold has emerged through consideration of the Charter's preparatory work, state practice, and *opinio juris*.[19] First, the framers of the Charter took an instrument-based, vice consequence-based, approach to the use of force prohibition.[20] While acknowledging that states are most concerned about the consequences of coercive activities (that is, the degree of injury, deprivation, or destruction), the framers recognized that a consequence-based criterion was too subjective to distinguish lawful from unlawful state coercion.[21] Because the term *force* connotes violence, injury, and destruction—consequences that pose the greatest threat to international peace and security—they adopted the instrument-based use-of-force standard as prescriptive shorthand. According to Professor Schmitt, such an approach "eases the evaluative process by simply asking whether force has been used, rather than requiring a far more difficult assessment of the consequences that have resulted."[22] According to this approach, the Article 2(4) prohibition does not extend to all forms of state coercion. For example, the instruments of economic and political coercion are not prohibited.[23] Less clear, but generally accepted, is that the prohibition is not limited to "armed" force—it may also encompass unarmed, nonmilitary physical force, such as releasing water from a dam.[24] The International Court of Justice highlighted this point in *Nicaragua v. United States* (hereinafter *Nicaragua*), when it concluded that arming and training guerrillas amounted to a prohibited use of force, even though it did not rise to the level of an armed attack.[25] Accordingly, the use of force threshold has traditionally been viewed as lying somewhere between purely economic and political coercion on the one hand and activities that result in physical damage or injury on the other.[26] As discussed below, discerning a clear use-of-force threshold in this gray area—a difficult task even in traditional kinetic context—has proven particularly difficult in the cyber context.[27]

Use of Force in Cyberspace. The difficulty of applying Article 2(4) in cyberspace is that the instrument-based paradigm does not cleanly translate to cyber operations, particularly for gray area operations that do not result in physical harm.[28] According to a strict instrument-based interpretation, even highly disruptive peacetime cyber operations may not qualify as a use of force because they lack the traditional kinetic characteristics associated with armed force.[29] Most commentators reject this strict interpretation because of the potential widespread destabilizing consequences of cyber operations. That said, by focusing on consequences to determine whether prohibited force has been used, these commentators call Article 2(4)'s instrument-based paradigm into question.

discerning the use-of-force threshold is really about predicting how states will respond to cyber incidents in light of prevailing international norms

The perceived shortcomings of Article 2(4) have led many to propose a new treaty law to govern cyber operations.[30] Others counter that states are unlikely to negotiate any meaningful treaties in the foreseeable future. They argue that divergent strategic interests and significant attribution problems make treaty enforcement unrealistic. They suggest that existing international norms, though imperfect, are adequate for extrapolating general principles governing the use of force in cyberspace and urge gradual expansion of international norms within the Article 2(4) framework.

Over the past two decades, proponents of this gradualist approach have developed several analytic frameworks to characterize the legality of cyber operations. First is the "effects-based" approach, which states that the quantum of damage, and not the means of attack, is all that matters. The advantage of this approach—which is generally favored by U.S. policymakers and military operators—is that it is fairly simple to apply and it acknowledges that states are principally concerned about consequences. The drawback is that it represents a hard break from the Charter's instrument-based approach and thereby relies on inherently subjective assessments among states that have divergent strategic capabilities, vulnerabilities, and interests. A second approach relies upon kinetic equivalency, arguing that cyber operations constitute a use of force only if the damage they cause could previously have been achieved only by a kinetic attack.[31] This framework generally adheres to the Charter's instrument-based approach, but it struggles to characterize hostile gray area cyber operations—such as projecting false targets on an adversary's early warning radars—that do not result in physical damage. A third approach applies a "strict liability" test for any cyber operations that target a state's critical infrastructure and vital interests because of the severe consequences that could result from such attacks. According to this model, the mere penetration of such systems—such as power production, stock exchanges, and air traffic control—can constitute evidence of hostile intent and thereby trigger the right of self-defense.[32] This framework suffers from the inherent subjectivity of defining what constitutes "critical infrastructure and vital interests," and because it expands the gray area to encompass activities such as computer network exploitation that are not currently prohibited by international law. Professor Schmitt's framework represents the fourth major model.

Schmitt Analysis

Professor Schmitt recognized that discerning the use-of-force threshold is really about predicting how states will characterize and respond to cyber incidents in light of prevailing international norms.[33] To aid in such predictions, his framework bridges the instrument- and consequence-based approaches. In keeping with the Article 2(4) instrument-based standard, his model consists of seven factors that represent the major distinctions between permissible (that is, economic and political) and impermissible (armed) instruments of coercion.[34] When applying these factors, the more closely the attributes of a

cyber operation approximate the attributes of armed force, the more likely states are to characterize the operation as a prohibited use of force. The Schmitt Analysis factors consist of the following:

- *Severity:* Cyber operations that threaten physical harm more closely approximate an armed attack. Relevant factors in the analysis include scope, duration, and intensity.
- *Immediacy:* Consequences that manifest quickly without time to mitigate harmful effects or seek peaceful accommodation are more likely to be viewed as a use of force.
- *Directness:* The more direct the causal connection between the cyber operation and the consequences, the more likely states will deem it to be a use of force.
- *Invasiveness:* The more a cyber operation impairs the territorial integrity or sovereignty of a state, the more likely it will be viewed as a use of force.
- *Measurability:* States are more likely to view a cyber operation as a use of force if the consequences are easily identifiable and objectively quantifiable.
- *Presumptive legitimacy:* To the extent certain activities are legitimate outside of the cyber context, they remain so in the cyber domain, for example, espionage, psychological operations, and propaganda.
- *Responsibility:* The closer the nexus between the cyber operation and a state, the more likely it will be characterized as a use of force.[35]

According to Professor Schmitt, evaluating these factors is an imprecise and subjective endeavor. The factors are useful but not determinative, and they should not be applied mechanically. Rather, they need to be applied holistically according to the relevant context—that is, which factors are important and how they should be weighted will vary on a case-by-case basis. Moreover, he never intended the factors to be exhaustive, though they are often treated as such.[36] Finally, the framework is more useful for post hoc forensic analysis of particular cyber attacks than for characterizing real-time operations.[37]

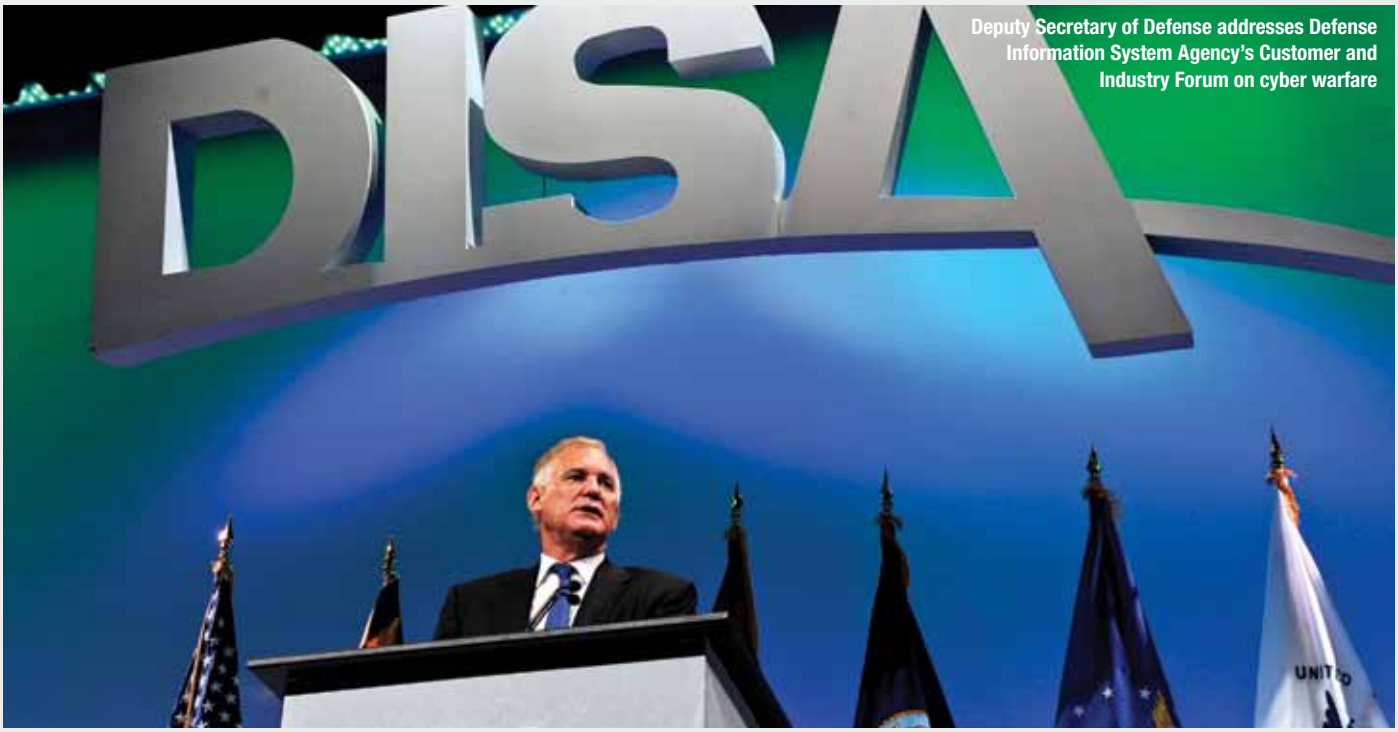
Professor Schmitt also acknowledged that his adherence to the Article 2(4) instrument-based paradigm appears tortuous, particularly given the appeal of simple effects-based frameworks. However, he reasoned that such adherence is necessary to properly describe where the cyber use of force threshold lies under prevailing standards—in contrast to the other leading models, which prescribe new standards for where the use of force threshold *should* lie.[38] He also believed that "reference to the instrument-based shorthand facilitates greater internal consistency and predictability within the preexisting framework. . . . As a result, subscription by the international community is more likely, and application should prove less disruptive and controversial."[39] In the end, the Schmitt Analysis has generally stood the test of time and remains one of the most commonly referenced frameworks for characterizing the use of force in cyberspace.

Characterizing Stuxnet

Stuxnet has been described as a game changer—the first digital "fire and forget" precision-guided munition and perhaps the first peacetime act of cyberwar.[40] According

U.S. Air Force (Lance Cheung)

Analysts attending Defense Cyber Investigations Training



Deputy Secretary of Defense addresses Defense Information System Agency's Customer and Industry Forum on cyber warfare

DOD (R.D. Ward)

to reports, the Stuxnet worm was designed to target gas centrifuges used in Iran's uranium enrichment program in Natanz. Specifically, the worm exploited the software used in programmable logic controllers (PLCs) manufactured by Siemens. These PLCs controlled frequency converter drives that, in turn, controlled the speed of the centrifuges. By manipulating the speed of already temperamental and frequency-sensitive centrifuges over time (weeks and perhaps months), Stuxnet caused as many as 1,000 of the centrifuges to break. Estimates suggest Stuxnet set Iran's nuclear program back by several years.[41]

Although some have described Stuxnet's code as a relatively unsophisticated "Frankenstein patchwork of existing tradecraft, code and best practices drawn from the global cyber-crime community," its true sophistication lies in the synergy of its components and its method of infection.[42] First, Stuxnet's designers required incredibly precise intelligence about Iran's PLCs and frequency converters, as well as the performance parameters of its centrifuges.[43] Second, the malware was self-replicating and designed to infect systems that were not connected to the Internet ("air-gapped"), thereby requiring the use of intermediary devices such as thumb drives. Stuxnet also employed four "zero-day" exploits[44] and two stolen digital signatures to gain access to targeted systems. Finally, Stuxnet appears to have been designed to avoid collateral damage.[45] If the malware did not detect the specific software-hardware configuration associated with Iran's enrichment program, the program would lie dormant. It was also designed to delete itself from thumb drives after infecting three machines, and it contained a built-in self-destruct feature. Thus, even though the worm is reported to have infected more than 100,000 hosts in 155 countries, 60 percent of the infections were localized to Iran, and there are no reports of physical damage outside of Iran.[46] Although no one has claimed responsibility for Stuxnet, it has the signature of a state operation.[47] Most speculation and some anecdotal evidence points to Israel, with possible support from the United States and/or Germany.[48]

Although there is an emerging consensus that Stuxnet constituted a use of force, there is value in looking beyond the physical damage to see what the operation reveals about the strengths and weaknesses of existing analytic frameworks, such as the Schmitt Analysis. Accordingly, the following analysis is offered not only to characterize Stuxnet, but to help evaluate Schmitt's framework.

Severity: According to this criterion, Stuxnet is per se a use of force because it caused physical damage. Moreover, the damage was inflicted upon a critical Iranian interest—its nuclear program. By setting Iran's nuclear program back several years, the duration of Stuxnet's consequences also supports characterizing it as a use of force—though this delay is due to sanctions that bar Iran from legitimately acquiring new centrifuges. It is also worth noting that the scope of the actual damage appears to have been relatively minor and fairly discrete, and that it posed no apparent risk of harm to personnel.

Immediacy: According to this factor, Stuxnet would probably not be viewed as a use of force. The attack, which consisted of at least three waves over 10 months, took time to evolve.[49] More importantly, once a targeted system was infected, it appears the damage took weeks or even months to manifest. Given the nature of how the attack unfolded, there was and remains adequate opportunity for Iran to mitigate the harmful effects and to seek peaceful accommodation. That said, given the physical damage inflicted, immediacy is probably not a factor that warrants much emphasis in this analysis.

Directness: There appears to be a direct causal connection between Stuxnet and the damaged centrifuges.

Invasiveness: Stuxnet represents a significant intrusion on Iranian sovereignty. Not only does it appear to have crossed international borders, but it targeted sensitive and highly secure systems that were air-gapped from the Internet. That said, Stuxnet would have been just as invasive if it had simply collected intelligence on the inner workings of the Natanz facility—an activity the interna-

tional community would likely not regard as a use of force.

Measurability: Taking into account the already high failure rate of Iran's centrifuges, the consequences attributed to Stuxnet appear both quantifiable and identifiable.

Presumptive legitimacy: Stuxnet does not enjoy presumptive legitimacy. Short of UN Security Council authorization or actions taken in self-defense—both of which would constitute *lawful* uses of force—there is no customary acceptance within the international community for damaging another state's nuclear facilities. Even so, it is worth considering the effect of existing Iranian sanctions upon this analysis. First, Iran cannot import or export nuclear-related materials or technology. If such Iranian-owned nuclear materials are discovered outside of Iran, they can be lawfully seized and destroyed. Second, prior to Stuxnet, Iran had been operating its centrifuges for several years in violation of multiple UN Security Council Resolutions.[50] Although these points may relate more to whether Stuxnet constituted a *lawful* use of force, they also seem to bear on the factor of presumptive legitimacy.

Responsibility: Although no state has claimed responsibility for Stuxnet, the worm's purpose and design strongly suggest state involvement. That said, it is possible that Stuxnet was created and launched by nonstate actors—such as Iranian dissidents working with freelance hackers—in which case it would not be subject to international laws governing the use of force.

On balance, the Schmitt Analysis suggests most states would characterize Stuxnet as a use of force. The worm was highly invasive, caused direct and measurable physical damage, lacked a clear presumption of legitimacy, and probably involved state support.

What does the foregoing analysis of Stuxnet reveal about the continued usefulness of Professor Schmitt's framework? Most importantly, the model's underlying analytic approach appears sound—that is, discerning the use of force threshold entails predicting how states will characterize cyber operations. That said, the analysis reveals several limitations with the framework, as well as opportunities for its expansion.

First, it appears that in any given Schmitt Analysis, the characterization of a cyber operation may be derived from a single factor: severity of the consequences. If true, then the framework could arguably be reduced to an effects-based model with little remaining affinity with the Article 2(4) instrument-based paradigm. To illustrate the point, what if instead of damaging Iranian centrifuges Stuxnet achieved the same effects by causing the centrifuges to operate inefficiently or not at all? Except for severity, each of Schmitt's factors would likely be evaluated the same. It is debatable, though, whether the international community would consider such an operation a prohibited use of force. This is not to suggest that the other factors are irrelevant, but it highlights what Professor Schmitt himself acknowledged: "severity is self-evidently the most significant factor in the analysis."[51]

Next, the characteristics of Stuxnet and its intended target suggest at least one additional factor that may be relevant when performing a Schmitt Analysis: apparent compliance with the Law of Armed Conflict (LOAC).[52] Assuming reports are true, the fact that Stuxnet was targeted so precisely and designed to minimize collateral damage

U.S. Navy (Joshua J. Wahl)

Commander of Navy Cyber Forces observes spectral warrior demonstration during exercise Bold Alligator 2012

reveals something about the identity and intent of its creators. First, it reinforces the notion that Stuxnet was a state-sponsored operation, which is important because Article 2(4) only regulates state conduct. Second, it suggests Stuxnet's creators were concerned about complying with LOAC, particularly the principles of military necessity, distinction, and proportionality.[53] Thus, the responsible state apparently regarded Stuxnet as the equivalent of an armed attack and executed the operation as such. Since an armed attack constitutes a use of force, the implication is that states are more likely to characterize cyber attacks as a use of force if they appear to comply with LOAC—even in gray area operations that do not result in actual damage.

A third observation involves one of the most technically challenging aspects of cyber operations: attribution. For Article 2(4) and the principles of jus ad bellum to apply, the responsible party must be identified as a state.[54] As noted above, without reliable attribution states generally must respond to cyber operations as a law enforcement problem. Yet each of the prevailing frameworks, including the Schmitt Analysis, treats attribution as a condition precedent to any use-of-force analysis.[55] In other words, without attribution, a Schmitt Analysis offers limited practical value. But if state attribution can be established, it is questionable whether a Schmitt Analysis would be necessary because more revealing indicators should be discernable, such as motive and intent.

Next, to the extent state attribution bears on the characterization of cyber operations, so too should the victim state's response. As the International Court of Justice noted in *Nicaragua*: "it is the State which is the victim of an armed attack which must form and declare the view that it has been so attacked."[56] Although Iran has acknowledged the presence of Stuxnet in its systems, it has denied any significant damage and has never claimed that it was subject to an armed attack. As U.S. Cyber Command's top lawyer, Colonel Gary Brown, has commented: "Iran's 'non-position' on the Stuxnet event has been frustrating to practitioners in the field of cyberspace operations. Finally, there was a well-documented, unambiguous cyber attack to dissect! And yet there was little official discussion of the issue because Iran passed up its opportunity to complain of an unjustified attack."[57] Unfortunately, Professor Schmitt's framework does not address the implications of such state inaction. It remains to be seen what, if any, impact Iran's "non-position" has on the development of use of force norms in cyberspace.

A more significant observation relates to Professor Schmitt's premise that states will principally rely upon existing norms, particularly Article 2(4), when making use-of-force determinations in cyberspace. As some commentators predicted—and Stuxnet demonstrated—Article 2(4) has proven to be a "weak constraint on offensive cyber-attacks."[58] This is due, in part, to the difficulty of observing, measuring, and attributing cyber operations. More importantly, it reflects the fact that international law is not static and that the principles of jus ad bellum are not the exclusive province of the UN Charter.[59] Whereas contemporary interpretations of Article 2(4) reflect the distribution of traditional instruments of power—that is, political, military, and economic strength—the current array of cyber capabilities and vulnerabilities does not mirror the traditional distribution.[60] Consequently, states with significant cyber capabilities or vulnerabilities—regardless of their political, military, or economic strength—are likely to consider factors well beyond Article 2(4) when characterizing the legality of cyber operations. Such additional considerations may include relative cyber strengths and vulnerabilities; strategic risks and opportunities; scope of potential consequences; ability to control escalation; effectiveness of cyber deterrence; potential reactions by adversaries, allies, and international organizations; domestic politics; state declaratory policies; emerging state practice (including state inaction); attribution problems; and other legal, political, and technical constraints.[61] Moreover, given the novelty of cyberspace, different

Commander of U.S. Fleet Cyber Command and U.S. 10th Fleet addresses Information Dominance Corps

U.S. Navy (Shauntae Hinkle-Lymas)

states will likely weigh their strategic risks and opportunities very differently.

Perhaps these additional considerations explain why there has been so little academic debate about the legal implications of Stuxnet. Even though most states would probably agree that Stuxnet constituted a use of force under Article 2(4), they may be reluctant to characterize the attack as *unlawful* since, by targeting an illicit program in a pariah state, it was justifiable. In this regard, it is worth noting that Stuxnet's objective was consistent with multiple UN Security Council mandates and it promoted those mandates without resorting to *armed* force. Thus, it remains to be seen whether Stuxnet represents a new form of tacitly condoned cyber vigilante-ism, or whether the perpetrator(s) will eventually be held in contempt. Either way, Iran's "non-position" has made it easy for the international community to sidestep the issue.

policymakers and cyber practitioners must be prepared to operate in an ambiguous and contested legal environment

Conclusion

Although Professor Schmitt's analytic approach to characterizing cyber operations remains sound, the analysis of Stuxnet reveals several shortcomings with his model. These include severity of the consequences as a potentially determinative factor, attribution as a condition precedent to a use of force analysis, and failure to account for a victim state's "non-position" toward a particular cyber operation. This analysis also reveals at least one additional factor states may consider when characterizing cyber operations—whether an attack appears to comply with LOAC.

More importantly, this analysis suggests the time has come to relax the model's strict adherence to the Article 2(4) instrument-based paradigm. By tying his framework to Article 2(4), Professor Schmitt anticipated more consistent, predictable, and relatively objective characterizations of force in cyberspace. However, state practice over the last decade suggests that states will treat Article 2(4) as just one of several factors to consider when characterizing cyber operations.[62] As Professor Schmitt himself acknowledged, as state practice emerges, other considerations and normative approaches—such as greater emphasis on consequences—may come to dominate the analysis.[63] In light of recent events in Estonia, Georgia, and Iran, it appears that time has come.

The Schmitt Analysis of Stuxnet also has implications for the broader debate over the use of force in cyberspace. For one thing, the lack of discussion over the legal implications of Stuxnet demonstrates that states are unlikely to reach consensus on what constitutes a cyber use of force any time soon. The lack of a discernable threshold also suggests that state-sponsored gray area cyber attacks are more likely.[64] Consequently, policymakers and cyber practitioners and their legal advisors must be prepared to operate in an ambiguous and contested legal environment, while at the same time shaping new norms of acceptable state conduct.[65] In the end, these evolving norms are not likely to be constrained by Article 2(4)'s narrow prohibition on the use of force. Rather, they will likely reflect the new realities and unique features of cyberspace, such as cyber's potentially devastating consequences, the nontraditional distribution of cyber capabilities and vulnerabilities, and the international community's response (or lack thereof) to seminal events like Stuxnet. **JFQ**

NOTES

[1] United Nations (UN), *Charter of the United Nations and Statute of the International Court of Justice* (San Francisco, CA: UN, 1945).

[2] Michael N. Schmitt, "Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework," *Columbia Journal of Transnational Law* 37 (1999), 925. See also U.S. Senate, *Advance Questions for Lieutenant General Keith Alexander, USA Nominee for Commander, United States Cyber Command: Before the Senate Armed Services Committee*, 11th Cong., 11th sess., April 15, 2010, 11.

[3] Walter Gary Sharp, Sr., *Cyberspace and the Use of Force* (Falls Church, VA: Aegis Research, 1999), 140; and David E. Graham, "Cyber Threats and the Law of War," *Journal of International Law & Policy*, 4 (2010), 91–92.

[4] Isaac R. Porche III, Jerry M. Sollinger, and Shawn McKay, *A Cyberworm That Knows No Boundaries* (Washington, DC: RAND, 2011), ix.

[5] Duncan B. Hollis, "Could Deploying Stuxnet Be a War Crime?" OpinioJuris.org, January 25, 2011; Gary D. Brown, "Why Iran Didn't Admit Stuxnet Was an Attack," *Joint Force Quarterly* 63 (4th Quarter 2011), 70–73; and John Richardson, "Stuxnet as Cyber Warfare: Applying the Law of War to the Virtual Battlefield," Social Science Research Network Working Paper, 2011.

[6] Ibid.; Michael N. Schmitt, interview by the author, December 1, 2011; and Colonel Gary D. Brown, interview by the author, December 2, 2011.

[7] *Information Operations Primer* (Carlisle Barracks, PA: U.S. Army War College, November 2011), 23.

[8] Ellen Nakashima, "Cyber-Intruder Sparks Massive Federal Response—and Debate Over Dealing With Threats," *The Washington Post*, December 9, 2011.

[9] See "Mike McConnell on how to win the cyber-war we're losing," *The Washington Post*, February 28, 2010; Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What To Do About It* (New York: Harper-Collins Publishers, 2010); Ryan Singel, "Is the Hacking Threat to National Security Overblown?" *Wired Magazine*, June 3, 2009; and Bruce Schneier, "The Threat of Cyberwar Has Been Grossly Exaggerated," *Schneier.com*, July 7, 2010.

[10] *National Security Strategy* (Washington, DC: The White House, May 2010), 27.

[11] *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World* (Washington, DC: The White House, May 2011), 14.

[12] Charles J. Dunlap, Jr., "Perspectives for Cyber Strategists on Law and Cyberwar," *Strategic Studies Quarterly* (Spring 2011), 84; and Eneken Tikk, Kadri Kaska, and Liis Vihul, I*nternational Cyber Incidents: Legal Implications* (Tallin, Estonia: NATO Cooperative Cyber Defence Centre, 2010), 79.

[13] Dunlap, 84.

[14] See Department of Defense (DOD), *Department of Defense Strategy for Operating in Cyberspace* (Washington, DC: DOD, July 2011), 5; *National Security Strategy*, 22; and *International Strategy for Cyberspace*, 14.

[15] As one commentator has noted, "Although the application of the UN Charter Article 2(4) to CNA [computer network attack] is an intellectually interesting question, there is reason to wonder whether, as a practical matter, the issue ever will arise in a context requiring an actual decision. The most important obstacle may be the difficulty of attributing CNA to State action. Moreover, even if State use of CNA were to emerge as a recognizable phenomenon, such CNA would have to occur in relative isolation in order squarely to pose the relevant legal issue. Because this seems improbable, it likely will be a long time, if ever, before the practice of States, decisions of the International Court of justice (ICJ), or other recognized sources of international law yield a clarification of how Article 2(4) applies to CNA." Daniel B. Silver, "Computer Network Attack as a Use of Force under Article

2(4) of the United Nations Charter," in *Naval War College International Law Studies* 76; Computer Network Attack and International Law, ed. Michael N. Schmitt and Brian T. O'Donnell, 77–78 (Newport, RI: Naval War College Press, 2002).

[16] Latin for "right to the war," more commonly understood as the "right to wage war." The principles of jus ad bellum are distinct from the related principles of jus in bello—or the Law of Armed Conflict (LOAC)—which govern how armed conflict is conducted.

[17] For example, compare Article 39's "breach of the peace" and "aggression" thresholds; Article 41's "measures short of armed force" standard; Article 42's "such action by air, sea, or land forces as may be necessary" language; and Article 51's "armed attack" threshold for self-defense actions.

[18] Schmitt, "Computer Network Attack and the Use of Force," 920.

[19] Ibid.," 905–907. *Opinio juris* means a sense of legal obligation. In the international law context, it is used to judge whether State practice and adherence to norms is due to a sense of legal obligation, vice political expediency, or convenience. *Duhaime.org Legal Dictionary*, available at <www.duhaime.org/ LegalDictionary/O/OpinioJuris.aspx>. When opinio juris exists and is consistent with nearly all state practice, customary international law emerges. For example, Article 38(1)(b) of the Statute of the International Court of Justice accepts "international custom" as a source of law, but only where this custom is: (1) "evidence of a general practice," and (2) "accepted as law."

[20] See, for example, Schmitt, "Computer Network Attack and the Use of Force," 909; and Duncan B. Hollis, "Why States Need an International Law for Information Operations," *Lewis & Clark Law Review* 11 (2007), 1040.

[21] Schmitt, "Computer Network Attack and the Use of Force," 914.

[22] Ibid., 911.

[23] Ibid. A compelling argument does exist, however, that political and economic coercion that threatens the territorial integrity or political independence of another state constitutes an unlawful use of force under Article 2(4). See Sharp, 89–90, 118.

[24] Sharp, 101.

[25] *Nicaragua*, para 228. According to the ICJ, the distinction between the threat or use of force (including armed force) and an armed attack is based on the operation's "scale and effects." *Nicaragua*, para. 195.

[26] Schmitt, "Cyber Operations in International Law," 155.

[27] See Matthew C. Waxman, "Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)," *The Yale Journal of International Law*, 36 (2011), 445–447.

[28] Hollis, "Why States Need an International Law for Information Operations," 1040.

[29] Ibid., 1041. Professor Schmitt highlighted this dilemma: "The advent of cyber operations threw the instrument-based approach into disarray by creating the possibility of dramatically destabilizing effects caused by other than kinetic actions." Schmitt, "Cyber Operations in International Law," 177.

[30] See Clarke and Knake, 219–255; Hollis, "Why States Need an International Law for Information Operations," 1053; and Silver, 78.

[31] See Hollis, "Why States Need an International Law for Information Operations," 1041; and Graham, 91.

[32] Sharp, 129–131; and Hollis, "Why States Need an International Law for Information Operations," 1041.

[33] Schmitt, interview by the author. In this regard, Professor Schmitt noted that states would likely seek to balance the conflicting objectives of maximizing their own freedom of action in cyberspace while avoiding the harmful consequences caused by adversaries. See also Schmitt, "Cyber Operations in International Law," 155.

[34] Schmitt, "Computer Network Attack and the Use of Force," 914.

[35] Professor Schmitt's responsibility factor is best understood as a measure of the degree of state attribution, although he did not describe it as such. State attribution is an important part of his model because Article 2(4) and customary international laws only govern the use of force between states.

[36] Schmitt, interview with author. See also, Michael N. Schmitt, "The Sixteenth Waldemar A. Solf Lecture in International Law," *Military Law Review*, 176 (2003), 417.

[37] Schmitt, interview with author.

[38] Schmitt, "Computer Network Attack and the Use of Force," 917.

[39] Ibid.

[40] See, for example, Lukas Milevski, "Stuxnet and Strategy: A Special Operation in Cyberspace?" *Joint Force Quarterly* 63 (4th Quarter 2011), 64; and Porche, Sollinger, and McKay, 1.

[41] See Kim Zetter, "How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History," *Wired.com*, July 11, 2011; Porche, Sollinger, and McKay; Nicolas Falliere, Liam O Murchu, and Eric Chien, *W32.Stuxnet Dossier* (Symantec, February 2011); and Hollis, "Could Deploying Stuxnet Be a War Crime?"

[42] Milevski, "Stuxnet and Strategy," 66 (citing James P. Farwell and Rafal Rohozinski, "Stuxnet and the Future of Cyber War," *Survival* 53, no. 1 [January 2011], 24.).

[43] According to reports, representatives from the International Atomic Energy Agency who had inspected Natanz did not even have this level of information. Ibid., 65.

[44] A *zero-day threat* is a software vulnerability unknown to the user or software developer that can be exploited before the vulnerability can be fixed.

[45] Richardson, 7.

[46] Falliere, Murchu, and Chien, 10. Despite early speculation that Stuxnet damaged an Indian satellite, the claim has never been substantiated.

[47] Porche, Sollinger, and McKay, 8.

[48] Zetter; Brown, "Why Iran Didn't Admit Stuxnet Was an Attack"; Richardson, 30; and William J. Broad, John Markoff, and David E. Sanger, "Israeli Test on Worm Called Crucial in Iran Nuclear Delay," *The New York Times*, January 15, 2011.

[49] Falliere, Murchu, and Chien, 8.

[50] See, UN Security Council Resolutions 1737 (2006), 1747 (2007), 1803 (2008), and 1929 (2010).

[51] Schmitt, "Cyber Operations in International Law," 156.

[52] The Law of Armed Conflict (LOAC)—also known as the Law of War and International Humanitarian Law—is the body of law governing the conduct of armed conflict. It is derived from both customary international law and treaty law, including The Hague and Geneva Conventions. The basic principles of LOAC include: military necessity, unnecessary suffering, distinction, proportionality, and chivalry. *Air Force Operations & The Law: A Guide for Air, Space & Cyber Forces* (Maxwell AFB, AL: The Judge Advocate General's School, 2009), 13–20.

[53] Ibid.

[54] Herbert S. Lin, "Offensive Cyber Operations and the Use of Force," *Journal of National Security Law & Policy* 4 (2010), 77.

[55] Schmitt, interview with author.

[56] *Nicaragua*, para. 195.

[57] Brown, "Why Iran Didn't Admit Stuxnet Was an Attack," 71.

[58] Waxman, 426.

[59] Graham, 88.

[60] Waxman, 448–458.

[61] Ibid. See also Graham, 89.

[62] Waxman, 448–458; and Sharp.

[63] Schmitt, "Computer Network Attack and the Use of Force," 917.

[64] As representatives from NATO's Cooperative Cyber Defence Centre of Excellence (CCDCOE) have noted: "it is the general murkiness, the lack of clear policies and procedures, the lack of direct evidence of the attacking entity's identity that may make such attacks even more attractive. In such a volatile environment, by deliberately remaining below the threshold of use of force and at the same time using national policy cover as shield against investigations and prosecution, an attacking entity may believe there is less likelihood of reprisal even if the attacker's identity is suspected." CCDCOE, *International Cyber Incidents: Legal Implications*, 103.

[65] Waxman, 426; Silver, 75.

U.S. Navy Secretary meets with Korean Minister of Defense in Seoul

U.S. Navy (Kevin S. O'Brien)

A FOCUS ON COSTS, NOT BENEFITS, Dampens Koreans' Desire for Reunification

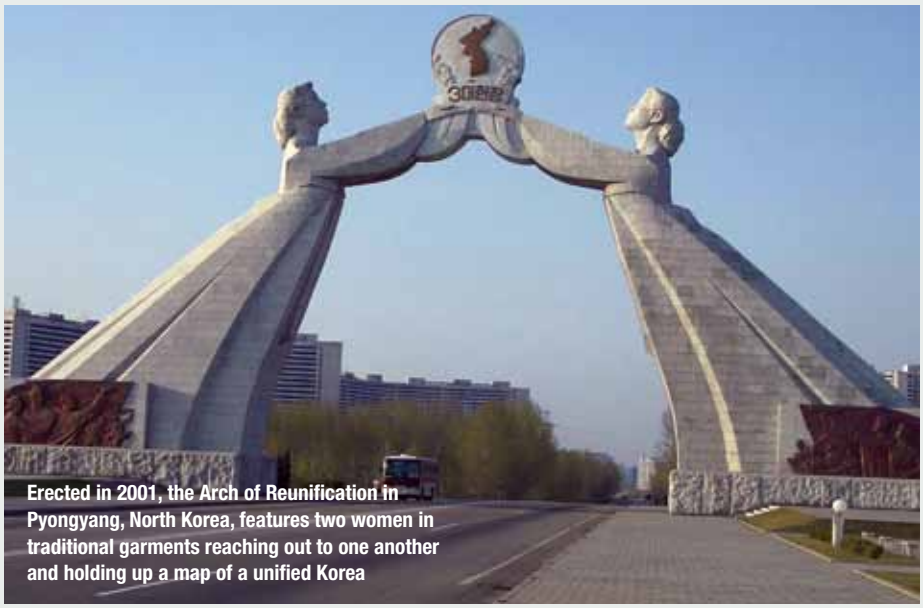
By GREGORY MACRIS

Young people think the financial sacrifice will be huge. That's why they may have negative emotions toward unification.[1]

—Republic of Korea President Lee Myung-bak, October 2011

While reunification remains South Koreans' preferred method of ending the peninsula's long division, Korean youth increasingly are contemplating alternatives such as permanent separation. Many consider North Korea another foreign country, albeit one whose inhabitants share language and ancestry. Numerous factors underpin their changing attitude. Sixty years have passed since the Korean War sealed the frontier, reducing familial ties and other linkages with the North. Rapid increases in wealth, plus advances in communications and transportation, have brought South Korea's mindset closer to the West. The strongest

Gregory Macris wrote this essay while a student at the National War College. It won the Strategy Article category of the 2012 Chairman of the Joint Chiefs of Staff Strategic Essay Competition.



Erected in 2001, the Arch of Reunification in Pyongyang, North Korea, features two women in traditional garments reaching out to one another and holding up a map of a unified Korea

catalyst of anti-unification sentiment among Republic of Korea (ROK) youth, however, is the monetary cost of unification, which could surpass $2 trillion. Overcoming anxieties that equate political union with impoverishment will require ROK decisionmakers to portray costs as investments and to highlight reunification's economic benefits, which will endure long after expenditures subside. Since a reunified Korea furthers long-term U.S. interests in Northeast Asia, the United States should support the ROK effort.

Once Solid, Support Begins to Dwindle

ROK politicians continue to promote peninsular union, fearing electoral blowback if they abandoned this longtime strategic objective. Nevertheless, recent polling shows support for integration dropping. Eighty percent of mid-1980s South Koreans asserted unification was imperative. That figure now reads 56 percent.[2] Young adults poll at 41 percent, while only 20 percent of ROK teenagers consider national union vital. Of citizens claiming that achieving reunification should be the government's highest objective, 83 percent were elderly. Most South Koreans under 30 assert the government should focus first on improving their job prospects.[3]

Despite loud pro-reunification rhetoric, ROK government policies often preserve the peninsular status quo. Examples include large-scale food and fertilizer donations to North Korea and continued funding of the Kaesong Industrial Complex north of the demilitarized zone, which conservatively provides $20 million yearly to the Kim family.[4] Curtailing financial support could hasten regime change and thereby increase reunification prospects. Nonetheless, prominent Korea watchers contend that Seoul prefers that the North undergo a China-like economic reform before unification proceeds.[5]

Electoral calculations explain the go-slow approach, as ROK citizens jealously guard their hard-won prosperity and punish politicians who risk it. Recently publicized cost estimates on reunification have stoked fears of a return to poverty. The Presidential Council for Future and Vision set the price tag for union at $2.1 trillion if the North Korean regime toppled today.[6] That figure represents $40,000 per ROK citizen and would raise the national debt from a manageable 38 percent of gross domestic product (GDP) to 135 percent.

What Is Behind These Enormous Figures?

South Korea's 49 million residents enjoy a per capita GDP of approximately $30,000. Corresponding figures for the North are unreliable, but demographers estimate the population at 24 million and GDP at $1,000 to $2,000. The South's assimilation of a population half its size and far poorer would require a gargantuan investment. Korea experts peg first-year expenditures—primarily for humanitarian assistance and resettlement—at $50 billion.[7] Costs could rise further if the nations reunified following a violent struggle, as in Vietnam.[8]

Infrastructure expenditures increase reunification's cost considerably. Compared to South Korea's infrastructure, the North's utility and transportation grids appear medieval. While the ROK rates among the most wired nations in the world, Internet connectivity is rare in North Korea. Much agricultural land lies fallow and environmental degradation is frightening in scope. Also worrisome is the North's woeful underinvestment in human capital. Although basic literacy surpasses that of most developing countries, the ideology-heavy student curriculum has a 1950s feel, and even engineers have limited computer proficiency. Furthermore, the mid-1990s famine and continuing malnutrition have stunted cognitive and physical growth of an entire generation of North Koreans.

South Koreans who fear union for financial reasons look worryingly at Germany, where reunification expenditures between 1989 and 2010 surpassed $2 trillion. West Germany faced a comparatively simple assimilation next to South Korea, which must incorporate a far larger, poorer, and less-educated population. Moreover, while a physical barrier separated Germany for nearly 30 years, it was hardly impassable. Significant East-West trade occurred even after the Berlin Wall was constructed. The governments in Bonn and Berlin maintained phone, mail, and transportation links, and had inked 30 treaties to minimize practical repercussions of the political division.[9] In sum, East German dependence on the West arising well before 1989 created conditions that smoothed unification. Linkages between North and South Korea pale by comparison.

Yet a closer look at the German example offers lessons and cost savings for South Korea. Germany's introduction of a common currency upon reunification proved costly because the East's ostmark had a pre-unification value just one-fourth that of the deutsche mark. Similarly expensive was the common wage scale for Easterners, whose pre-1989 productivity rated just 25 percent of their Western cousins.[10] Unfettered migration rights and migrants' immediate qualification for social welfare raised expenditures further. With each measure, the German government sought to solidify political union by leveling incomes regionally.

Nevertheless, examples abound of politically stable nations whose regions differ widely in wealth. China's boom has little enhanced its central and western provinces, while in Italy, Sicilian incomes are barely one-third of those in Milan. Even in the United

States, per capita GDP in the South trails the North, 147 years after the Civil War. Any attempt by a unified Korea to quickly harmonize Northern and Southern incomes would drain government coffers and ultimately fail.

A RAND Corporation study proposes a more modest effort. Rather than pegging North Koreans' income as a percentage of Southerners' income, RAND's model aims only to triple existing Northern GDP. The resulting reunification cost estimates range widely because of one variable difficult to fix: the current size of the North Korean economy. Nonetheless, RAND predicts a more manageable price tag of $50 to $667 billion; private funding from South Koreans' savings and the global capital market could cover half, with governments and international financial institutions providing the remainder.[11]

Increased Economic Activity: The Other Side of the Ledger

The financial benefits of peninsular reunification receive short shrift in South Korean media, with expected negative results on under-30 public opinion. Many youth are unaware a political agreement would bring both short- and long-term economic stimulus. First to benefit would be South Korean construction firms, owing to aforementioned infrastructure requirements in North Korea. Longer term, the North's greater fecundity would help alleviate what is perhaps South Korea's greatest strategic challenge: a birth rate in 2010 that ranked as the world's lowest (1.14 children per woman).[12]

Significant savings would accrue from reduced military spending, redirecting capital to more productive parts of the Korean economy. Experts calculate a unified Korea would require 500,000 men in uniform (corresponding figures for North and South Korea today are 1.1 million and 680,000, respectively.)[13] Owing to the low wages paid in the North and the expectation its soldiers would comprise a large percentage of the unified military, shrinking the ROK army would provide a significant "peace dividend." Further, universal ROK conscription delays young males' entry into higher education and the labor force, with predictably negative economic consequences.

Its only land frontier sealed, South Korea resembles an island economy plagued by high transportation costs. Erasing the fortified border would allow land shipment of goods to and from China and Russia. Energy costs would fall, as an envisioned pipeline from Vladivostok to Seoul would reduce seaborne shipments of expensive liquefied natural gas.[14] Reunification also would lower capital costs since government and private industry currently pay higher interest rates because of political uncertainty.

Costs a Factor, Not a Non-Starter

Recent developments on the Korean peninsula, from North Korea's 2010 sinking of the *Cheonan* to its continuing nuclear and ballistic missile activities in contravention of international sanctions, seemingly make discussion of reunification an academic exercise at best. Yet might an "outlier" be lurking? In 1989, few analysts were predicting the fall of the Berlin Wall or collapse of the Soviet

South Korean marines participate in urban operations training at Korea Training Center where U.S. Marines take part in Korea Interoperability Training

U.S. Marine Corps (John Kennicutt)

U.S. Navy (Melissa Pelosi)

Chairman of South Korean Joint Chiefs of Staff talks with commanding officer of USS *Chafee* during exercise Foal Eagle 2012

Union. It thus behooves the South Korean government (and its strongest ally, the United States) to plan prudently for reunification, irrespective of timing and likelihood.

President Lee Myung-bak has gotten the message. Even as his electorate is turning rightward, demanding swift retribution for any future *Cheonan* incidents, Lee's administration is tacking to center. It is executing a robust public diplomacy campaign, for example, whose capstone television programs—delivered in sitcom and reality show formats favored by South Korean youth—aim to portray North Koreans in a more favorable light and tout the economic benefits of reunification.[15] Reshaping public opinion is no easy task, however, and will require great patience and even greater resourcing. The United States should seek opportunities to echo Lee's pro-unity message toward Koreans under age 30. It should utilize both high-profile encounters, such as President Barack Obama's March 2012 visit for the Seoul Nuclear Security Summit, and lesser known tools like Fulbright Scholarships and grants for prominent unification supporters to convince Korean youth that reunification under an open democratic system offers the greatest chance for regional stability and economic growth. **JFQ**

NOTES

[1] Chico Harlan, "South Korean Young People Are Wary of Unification," *The Washington Post Online Edition*, October 17, 2011.

[2] Ibid.

[3] Christine Kim, "Paying for Unification: Only 10.8% Want Taxes," *Joinsmsn.com*, March 3, 2011.

[4] Dick Nanto and Mark Manyin, *The Kaesong North-South Korea Industrial Complex* (Washington, DC: Congressional Research Service, March 17, 2011), 1.

[5] Andrei Lankov, "Working Through Korean Unification Blues," *Asia Times Online*, November 15, 2007.

[6] "Sudden Reunification Would Total $2.1 Trillion," *The Chosun Ilbo Online Edition*, November 4, 2011.

[7] "Korean Reunification Would Cost $2.38 Trillion," *Asia Pulse Online,* October 7, 2011.

[8] Peter M. Beck, "Contemplating Korean Unification," *The Wall Street Journal*, January 4, 2010.

[9] Hanns Gunther Hilpert, "A Comparison of German and Korean Division: Analogies and Differences," *International Journal of Korean Reunification Studies*, Korea Institute for National Reunification, June 30, 2010.

[10] Charles Wolf, Jr., "Korean Unification: How It Might Come Along, and at What Cost?" *Defense and Peace Economics* 17, no. 6, 681–690.

[11] Ibid.

[12] Theresa Kim Hwa-young, "South Korea Has World's Lowest Birth Rate," Asia News IT, February 26, 2010.

[13] *Asia Pulse Online*, October 7, 2011.

[14] Jason Struther, "Russia, Two Koreas Renew Talks on Stalled Gas Pipeline," *VOA News Online*, September 20, 2011.

[15] Harlan.

U.S. Air Force and naval aircraft fly over USS *Abraham Lincoln*, USS *Kitty Hawk*, and USS *Ronald Reagan* carrier strike groups during exercise in Philippine Sea

U.S. Navy (Todd P. Cichonowicz)

Delivering Air Sea Battle

By MARK P. FITZGERALD

Reminiscent of the capabilities in a Tom Clancy novel, the Services have teamed together to deliver a new concept of operations called Air Sea Battle (ASB). Chief of Naval Operations Admiral Jonathan Greenert and Chief of Staff of the Air Force General Norton Schwartz have provided in their recent article[1] an excellent high-level look at the challenges they face, yet many questions remain about the concept of operations and the programs that will underpin this effort.

For the first time since the Cold War, the Services have a chance to design coherent, interoperable capabilities against a common, agreed upon challenge. Getting the requirements correct will be vitally important to our national defense. While ASB and the higher level Joint Operational Access Concept counter–antiaccess/area denial (A2/AD) strategy will be the yardstick against which future programs will be funded, this ASB imprimatur must bring with it capabilities that are interoperable and networked and that hold entire enemy capabilities at risk. It is not clear that current programs are moving in that direction.

Free access to the maritime commons remains the foundation of our maritime strategy. However, the growing threat from long-range antiship ballistic missiles—such as the Chinese DF-21D, long-range cruise missiles such as the Chinese DH-10, advanced combat aircraft such as the Chinese J-20 or Russian PAK-FA, and improved mobile ballistic and air defense missiles including the Russian S-300/400/500 and Chinese HQ-9 variants—allow potential adversaries to threaten our naval and air freedom of movement hundreds of miles from an adversary's shore from bastions deep inside its territory. While the United States may never fight China or Russia,

Admiral Mark P. Fitzgerald, USN (Ret.), is Chairman of the Board of the Association of Naval Aviators and Vice Chairman of the Naval Aviation Museum Foundation. At the time of his retirement in 2010, he was Commander, Allied Joint Force Command Naples.

the inevitable proliferation of these types of systems to many other countries increases the threat to the maritime commons and to our allies and partners. A2/AD attempts to deny freedom of strategic mobility as well as the ability to hold any target at risk, anywhere and anytime within the denied battlespace. The response to these threats has to be multidimensional and provide the necessary "offense-in-depth" to hold all enemy capabilities at risk.

The Services have shown that they can work together in the air defense and strike warfare missions, but this has been accomplished largely through the use of uncontested rear area bases both afloat and ashore. How will the United States fare against an enemy that has learned the lessons of America's power projection advantages and is determined not to let us have that advantage in the future? I believe there are three aspects to this future challenge that must be examined to define the systems and architecture that will provide "networked, integrated, attack-in-depth" capabilities and ensure the force can operate in this new environment.

First Challenge: Countering the Missile Threat

A large salvo of ballistic and cruise missiles against our land and sea bases has the potential to deny us the advantages we have used in the past to win. The fact that launchers and delivery aircraft can be hidden deep in enemy territory far from our air/sea umbrella demands new capabilities to reduce salvo size and accuracy. In some cases, an adversary can leverage political and geographic factors to allow a mix of high- and low-tech systems to prevent U.S. forces from conducting "business as usual" air-centric intervention operations from nearby bases and seas. To counter this threat, persistent intelligence, surveillance, reconnaissance, and strike (ISR-S) systems will be required to operate at significant range from land and sea bases to counter efforts to inhibit freedom of navigation and to intimidate the adversary's neighbors.

Missiles provide a means to rapidly and reliably strike airfields, air and missile defense sites, and naval battle groups in the opening minutes of a campaign. For air bases and carriers, the missile strikes are designed to "paralyze" operations for several hours. This allows followup attacks by fixed-wing aircraft and/or cruise missiles to "annihilate" the bases/carriers before critical mission capabilities are brought back online. The key to countering the "paralyze first, annihilate later" doctrine is to operate from ranges beyond the effective reach of the follow-on systems. Systems such as the Air Force Long-range Strike Bomber (LRS-B) and the Navy Unmanned Carrier-launched Airborne Strike and Surveillance Aircraft (UCLASS) are keys to future success. They will enable us to originate far from the adversary's effective radius of action while holding his strategic systems at risk.

Furthermore, countering missile attacks will require dedicated network attack aimed to deceive, deny, disrupt, and destroy enemy networks. It will additionally require electronic and kinetic attack to disrupt targeting solutions on our ships and aircraft as well as enemy command and control. It will require ISR-S capable of locating transporter erector locators and bombers as they uncover, and then destroying them. If the salvo size can be reduced, leaker missiles can be defeated using theater, area, and point defense ballistic and cruise missile interceptors and directed energy weapons systems.

the fact that launchers and delivery aircraft can be hidden deep in enemy territory far from our air/sea umbrella demands new capabilities to reduce salvo size and accuracy

Disabling adversary bases will not be enough. We will need to track down and kill aircraft on the ground and ballistic missile support systems, which will require rapid, dynamic targeting enabled by persistent ISR-S and enterprise architecture. A dedicated and coordinated effort against these missile/aircraft systems will be required to allow operations against an A2/AD adversary.

Persistent deep strike capabilities are not in our inventory now in the quantities and with the capabilities needed, but the advent of survivable long-dwell systems are in the Planning, Programming, and Budgeting process. However, the requirements and networks for these systems have not been well articulated or particularly stable. Future warfare will demand that these systems operate in the deep battlespace and be capable of linking together with surrogate stand-in jammers, collectors, and weapons to achieve the attack-in-depth envisioned by the Service chiefs. They will have to be tightly coordinated and use each other's capabilities to avoid enemy defenses far from other supporting capabilities. Only then will we be able to hold the entire battlespace at risk. The requirements process for defining these systems must look to the future, not the past, as we bring new capabilities such as LRS-B and UCLASS online.

Second Challenge: Operating in a Highly Contested Electromagnetic Environment

ASB postulates reducing our dependence on satellite communications and Global Positioning System in the future warfighting environment. For systems operating near or over enemy territory, it will be important to find ways to hide or harden within the electromagnetic spectrum. The ability to bring groups of systems together to manage and fight the local tactical battle will be critical to survivability.

The use of self-forming network architectures, both line of sight and wide area networks using surrogate air-breathing satellites and point-to-point laser or radio frequency satellite communications, will be critical to maintaining our network advantage. Regarding missile defense, the battlespace is at risk if our networks cannot survive in this environment. There seems to be little progress in this area, and too many of our systems are unable to communicate with each other. The Office of the Secretary of Defense (OSD) and Services must agree on a communications architecture that provides wide-band and line-of-sight digital networks. Too many systems link into a "cloud"—one without lightning bolts—that has yet to be defined or developed. As new weapons systems have come on line, it has become quickly apparent that the communications architecture is woefully inadequate and well behind the weapons systems' development timelines. Network architecture and systems need to be agreed on and programmed now.

Third Challenge: Providing Long-range Strike against Time-critical Targets in Contested Battlespace

Our current processes in the Air Operations Center (AOC) and the Maritime Operations Center (MOC) rely on operational

command and control to make the correct weapons/target pairing assignment for a target and then deliver the effect. As we have seen in the above two challenges, these operations centers may not have the necessary communications, bandwidth, or reaction time to accomplish this mission in the future battlespace. To the extent that they are either at fixed sites or have large communications signatures, they may be at high risk of attack by enemy long-range precision weapons. We must look at how these tasks will be accomplished from survivable locations/platforms inside the enemy's observe, orient, decide, and act loop.

The future AOCs and MOCs must be tightly linked and able to pass control to forward local area battle managers. New ISR collection methods using time-stamped signal, electronic, electro-optical infrared, and other data will allow rapid target mensuration and prosecution of time-critical targets. Tactical data links must allow for collection, local compilation, and dissemination of the data to the systems within the network. Every system will be a sensor. Assignments to surrogates within the network for enterprise architecture, tactical-level computer network attack, and kinetic attack should be made within this local network. In deep battlespace, this can be done automatically between unmanned systems.

In the future battlespace, the AOC will provide a continuous flow of resources into the fight and *shift* the battle management tasks forward. Providing on-scene aircrew/systems with "mission-oriented orders" and trusting them to implement solutions and adapt as conditions evolve may be less efficient than the highly controlled operations we have conducted over the past two decades against weak opponents. But delegating these tasks forward will require far less real-time, long-range communication and is therefore more robust against enemy network attacks.

Conclusion

ASB is a timely and proper concept that the Services' requirements and acquisition authorities should embrace. To deliver ASB, the shortcomings highlighted above must be fixed soon. Most important will be to quickly define and fund our network architecture and systems. OSD and the Services must come together on this requirement in short order so we fight as a truly networked force.

As we develop our future systems, they will be designed with common functionality to create an attack-in-depth capability to counter the A2/AD threat. A Family of Systems (FOS) tightly integrated and synchronized will be the key to survivability, particularly in the deep battlespace patrolled by unmanned aircraft and surrogates. This FOS will be critical to solving the problems of missile defense, and time-critical targeting must be enabled by a flexible, hardened network that will enable the rapid dissemination of data and near real-time targeting.

Unmanned systems in the deep battlespace will be a critical part of the high-level strategy of providing "networked, integrated, attack-in-depth" capabilities that hold an adversary at risk. We must clearly define the requirement and how these future platforms will perform within the FOS. Too many divergent views currently exist on this requirement.

It will also be important that the concept be properly constructed and that a truly joint solution emerges that Congress understands and supports. As Representative Randy Forbes (R-VA) stated in his article in *The Diplomat*,[2] "Air-Sea Battle will remain incomplete without the enduring political and budgetary support of the Congress. Similar to the role it played in the early 1980s, it will be up to the Congress to ensure the shifting balance of power in the Asia-Pacific region is reversed by properly investing in the capabilities necessary to project power throughout the region." To gain the support of Congress, the ASB concept must be solidly vetted, wargamed, and funded. ASB is too important to the Nation to fail. **JFQ**

NOTES

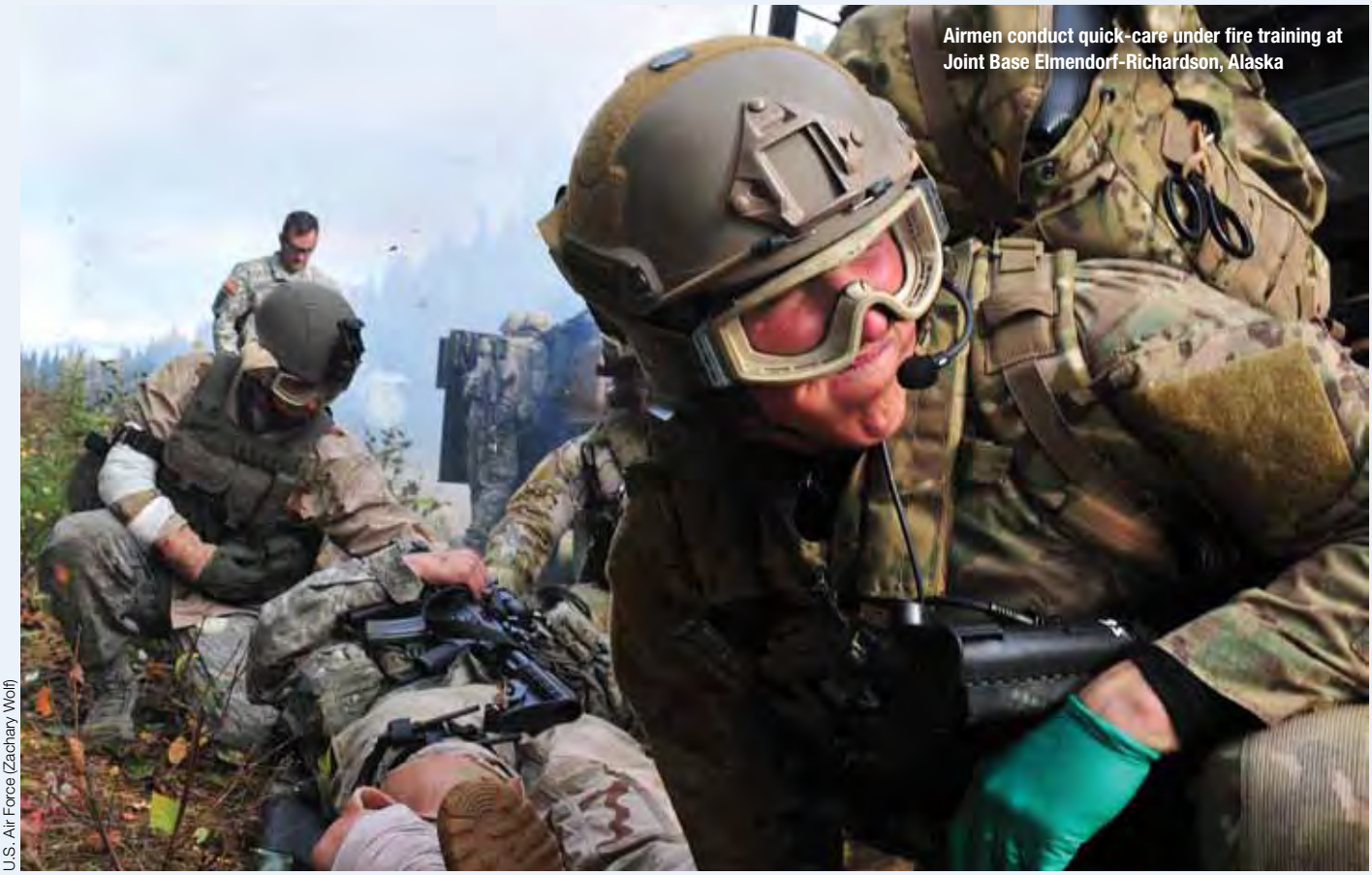
[1] General Norton A. Schwartz and Admiral Jonathan W. Greenert, "Air-Sea Battle Promoting Stability in an Era of Uncertainty," *The American Interest*, February 20, 2012.

[2] Representative J. Randy Forbes, "America's Pacific Air-Sea Battle Vision," *The Diplomat*, March 8, 2012.

U.S. Air Force (Jason Robertson)

California Air National Guard F-16s, exercise RIMPAC

Improving U.S. Posture in the Arctic



Airmen conduct quick-care under fire training at Joint Base Elmendorf-Richardson, Alaska

U.S. Air Force (Zachary Wolf)

By PETER OHOTNICKY, BRADEN HISEY, *and* JESSICA TODD

The United States became an Arctic nation when it purchased Alaska from Russia in 1867. Since then, the U.S. military has had a presence in this vast territory. Indeed, both the U.S. Army and Navy were responsible for administration of the territory in the course of its history. Alaska has been the site of World War II battles and Cold War conflict. Airpower pioneer Brigadier General Billy Mitchell went so far as to testify during 1935 congressional hearings that "Alaska is the most strategic place in the world."[1]

Until this point, the Arctic Ocean north of Alaska has been easily protected and of limited strategic importance due to the ice that has shielded it, impeding both access and use. Now the ice is melting, creating new opportunities and potential threats to U.S. national interests. This shift in the geopolitical environment requires prompt reexamination of U.S. military capabilities, roles, responsibilities, organizations, and command structure in Alaska. To ensure that U.S. national interests in the Arctic are met, the United States needs a realigned subunified command in Alaska that is empowered, resourced, and organized to coordinate the implementation of national and Department of Defense (DOD) Arctic strategy within the U.S. Northern Command (USNORTHCOM) area of responsibility (AOR).

Lieutenant Colonel Peter Ohotnicky, USAF, is Deputy Chief of Staff, Alaskan Command/Joint Task Force–Alaska, at Joint Base Elmendorf-Richardson, Alaska. Lieutenant Colonel Braden Hisey, USMC, is a Staff Officer in II Marine Expeditionary Force. Jessica Todd is the Multinational Experiment 7 Cyberspace Operations Lead in Joint Staff J7, Joint and Coalition Warfighting.

The Growing Importance of the Arctic

There is no universally accepted definition of what the Arctic is or where its borders lie. Generally speaking, the Arctic is predominantly an oceanic region plus the northern landmasses of its encompassing continents. More specifically, it can be considered the circumpolar region, including both marine and terrestrial systems extending southward from the North Pole, covering over 15 million square miles (about 8 percent of Earth's surface) and home to a population of about 4 million.[2] Territories of eight countries are within the Arctic: Canada, Denmark (representing the dependencies of Greenland and the Faroe Islands), Finland, Iceland, Norway, Sweden, the Russian Federation, and the United States. For a significant proportion of each year, these countries are "continentally" united by winter's spread of Arctic sea ice.

Sea ice has been a feature of the Arctic Ocean for at least 47 million years. According to best current estimates, there has been year-round sea ice in the Arctic for at least 800,000 years.[3] Nevertheless, the average size of the polar ice sheet in September—generally the time of the year when it is smallest—has dropped by more than 30 percent since 1979, when satellite records began.[4] In particular, the last 5 years (2007–2011) have had the five lowest September ice extents in the satellite record, and the thaw in 2011 was second only to the record melt in 2007 when 40 percent of the central Arctic Ocean became open water.[5] Owing to historical data extending back to 1880 that show recent years as being some of the warmest on record, predictions are that the Arctic will be free of summer ice by the end of the century. Moreover, current data suggest this could happen between 2020 and 2050.[6]

As the icepack shrinks, new opportunities for commerce and trade appear. In addition to making the few routes near shore navigable for a greater duration of the short Arctic summer, new sea lanes are opening. More abundant year-round ice had made these routes impassable, but in recent summers the annual ice melt has revealed new oceanic routes significantly shorter than traditional coastal Arctic lanes. Indeed, if predictions hold true that the polar icecap will completely disappear, then new sea lanes would traverse the North Pole itself. Irrespective of which polar sea lane is used, in comparison to a journey across more temperate oceans, routes through the Arctic are attractive because the distance traveled is significantly shortened.

For example, hugging the northern coast of Siberia is the Northeast Passage (the Russians refer to it as the Northern Sea Route). The voyage from the Dutch port of Rotterdam to Yokohama, Japan, along the Siberian coast, is about 4,450 miles shorter than the currently preferred route through the Suez Canal.[7] By trimming days off the trip and the associated savings in fuel costs, the inherent risks of Arctic oceanic voyages become increasingly outweighed by the progressive advantages of the disappearing icepack.

Along the northern coast of North America amid the Canadian Arctic Archipelago is a sea route known as the Northwest Passage, which connects the Atlantic Ocean to the Pacific. By using this route ships cut huge distances off their transits. Nevertheless, the Northwest Passage is not without controversy—Canada is concerned about its use and regulation.

The Canadian government considers the Northwestern Passage (a name also used for the Northwest Passage) part of Canadian Internal Waters, thus giving Canada the right to bar transit. However, most maritime nations, including the United States, consider the passage an international strait where foreign vessels—such as commercial or naval ships, planes, and submarines—have the right of "transit passage." The Northwest Passage is particularly enticing for massive supertankers too big to pass through the Panama Canal and must navigate around the tip of South America.

As the polar icecap melts, it not only creates new routes for transoceanic travel, but it also makes new international waters available for fishing. The Arctic Ocean is encircled by the littoral states of Canada, the United States, Russia, Greenland, and Norway. Waters within 200 nautical miles of shore are the Exclusive Economic Zones of these countries. In the center of that northern ring known as the "Arctic Donut," however, lies 1.1 million square miles of international waters—an area as big as the Mediterranean Sea—not currently governed by any international fishery agreements.[8] Unless an international agreement is completed, the region remains entirely open to the type of exploitation that severely depleted fish stocks in the Bering Sea in the 1980s due to unregulated fishing by Poland, South Korea, and Japan.[9]

The receding polar icecap also exposes more of the sea floor to exploration. By some estimates, the Arctic is believed to hold 15 percent of the world's undiscovered oil reserves and 30 percent of its natural gas.[10] As Arctic waters become increasingly used for trade routes and a source of offshore oil and gas deposits, enormous commercial interests are at stake. Concerns have been raised about the ability to respond to an oil spill in the Arctic—certainly a more difficult and technically challenging response than those confronted in open waters or in more temperate climes.

Canadian Armed Forces (Darry Veillette)

HMCS *Toronto* passes iceberg off Baffin Island during sovereignty patrol

In addition to commercial shipping, ecotourism must also be taken into account. The growing popularity of ocean travel and the desire for exotic destinations have led to increasing numbers of passenger ships in the polar seas. Any ship operating in the remote Arctic environment is exposed to a number of unique risks. The increased interest and traffic in this region and the unique operational, environmental, and search-and-rescue concerns peculiar to the area make rescue or cleanup operations difficult and costly.

No broad international accord covers the Arctic, unlike the Antarctic, which has an international treaty specifically governing its use. The Arctic's prevailing arrangement is via the umbrella treaty United Nations Convention on the Law of the Sea. This is a binding agreement ratified by 161 countries that empowers regulation of fisheries in international waters through regional agreements negotiated between countries. It has been signed by all Arctic nations except the United States. This unratified treaty and, more particularly, the lack of an international accord that governs ventures in the Arctic will continue to make the region and especially its international waters vulnerable to exploitation by far-ranging nations. The U.S. official position is that the Arctic does not need a specific overarching international accord—a position that affords greater sovereignty but also increases the risks associated with a lack of stability.

Notably, the eight Arctic nations do participate in a consultative body known as the Arctic Council, which is an intergovernmental organization exclusive to the Arctic nations but that also grants observer status to interested states, several indigenous tribes, and select or nongovernmental organizations. Its purpose is to provide "a means for promoting cooperation, coordination and interaction among the Arctic states, with the involvement of the Arctic indigenous communities and other Arctic inhabitants on common Arctic issues, in particular issues of sustainable development and environmental protection in the Arctic."[11] Founded in 1996 to address environmental issues, its scope has gradually broadened as the warming Arctic has created more opportunity. In 2011, the first legally binding accord was signed by the council's members. This new agreement is singular in scope: it simply coordinates search-and-rescue operations across the millions of square miles of ocean that are becoming more navigable as Arctic sea ice decreases. Although the Arctic Council creates an overall atmosphere of cooperation for the Arctic among stakeholders, it is important to note that, by charter, it does not address security issues.

Unsurprisingly, the increasingly accessible Arctic has attracted more attention from countries farther south. A warming Arctic is opening up new competition for resources that until recently were out of reach, protected under a thick layer of ice. Consequently, countries such as China are showing more than a casual interest in the Arctic. To illustrate, China has an unusually large embassy in Iceland and an Arctic science center on Norway's Svalbard Archipelago.[12] Recently, a large Chinese development company made a bid to buy land in Iceland to build a hotel development. The vast plot of land sought makes up 0.3 percent of the island's landmass, and raises suspicion of a Chinese attempt to gain a strategic foothold in Iceland as melting Arctic ice creates navigable inroads.[13]

China has an unusually large embassy in Iceland and an Arctic science center on Norway's Svalbard Archipelago

Even though the potential for armed conflict in the Arctic is low, the increased interest in the region could become a conduit for "strategic spillover," whereby conflicts that do not originate in the Arctic still affect it. As the Arctic becomes progressively more accessible, its importance will grow. As an Arctic nation, the United States has a range of enduring interests there and must ensure it is properly positioned to protect them.

In particular, DOD has a strong role to play because many nations are currently increasing their military presence in the Arctic, which in a broad sense is along American borders. Public statements and strategy documents indicate that other nations seek peace and cooperation as they expand their involvement and protect their sovereignty in the region. Meanwhile, military build-up is occurring at varying speeds, but there remains a shared singular focus of placing military forces forward into the Arctic. For instance, Russia's military has increased its air and naval patrols[14] and has established its presence in several ports. Russia has also contracted for a new fleet of icebreakers—three nuclear and six diesel—and is training specialized brigades to be based in the Arctic.[15] Similarly, Canada is establishing deep-water ports as well as naval and army bases dedicated to cold weather training. In August 2011, Canada held a military exercise in the north with over a thousand troops.[16] For its part, Denmark is coordinating with Greenland and the Faroe Islands on a North Atlantic operational command structure and is creating an Arctic Response Force.[17] Norway was the first country to move its military command leadership to the Arctic. These actions exhibit a military tendency northward for which the United States must prepare in order to protect its own national interests and be able to support its allies.

National Security Policy for the Arctic

The Department of State is the lead government agency for the Arctic, and strategic-level whole-of-government efforts are further coordinated through the Interagency Arctic Policy Group that was established in December 1971 by National Security Decision Memorandum 144. The group provides a forum for overseeing U.S. policy and for reviewing and coordinating activities in the Arctic.[18] Contemporary U.S. policy concerning the Arctic region was established in January 2009 in National Security Presidential Directive 66 and Homeland Security Presidential Directive 25. The policy recognizes the strategic importance of the region and directs implementation actions to protect U.S. safety, security, and economic interests. These actions include improving U.S. ability to protect its air, sea, and land borders and increasing maritime domain awareness capability in order to support commerce, critical infrastructure, and key resources. The policy also addresses issues such as governance, boundary lines, scientific research, energy development, environmental protection, and maritime transportation.[19]

The Unified Command Plan (UCP) 2011 was revamped to remove areas of responsibility in the Arctic from U.S. Pacific Command (USPACOM). U.S. European Command (USEUCOM) and USNORTHCOM now share responsibility for the region, with USNORTHCOM being the designated advocate for Arctic capabilities.[20] The realignment

streamlines what had been previously shared among the three combatant commands.

DOD Command Structure in Alaska—Historic and Current

During World War II, pivotal lapses in unity of command during the battle for the Aleutian Islands highlighted the need for a stronger, more cohesive approach to defense of the homeland regarding Alaska. Consequently, Alaskan Command (ALCOM) was stood up in 1947 under the Joint Chiefs of Staff to defend Alaska and provide humanitarian assistance throughout the region in the event of a natural disaster. A defense drawdown after the Vietnam War resulted in the piecemeal reassignment of Alaskan Command's responsibilities until the unit was eventually deactivated in 1975.

After a 1987 joint exercise underscored the disorganized defense effort in the region, ALCOM was reactivated in 1989. Headquartered at what is now Joint Base Elmendorf-Richardson in Anchorage, ALCOM is a subunified command under USPACOM that was given responsibility for the land and maritime defense of Alaska as well as all air missions not assigned to Alaskan NORAD (North American Aerospace Defense Command) Region (ANR), such as air rescue and other civil support. Its role was again modified when the September 11, 2001, attacks led to the 2002 creation of USNORTHCOM and its broad mission to unify command and control of homeland defense efforts and to coordinate defense support of civil authorities. To better manage its northern responsibilities, USNORTHCOM created Joint Task Force–Alaska (JTF-AK) and charged it with the mission "to deter, detect, prevent and defeat threats within the Alaska Joint Operations Area . . . in order to protect U.S. territory, citizens, and interests, and as directed, conduct Civil Support."[21] Through a Command Authorities Agreement between USPACOM and USNORTHCOM, JTF-AK is primarily manned and executed by ALCOM.[22] The outcome is that there is a single commander and staff that must report to two different combatant commanders.[23]

Most military forces in Alaska remain under USPACOM because of their focus on the USPACOM AOR. ALCOM's role as USPACOM's subunified command is coordinating all military activities in Alaska, and planning and conducting joint training for rapid long-range deployment missions in support of USPACOM. ALCOM's subordinate commanders include the commander, 11th Air Force, and commanding general, U.S. Army Alaska (USARAK). In total, forces in Alaska number more than 20,000 Army, Navy, Marine, and Air Force personnel, and 4,700 Guardsmen and Reservists—though only approximately 80 personnel from all military branches staff the "pooled" command of ALCOM/JTF-AK.[24] When commander, Alaskan Command, functions as commander of JTF-AK and ANR, he provides unity of command to USNORTHCOM for U.S. and Canadian forces and all of these missions in Alaska through his designation as commander ANR and JTF-AK. Thus, JTF-AK and ANR are the "Alaska equivalent" to the dual command of USNORTHCOM and NORAD for all of North America.

Also of importance is that the commander of ALCOM is the lieutenant general who commands 11th Air Force. He is additionally designated as the commander of JTF-AK and ANR. The Army's major general who commands USARAK is by design also the deputy commander of ALCOM and JTF-AK.

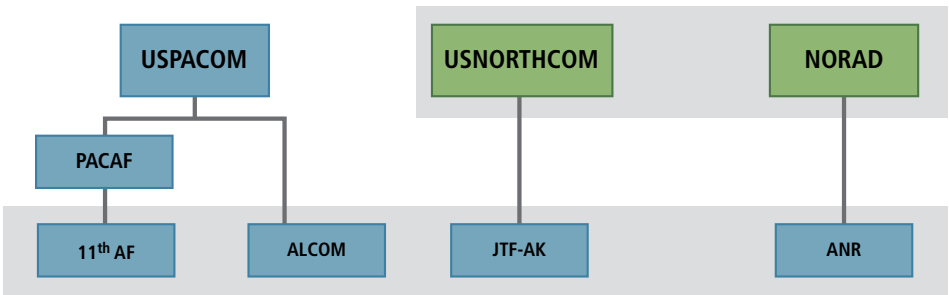
Operational Command for the Arctic

The history of inadequately organized operational command in Alaska is once again repeating itself. USPACOM retains the most clout in the region as the combatant command with authority over the joint headquarters (ALCOM) and the major operational forces stationed in Alaska (11th Air Force and USARAK) even though the 2011 revision of the UCP removed the Arctic from USPACOM's AOR. This limits USNORTHCOM's real authority in the region, thus hindering its responsiveness at the operational level to rising national interests in the Arctic.

The current UCP is an important evolution in the correct strategic direction because it reduced the division of responsibilities in the Arctic region. However, a significant seam is now obvious at the operational level when it comes to ALCOM and JTF-AK. Having a "pooled" headquarters working for two different combatant commanders violates the principles of simplicity and unity of command. It is true that ALCOM does have the important responsibility to support the USPACOM exercise and training program, and this mission cannot be discarded. However, the overall balance of strategic interests due to the rising importance of the Arctic requires a realignment of command arrangements for ALCOM.

The current command arrangement is not well postured to address the Arctic. USNORTHCOM's mechanism to conduct its mission in this region is the provisional JTF-AK—which contributes minimally to the resourcing of the joint headquarters—and thus JTF-AK is totally reliant on ALCOM to conduct its mission. In essence,

Figure 1. Current Command Structure



USNORTHCOM is dependent on USPACOM's goodwill when it comes to the Arctic. Meanwhile, USPACOM no longer has Alaska or the Arctic as part of its AOR, and thus the region is no longer part of its strategic focus. So there is a risk that national security interests in the Arctic will not be adequately met despite the fact that the ideal mechanism to address these needs already exists.

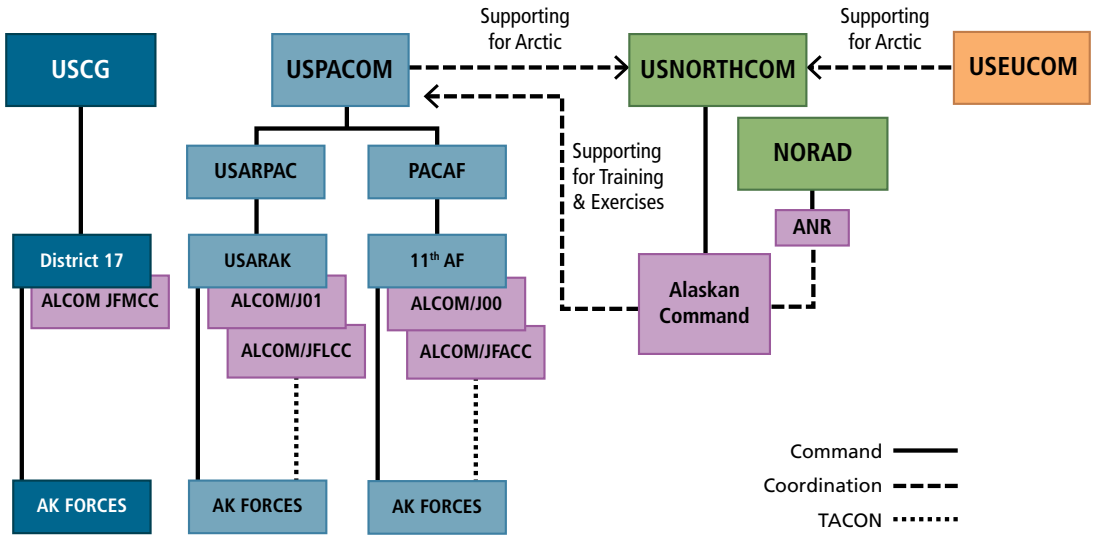
The problem can be resolved by dissolving the JTF-AK organization, assigning its responsibilities and resources to ALCOM, and then making this "new" ALCOM a subunified command under USNORTHCOM, while leaving forces in Alaska assigned to USPACOM. USPACOM should retain command over the forces in Alaska due to the possibility of significant, time-critical, major contingency operations that could occur in its AOR. This arrangement is appropriate since outright conflict is much less likely to occur in Alaska or the Arctic.

Reorganizing ALCOM under USNORTHCOM would make for a better arrangement to address national security interests. ALCOM would be able to serve as a true mechanism for joint operations in the Arctic, a capability that is currently lacking, according to the Congressional Research Service.[25] ALCOM is the joint headquarters in the region, with established relationships with the Service components in Alaska. It maintains a continuing focus on the Arctic and sponsors frequent joint exercises in the region. USNORTHCOM needs to fully command ALCOM in fulfilling its Arctic responsibilities since ALCOM is in an excellent position to identify these capabilities from a joint perspective.

Dissolving JTF-AK and aligning ALCOM completely under USNORTHCOM simplifies the joint command relationships in the region and makes them consistent with what one would expect from the UCP. This approach is also consistent with joint doctrine on subunified commands—which exist to "conduct operations on a continuing basis"—and JTFs, which are for "specific, limited missions."[26] Similar subunified commands exist in DOD. U.S. Strategic Command has a subunified command, U.S. Cyber Command, to centralize command of cyberspace operations.[27] Joint Special Operations Command, a subunified command of U.S. Special Operations Command, performs specific research, standardization, and planning tasks.[28] Perhaps the best analogies to a repositioned ALCOM are U.S. Forces Korea and U.S. Forces Japan; both are subunified commands under USPACOM with continuing responsibilities to defend the security interests of the United States and its allies in a specific geographic region.

A significant portion of the Arctic falls also within the USEUCOM AOR. Consequently, USEUCOM, and the North Atlantic Treaty Organization (NATO) along with it, have roles in ensuring the security interests of Western nations in the Arctic, especially vis-à-vis Russia.[29] Rather than a Brussels-based or Stuttgart-based military presence in the Arctic, the United States might be better served to have its military presence in Alaska, especially since its national policy is to "encourage the peaceful resolution of disputes in the Arctic region,"[30] and it is Alaska that makes the United States an Arctic nation. Canadian Prime Minister Steven Harper has argued against NATO involvement in the Arctic, noting that the push was coming from nations in Europe that want to exert their influence in the region but who are not themselves Arctic nations.[31] In short, NATO's involvement could complicate the achievement of U.S. national interests. USEUCOM should be the supporting commander to USNORTHCOM for the overall Arctic theater campaign strategy, which should be developed by and executed through ALCOM. Additionally, USNORTHCOM and NORAD already enjoy a close and longstanding relationship with Canada in defending the continent's northern border. The establishment of a strong joint force headquarters in Alaska with a particular focus on the Arctic strengthens the bilateral coordination with Canada already present in NORAD, and elsewhere, it sends an important message that the United States is ready

Figure 2. Proposed Command Structure



to defend its interests and fulfill its responsibilities in the region.

Roles for a New Alaskan Command

As a standing joint subunified command, Arctic- and Alaska-specific contingency planning would be the focus for ALCOM, along with answering the need for a comprehensive Theater Campaign Plan that addresses important issues such as military-to-military engagement with Arctic nations, security needs of native Alaskan peoples, maritime surveillance, and search and rescue. The unique operating environment of Alaska and the Arctic requires its own specific contingency plans for Homeland Defense and Defense Support of Civil Authorities, especially as compared to most of the USNORTHCOM AOR. The extraordinary challenges of operating in the Arctic and Alaska are plentiful: weather extremes of wind, cold, snow, and sea ice; daylong periods of darkness or light; harsh geography with mountains, glaciers, boggy tundra, volcanoes, and earthquakes; vast distances; electromagnetic interference; and lack of a robust infrastructure. This taxing environment makes maintenance and operation of equipment strenuous and demanding. It will fall to ALCOM to ensure the existence of, or advocate for, appropriate joint capabilities to function in this extreme environment.

The overall concept for this reorganized and realigned ALCOM is that it will be the focal point for a comprehensive and consistent effort to implement defense policy and address national security concerns in this unique region. When it comes to defense, the following organizations are currently stakeholders in Alaska and the Arctic: all four Services, USNORTHCOM, USPACOM, U.S. Strategic Command, USEUCOM, NORAD, NATO, the National Guard, and the Missile Defense Agency. Clearly, on the defense side alone, synchronizing efforts among all these organizations is difficult. The Arctic effort is substantially more complex when the whole of government is considered. The Department of State, the state of Alaska, local governments (especially on the north slope of Alaska), the U.S. Coast Guard (USCG), Bureau of Indian Affairs, Bureau of Land Management, and U.S. Customs all fulfill national security roles in the Arctic. The USCG is especially important since it is essentially the "maritime" component in the region on a persistent basis. (The territory defined by USCG District 17 is basically Alaska and its surrounding waters.) Fortunately, ALCOM already has relationships with many of these agencies. The realignment of ALCOM under USNORTHCOM, coupled with a mandate to implement national security strategy in the region, would be a significant step toward ensuring unity of effort for the Arctic.

The proposed rearrangement of ALCOM would be equivalent to other Arctic nations' joint headquarters in the north and would facilitate military-to-military coordination and engagement. Canada already has a significant presence in Alaska: the combined Alaska NORAD Region headquarters is collocated with ALCOM, and ALCOM/JTF-AK and Canada's JTF-North in Yellowknife frequently send observers to each other's exercises.

Alaska's 229 Federally recognized tribes are significant stakeholders in the Arctic. Unfortunately, environmental change, competition for mineral and fishing resources, increased shipping and tourism traffic, and the possibility of international conflict all threaten their ways of life. Some encroachment is perhaps inevitable, but our nation would do well to avoid the mistakes it made 150 years ago with native peoples in the western United States. The voice of indigenous peoples in the Arctic must be heard and their rights respected. Defense planning and joint operations must include special considerations of these tribes, as required by Executive order 13175.[32] ALCOM will remain postured to ensure this happens since this headquarters employs a full-time native liaison who is involved and engaged in planning and operations.

Maritime surveillance is another important role for ALCOM. Already, there is the long-established history of successful combined defense between the United States and Canada on airspace surveillance through NORAD. This relationship, along with its associated personnel and infrastructure, should be expanded to include maritime surveillance in the two countries' Arctic waters. The United States would especially benefit since the Canadians have already tested and deployed capabilities, including Radarsat satellites, sonar arrays, and surface wave radars.[33] The United States can bring the Broad Area Maritime Surveillance Unmanned Aerial Vehicle capability and develop a concept of operations for its employment in the Arctic region. Most important is the headquarters function to fuse the various sensor inputs to provide awareness to operational decisionmakers in the theater. The expansion of NORAD for maritime surveillance makes sense because a maritime threat for one nation is a threat for the other—threats which include adversary military presence, but also international smuggling, terrorism, and illegal fishing

F-16C Fighting Falcon lands at Eielson Air Force Base during exercise Distant Frontier and Red Flag–Alaska

U.S. Air Force (Christopher Boitz)

vessels. If Arctic nations do not exert their sovereignty in the region, other actors could seek to exploit the ungoverned spaces. ALCOM and ANR should begin working now with the U.S. and Canadian navies to begin to build this capability.

Another operational function for ALCOM to develop further is search and rescue. The primary agents for this mission are the USCG at sea, and the 11th Air Force Rescue Coordination Center, Alaska State Troopers, and local authorities on land. However, all agencies recognize that the U.S. military and even international countries will have important roles to play in a large-scale search-and-rescue incident in the Arctic. In 2011, the Arctic Council approved an accord establishing international search-and-rescue support in the Arctic.[34] This agreement is especially significant because it lists the USCG and DOD as the U.S. search-and-rescue agencies. ALCOM must continue to support, plan, and advocate for multilateral exercises concerning this important mission, particularly since international cooperation in this area can be an important means of building dialogue and trust in the Arctic.[35]

Conclusion

Although a joint headquarters exists in Alaska, it is not correctly organized and aligned to meet U.S. security needs. By bringing ALCOM into line completely under USNORTHCOM and empowering it to become DOD's primary operational-level headquarters for the Arctic, the United States would be better postured to address its national interests in the region. Although conflict in the Arctic or Alaska is unlikely, it is not unprecedented, nor can it be assumed away given the competing national interests in a region where homeland defense is not an easy task. Climate change, global economic trade, and energy demand have converged in the 21st century to bring a new level of activity to the region, along with a corresponding need to defend U.S. national interests. Clearly, the Arctic is entering a new era; an ALCOM subordinated to USNORTHCOM and vested with the role of sole Arctic coordinator will best carry U.S. interests northward. **JFQ**

NOTES

[1] U.S. Congress, House, Committee on Military Affairs, *Permanent Stations for Army Air Corps* (Washington, DC: U.S. Government Printing Office, 1935).

[2] United Nations Development Program. *Arctic Regional Human Development Report 2004*, accessed October 24, 2011, at <http://hdr.undp.org/en/reports/regionalreports/other/name,3262,en.html>.

[3] The Pew Environmental Group, *Arctic FAQ*, accessed October 24, 2011, at <http://oceansnorth.org/arctic-faq>.

[4] Katherine Leitzell, National Snow and Ice Data Center, *Summer Predictions for Arctic Sea Ice*, June 16, 2011, at <http://nsidc.org/ice-lights/2011/06/16/summer-predictions-for-arctic-sea-ice/> (accessed October 24, 2011).

[5] Ibid.; The Pew Environmental Group, *New Maps of Melting Ice*, accessed October 24, 2011, at <http://oceansnorth.org/new-maps-melting-ice>.

[6] "Climate Change in the Arctic: Beating a Retreat; Arctic Sea Ice is Melting Far Faster Than Climate Models Predict. Why?" *The Economist*, September 24, 2011, accessed October 24, 2011, at <www.economist.com/node/21530079>.

[7] Andrew E. Kramer, "Warming Revives Dream of Sea Route in Russian Arctic," *The New York Times*, October 17, 2011, accessed October 24, 2011, at <www.nytimes.com/2011/10/18/business/global/warming-revives-old-dream-of-sea-route-in-russian-arctic.html?_r=2>.

[8] The Pew Environmental Group, *Oceans North International*, accessed October 24, 2011, at <http://oceansnorth.org/international>.

[9] Ibid.

[10] "Climate Change in the Arctic," *The Economist*.

[11] Arctic Council Secretariat, *About the Arctic Council*, accessed October 24, 2011, at <http://arctic-council.org/article/about>.

[12] Helena Spongenberg, *Nordic Countries Get an International Voice in the Arctic*, June 23, 2011, at <www.norden.org/en/analys-norden/tema/the-fight-for-the-arctic/nordic-countries-get-an-international-voice-in-the-arctic> (accessed October 24, 2011).

[13] "Iceland and China: Hands Off Our Wilderness; An Ambitious Chinese Entrepreneur Spooks Wary Icelanders," *The Economist*, September 24, 2011, at <www.economist.com/node/21530165> (accessed October 24, 2011).

[14] Peggy Stolyarova, "Engage in the Arctic Now or Risk Being Left Out in the Cold: Establishing a JIATF-High North," thesis (Newport, RI: Naval War College, 2010).

[15] *Alaska Dispatch*, accessed October 18, 2011, at <www.alaskadispatch.com/article/russia-moves-bolster-arctic-military-presence>.

[16] Ibid.

[17] Arctic Council, "Denmark, Greenland and the Faroe Islands, Kingdom of Denmark Strategy for the Arctic 2011–2020," accessed October 20, 2011, at <http://arctic-council.org/filearchive/Arktis_Rapport_UK_210x270_Final_Web.pdf ()>.

[18] Henry A. Kissinger, *United States Arctic Policy and Arctic Policy Group*, National Security Decision Memorandum-144 (Washington, DC: National Security Council, December 22, 1971).

[19] George W. Bush, *Arctic Region Policy*, National Security Presidential Directive-66/Homeland Security Presidential Directive-25 (Washington, DC: The White House, January 9, 2009).

[20] Barack Obama, Unified Command Plan 2011 (Washington DC: Department of Defense, April 8, 2011).

[21] U.S. Northern Command, About *USNORTHCOM*, accessed November 3, 2011, at <www.northcom.mil/About/index.html>.

[22] U.S. Alaskan Command, *Joint Base Elmendorf-Richardson*, March 23, 2011, at <www.jber.af.mil/library/factsheets/factsheet.asp?id=5286> (accessed October 10, 2011).

[23] Ibid.

[24] "Alaska Command," *Techbastard*, October 18, 2011, accessed October 19, 2011, at <www.techbastard.com/afb/ak/ac.php>.

[25] Ronald O'Rourke, *Changes in the Arctic: Background and Issues for Congress*, Congressional Research Service Report for Congress (Washington, DC: Congressional Research Service, 2010).

[26] U.S. Joint Chiefs of Staff, *Joint Publication 3-0, Joint Operations* (Washington, DC: Department of Defense, 2011).

[27] U.S. Strategic Command, US *Cyber Command*, October 2011, at <www.stratcom.mil/factsheets/cyber_command/> (accessed October 25, 2011).

[28] U.S. Special Operations Command, *Joint Special Operations Command*, at <www.socom.mil/Pages/JointSpecialOperationsCommand.aspx> (accessed October 25, 2011).

[29] Sven G. Holtsmark, *Towards Cooperation or Confrontation? Security in the High North*, Research Paper (Rome: NATO Defence College, 2009).

[30] Bush.

[31] J. Barrera, "While Harper Talked Tough with NATO on Arctic, US believed PM All Bark No Bite," *APTN National News*, May 11, 2011, at <aptn.ca/pages/news/2011/05/11/while-harper-talked-tough-with-nato-on-arctc-u-s-believed-pm-all-bark-no-bite>.

[32] William J. Clinton, *Consultation and Coordination With Indian Tribal Governments*, Executive Order 13175 (Washington, DC: The White House, November 6, 2000).

[33] Jim Hodges, "Commanding the Arctic: Canada Leads Search for Surveillance Solutions," *C4ISR Journal*, March 2011.

[34] Arctic Council, *Agreement on Cooperation on Aeronautical and Maritime Search and Rescue in the Arctic* (Nuuk, Greenland: Arctic Council, 2011).

[35] Reginald R. Smith, "The Arctic: A New Partnership Paradigm or the Next 'Cold War'?" *Joint Force Quarterly* 62 (3d Quarter 2011), 117–124.

U.S. Air Force (Patrick Corkey)

United Alliance Delta IV medium rocket lifts off from Cape Canaveral carrying Wideband Global satellite to provide warfighter communications

SPACE *and the* JOINT FIGHT

By
ROBERT L. BUTTERWORTH

The world first saw the power of space to transform warfare in the 1991 Gulf War. In the years since, the U.S. military has come to depend heavily on space throughout its peacetime and combat operations. Satellites acquired by the Department of Defense (DOD) principally provide protected communications; data for position and timing, terrestrial and space weather, missile launch warning and tracking, and space situational awareness; and experiments and other research and development activities. Satellites for reconnaissance and surveillance are the domain of the National Reconnaissance Office (NRO), under the Director of National Intelligence (DNI).

Robert L. Butterworth is President of Aries Analytics, Inc., a space consultancy. He has held government positions in the Defense Department, the Senate, and the White House, and recently served Air Force Space Command as Chief of Strategic Planning, Doctrine, and Policy.

Today's capabilities emerged over five decades of changing technologies and threats, factors that are now forcing earlier plans for legacy systems to be reconsidered. Technology has extended space progressively deeper into warfare, while potential adversaries are developing capabilities that could extend warfare into space. The former demands finding new arrangements to provide tactical space reconnaissance; the latter demands seeing more clearly how space is essential to the emerging joint fight. Exploiting the advances in technology calls for new capabilities, authorities, and processes; countering the advances in threats calls for assessing architectures, plans, and options to set priorities for mission assurance.

decisionmakers must consider space not only as a component of existing capabilities but as an integrative enabler of the future joint fight

Mission Assurance

The mission that needs to be assured depends on what is needed for the joint fight, and is not necessarily a space system.[1] Some satellites enable terrestrial capabilities; some are integral components of those capabilities; some may protect those capabilities by denying enemy use of space; some may be important at first contact, while others contribute later. But, in every case, the measure of military merit and the significance of space is the contribution to the joint fight. The importance of space systems, like the importance of fighters, tanks, or submarines, derives from their role in winning the war—what General James P. Mullins, USAF (Ret.), called "the only truly meaningful measure of merit, enhanced combat capability."[2]

This measure establishes priorities for investment and protection. It also corrects the common but misleading demand that we build and maintain a space force "second to none," or "the best in the world." What is wanted, more precisely, is a military capability that can assure national interests against any and all attackers. Space can be essential to that capability, and what the space force needs to do is determined by how the U.S. military plans to fight the war, not by what other countries might build and launch. Whether that would also include war in space depends on the military context and how U.S. commanders plan to defeat the plans and capabilities of others.

That said, in practice, military space programs have been planned and acquired somewhat apart from the planning for future combat forces. For varied technical, programmatic, and bureaucratic reasons, they do not fit conveniently into the procedures by which conventional force acquisition plans are adjusted by anticipated resources. At any given time, therefore, there is likely to be only a rough synchronicity between development programs for space and those for other force capabilities. Particularly when reduced budgets bring program cancellations and stretch-outs, there are likely to be some space programs in which there is too much investment, others in which there is too little, and perhaps one or two that may be superfluous relative to the force development programs they are intended to support.

Deciding which space programs to cut, delay, or accelerate is not simply a matter of mirroring budgetary developments for major weapons programs. Space systems almost never serve a single need or customer, and they have often provided capabilities and met needs that were unanticipated when they were designed and launched.[3] Prudent decisionmakers must consider space not only as a component of existing capabilities but as an integrative enabler of the future joint fight. Cyber and drone technologies today, for example, are defining new military options that may supplant some legacy space functions, create needs for new ones, and compel new operational interfaces.

Because the mission to be assured is a joint fight capability, both mission assurers and potential attackers face the challenge of determining what the loss of a particular satellite would mean in combat. Links between specific space systems and specific combat support functions can be difficult to trace, and so can the terrestrial consequences of losing a satellite. Few satellites are single function, and their military role depends not only on the capabilities of the satellite but on the chain of ground stations, command and control nodes, and data processing and dissemination systems that make the satellite's capabilities relevant to the warfighter. Those capabilities can also sometimes increase, as when new ground processing techniques create new applications for existing sensors in orbit. Finding reliable alternatives to space can also be difficult; options that were initially expected to serve as substitutes for a space capability can be difficult to test and, in times of stress, may be quickly oversubscribed or prove to depend on other satellite links that are themselves vulnerable.

Synchronicity questions notwithstanding, military space is characterized by what the space systems can do in responding to military requirements to meet military needs under military exigencies in times of peace, crisis, and war. Consequently, the military needs assurance that those space systems providing uniquely essential help to the joint fight will be able to do so as long as needed, despite risks in the environment (collision, bursts of intense radiation), in design and fabrication, and from hostile action. Risk mitigation for environmental and engineering risks seems generally well understood (though problems still arise). Mission assurance is more heavily driven by developments in potential threats of hostile action. The military importance of space to U.S. forces makes space systems part of the enemy's target set. In recent years, potential adversaries have demonstrated antisatellite capabilities, including jamming, laser probing, and direct-ascent kinetic intercepts. Preparations for cyber assaults are certainly underway, and the longstanding possibility of scorched-space nuclear bursts cannot be ruled out.

When mission assurance does call for protecting space-based capabilities, the options today are the same four that were formulated by Amrom Katz almost 50 years ago: make them invulnerable, make them replaceable, make them invisible, or prepare them to shoot back.[4] The "invulnerable" approach can include hardening satellite subsystems and components against thermal and electronic interference and attack, but it also refers to constellations that can remain functionally capable despite the loss of some constituent satellites. Military space architecture could, for example, hedge the risks of satellite failure by deploying constellations of systems that provide redundancy for combat-critical functions. The architecture might be able to make use of satellites operated by other governments and commercial entities in a "virtual armada," involving the use of satellite data from allied and other government systems, preferably going beyond formal requests for

copies of imagery to obtaining direct combat support in time of need.[5] Some military sensors might become "hosted payloads" on commercial or foreign government satellites.[6]

The "replaceable" approach pursues the same goal, seeking to reduce the strategic advantage an adversary might gain from attacking specific satellites. The concept includes augmentation and may aim to provide substitutes or surrogates for particular functions, rather than entire satellites. One of the intentions behind the Operationally Responsive Space program (though not part of the program as executed) was to provide options for the rapid launch of militarily essential capabilities to augment, replace, or sustain peacetime systems.

Both of the other two options, "invisibility" and "shootback," are undeniably appealing for special applications and situations.[7] But mission assurance for combat support seems sure to require relatively extensive deployments of satellites in various orbits, which argues against either of these options becoming the preferred approach. Shootback would require deployment of additional capability for space situational awareness and command and control, while invisibility is not a viable option due to considerations of technology, cost, and utility.

In sum, lest dependence become a vulnerability, military space must evolve to the assured provision of uniquely essential space capabilities designed, acquired, and operated to enable combat effects that bring success on the battlefield. To find those requirements, planning for space will have to become closely integrated with force development planning overall, both internally within DOD and across the national security space enterprise.

Tactical Reconnaissance

New demands for mission assurance are one kind of strong pressure, forcing changes in planning for legacy systems; another pressure for change arises from advances in technology that can bring space-based reconnaissance and surveillance to the foxhole. These advances permit developing a capability that for present purposes can be called tactical reconnaissance—essentially "that kind of reconnaissance performed during combat (during the period of actual hostilities) in support of military activities which are neither those of the cold war nor those of the all-out central thermonuclear war."[8] The great challenge for mission assurance is threat assessment; the great challenges for tactical reconnaissance are organizations and authorities.

From the very early days, space-based reconnaissance and surveillance have been the purview of the National Reconnaissance Office, which was created to develop, acquire, and operate the Nation's "spy satellites." Conceived as a partnership between the Central Intelligence Agency (CIA) and DOD, the NRO's mission emphasized national intelligence programs—that is, topics of interest and concern to the President (and later, Congress). At the outset, top priority was given to collecting data for strategic intelligence, such as indications and warning of attack, foreign research and development efforts, weapons capabilities, and major force movements, and the technologies available at the time best suited those topics. Though there was hot competition between the CIA part of the NRO ("Program B") and the Air Force part ("Program A"),[9] their struggle concerned alternative management and programmatic options for accomplishing the NRO's mission, not the mission itself. Outside the national reconnaissance arena, the Navy and Air Force pursued space programs providing other military support (principally communications and weather).

an NRO satellite and a military satellite might collect the same data from the same target, but the data would be used by different customers for different purposes

By the early 1970s, advances in space reconnaissance technology led DOD to fund adjuncts and modifications that would make the national reconnaissance systems increasingly useful for tactical military operations. *Desert Storm* military operations against Iraq in 1991 made plain the success of those efforts.[10] Commanders quickly demanded more and better support from space, including broader and more frequent coverage, and more responsive command and control. The NRO, together with DOD and the Director of Central Intelligence (DCI), worked hard to address these and other military needs during the mid- to late-1990s, holding innumerable interagency meetings to set and review requirements, including validation by DOD's Joint Requirements Oversight Council. Still, the NRO, charged with meeting requirements established by the national intelligence community and also with providing military support, controlled the acquisition process, making the difficult "factory floor" decisions about sacrificing some promised performance goals to meet schedules and budgets. Those decisions seldom provided all the capability desired by defense interests.

To be sure, national intelligence priorities included support to military operations. Like spies and other intelligence assets, the national reconnaissance systems could and did provide data important to military planners and operators. But they were not themselves military capabilities, and the differences become acute in the tactical arena. An NRO satellite and a military satellite might collect the same data from the same target, but the data would be used by different customers for different purposes.[11] The military, for example, needs systems that can address multiple targets in strategic depth and that are resistant to enemy interference. National intelligence users often can be more patient and more selectively focused, and can depend on secrecy for both access and protection. While the complementarity can be extensive, the timeliness of data collection and the efficiency with which raw data are converted to actionable information are typically more important in military operations, while intelligence systems often need higher resolution. A representative problem for national intelligence users is collecting data that can help assess the plans, capabilities, and economic capacity of potential adversaries. A representative problem for military users is tracking enemy forces and determining fire control solutions. These different needs and priorities lead to different investment decisions, operational procedures, and designs for satellites and constellations.[12]

Even as technology advanced and offered more support for tactical military operations, authority to use that technology moved more under the DCI's control. In 1965, the NRO director reported to a three-person executive committee: the DCI; the President's scientific advisor; and the Secretary of Defense, as chairman. Each of these members could appeal directly to the White House for

redress for any particular decision. A decade later, the NRO director reported to a foreign intelligence committee chaired by the DCI. Another 10 years found the DCI overruling the technical decisions of the NRO director about the design of new programs. Moreover, the mid-1990s brought tighter budgetary control by the intelligence community staff, following the "forward funding" exposé triggered by construction of the new headquarters of the NRO.[13]

Tensions between national intelligence and tactical military needs have prompted several high-level reviews over the past 40 years, and each time the result has been what it is today: management rather than resolution, in the hope that "compromise and innovation" will continue to bridge the differences of view and perspectives. In 2001, the congressionally mandated "Rumsfeld Commission" recommended that "a successful approach to the organization and management [of national security space] must . . . [p]rovide methods for resolving the inevitable issues between the defense and intelligence sectors on the priority, funding and control of space programs."[14] Secretary of Defense Donald Rumsfeld's efforts to provide those methods, however, tried to reverse the tides of both technology and authority. Rather than trying to manage these long-recognized differences and trends through compromise and improvisation, Rumsfeld and staff set out to integrate fully the defense and national reconnaissance space programs. This leap into the past went nowhere beyond Pentagon press releases—DOD never fully integrated its own space programs, and the Intelligence Community simply said "no."

The NRO did, however, participate heavily in DOD's successive efforts to design a major new program: a radar satellite that would serve both national and tactical reconnaissance needs. Unable to overcome essential differences in shaping the first "Space-Based Radar" program, the Air Force renamed the effort and tried again with the "Space Radar" program. Both efforts collapsed, unable to find the technology that could integrate the incompatible military and intelligence requirements into a single program. The entire "black-white integration" effort, which sought to fuse the management of the national intelligence space programs under the NRO (the "black") with the military space programs of DOD (the "white"), then collapsed as well. This ironically proved what many supporters of the Space-Based Radar program had said earlier: the program "in fact, could become the poster child of horizontal integration development," that is, of black-white integration.[15] In 2005, a new director of the NRO was appointed, and, for the first time ever, the NRO director was not also appointed to be an Under or Assistant Secretary of the Air Force. Finally, in 2011, a new agreement between the Secretary of Defense and DNI, characterized as an "amicable divorce," further registered and formalized the distance between DOD and Intelligence Community space programs.[16]

These differences and divisions are thus not "management" problems, and management reforms cannot resolve them. Nor can they be obviated by reciting the solecisms of net-centricity.[17] They are rooted instead in the advance and expansion of space technologies in the service of two communities with core mission needs that diverge sharply. Yes, the national and tactical space reconnaissance systems can collaborate in many areas—national systems, for example, can help provide early information about enemy capabilities and dispositions, target selection, and battle damage assessment, while military space systems can support national reconnais-

Atlas V rocket transported to launch pad at Cape Canaveral carrying space-based infrared system satellite to enhance missile defense and detection capabilities

U.S. Air Force (Lou Hernandez)

sance and track potential threats (environmental and hostile).

But what they have not been able to do, and cannot do now, is field a single space system that meets the divergent operational needs of two communities with different core missions. For over 40 years, military leaders complained about having too little influence on the design and operation of the national reconnaissance space architecture. Their complaints were met with important but essentially marginal improvements. Now, after 50 years of national security space, the need is indisputable. Space systems are essential to virtually all military deployments and operations—particularly combat—and the earlier dedication to fielding only unitary programs under NRO control has reached an impasse.

Recognition of these differences and divisions was long resisted with solemn warnings that the Nation could not afford separate space programs for defense and intelligence. Lack of evidence never dinted the popularity of this bromide, but once space had become more fully integrated with military operations, it became clear that the Nation would pay a high price to keep pruning military needs to suit intelligence capabilities. As the Space (Based) Radar effort showed, forced union now could prove barren and impose costs in the most expensive terms: forgone military capability.

tactical reconnaissance will increasingly have to include space itself, as potential adversaries develop counterspace capabilities

For strategic planning, weapons development, overseas basing and deployments, international negotiations, and the like, the space systems serving military needs may be identical to those built for the national reconnaissance program. But what the military needs for combat is different from what the intelligence collector needs. The distinction is similar in some ways to that between a spy and a soldier—the spy's job typically requires remaining undetected and avoiding or escaping from shootouts, while the soldier's job may well require overt identification and the ability to win shootouts.

The realignment of responsibilities envisioned in the 2011 Memorandum of Agreement (DOD Directive 5105.23) might benefit both the spy and the soldier. The agreement does not balance defense and intelligence authorities; the NRO director remains the principal advisor to the Secretary of Defense on space matters, and authority for space matters within DOD remains fractionated and fractious (the primary aspirants may meet in a defense space operations council, which includes the NRO director; the council may make recommendations to the Deputy's Advisory Working Group, which in turn may make recommendations to the Deputy Secretary of Defense). But the new agreement might inspire military planners to develop a variety of space-based systems, stimulating competition in innovation and production and yielding advanced field capabilities enabled by less vulnerable satellites that were produced more efficiently, thereby enriching the space techno-industrial base that supports the national security community overall.

Yet the new arrangements seem unplanned, in these terms, and so could prove counterproductive. There is at present no visible initiative at the national level to ensure that sensible opportunities for cooperation and collaboration are pursued across the national space enterprise, that the consequences of particular decisions for other programs are taken into consideration, that timely action is taken to address emerging threats, and that the space programs collectively constitute a coherent contribution to the overall national security strategy. Parochialism could transform productive competition into useless duplication. Decentralization could encourage individual budget decisions that impose higher costs on the overall enterprise. Distributed authority could delay common action against common threats. Individual priorities could supplant national ones.

Proposals for collective management are probably not far away, if only because their absence presents a vacuum that Congress will naturally move to fill. To be expected are renewed calls for an executive committee similar to that of the 1960s, for joint committees and councils on research and common functional areas, for separate monolithic controls within the defense and intelligence space programs, for a national space council and/or strategy, for a Blue Ribbon review commission, and for special reports to Congress. Still, none of these procedural mechanisms promises a clear path to resolving the complex substantive issues at hand.

Acquiring capabilities to address the differences between national intelligence and military space systems, however, promises to be more than a bit complicated. Some desired attributes have long been evident in the shortcomings of the national systems "apps." Combat forces need to train and exercise with the systems they will need in combat; to share data across units and functional activities, including allies and other coalition partners, from which to draw a user-defined operating picture; and to know when and how well their requests for space support will be satisfied. How can the capabilities of advanced intelligence satellites be protected if the same technologies are providing tactical reconnaissance? In addition, tactical reconnaissance will increasingly have to include space itself, as potential adversaries develop counterspace capabilities. Broadly speaking, the extension of military competition to space will compel extensive development of two new architectures: one to provide intelligence preparation of the space battleground and continuing tactical reconnaissance of it, and another to provide the command and control systems to make use of the improved "space situational awareness."

Here again, as with mission assurance, planning for military space must become far more tightly integrated with other elements of force development, both internally to DOD and across the national security space enterprise.

Forces-based Planning

However the authorities and processes for military space are finally arranged, and while management options are being explored, DOD's space programs will be called on to show their military value to the future joint fight. At present, there seems to be no process within DOD that develops space requirements as part of planning the future joint fight, incorporates space as an integral part of development planning for combat forces, determines the space capabilities U.S. military forces would need to create the effects they would want to achieve, and reflects integrated plans for tactical operations, intelligence, technology, and space systems. Such a process would assess how space systems might

address problems and deficiencies in the joint fight, or how planned systems might be made more effective through new applications or integration of space data, or the cross-domain trades among new systems and technologies that might reduce dependence on space.

To start determining operational requirements, one might look back to the time between the World Wars, a period defined by rapid change in military technologies when the basis for operational requirements could not be distilled from experience of a major war. During those years, U.S. forces conducted several experiments to determine doctrine, organizations, and force structure, including the Navy's fleet experiments (how to use aircraft carriers), Mitchell's ship bombing, and the Army's Louisiana Maneuvers (mobility, how to use tanks). A series of experiments[18] or demonstrations or explorations might be undertaken today to help planners better understand several important operational issues. It seems reasonable, for example, to expect that different types of sensors would be important at different phases of conflict (zero through five, as well as subdivisions of each).[19] Presumably the need for and approach to mission assurance, including satellite protection, will change similarly. Perhaps, too, different approaches to command and control of the platform, the payload, data processing, and information dissemination might be better suited to different conflict phases and different space missions. Different sensor technologies, together with the nature of the mission, might affect the relative desirability of "direct downlink"—delivering sensor data directly to the warfighter—or of downlinking data to a central facility for processing and filtering before it is sent on to the warfighter. Experiments could also be used to check whether there might be some elasticity in initial data requirements (resolution, area coverage, frequency of revisit, and the like).

Another approach to determining some requirements is participation in combat "lessons learned" activities, and this approach could be used right away. The Center for Army Lessons Learned at Fort Leavenworth, for example, studies cases in which circumstances went badly for ground forces in Iraq and Afghanistan, with a view to recommending changes in tactics, techniques, and procedures (and sometimes more). Including space sensor and systems design engineers in this work might suggest different ways to get better combat outcomes by using different space systems, or different applications of current ones.[20] The intent here is not to evaluate the current activities but instead to involve space experts with specialists in tactical terrestrial operations.

Leadership for these activities seems best suited to U.S. Strategic Command. As the supporting command for regional wars being fought by geographic combatant commanders, it is well positioned to ensure a "joint fight first" approach to determining future space requirements. As the supported warfighting command for space and cyber, it already confronts the challenges of determining what cyberwar and space warfare might require, and how the powerful integration of space and cyber capabilities should be shaped.

space systems enabled a revolution in American military affairs; the military now needs a revolution in military space planning

In addition, organizational devolution and the increased specialization of space applications will require some mechanism in the national framework to foster collaborative as well as cooperative independent initiatives. At present there is no mechanism to integrate the planning and investment in satellite reconnaissance between the intelligence and defense communities across the national security enterprise. Moving toward an organizational resolution should probably wait until processes and programs for military space are further developed. But a manageable option to start now would be a national-level advisory board that has no formal authority but that has considerable influence and that reports to the Oval Office—a "President's Foreign Intelligence Advisory Board" for space. This group would examine space issues on its own initiative, perhaps to see whether important opportunities were being missed, and could also respond to government agencies' requests for help with difficult technical or bureaucratic issues.[21]

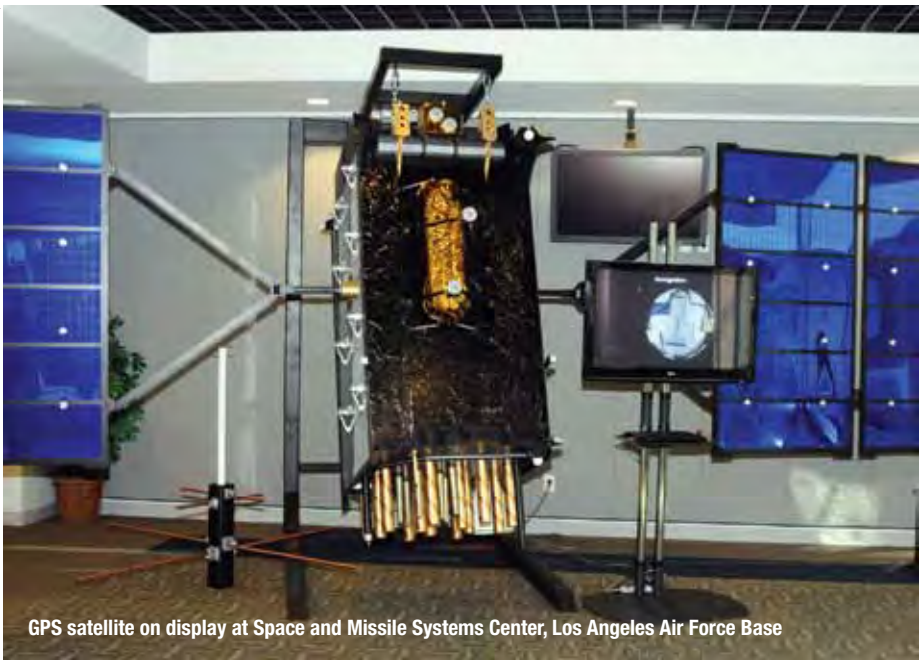
Conclusion

Space systems enabled a revolution in American military affairs; the military now needs a revolution in military space planning. What should a warfighting space architecture involve? Do military demands on space systems change in different phases of conflict? What functions must be maintained in wartime, and are they specific to particular satellites? If so, should the approach be to protect those satellites or to augment or replace them with new launches or with orbiting "silent spares"? What is the architecture that can ensure that data collected separately from intelligence and defense platforms will be shared to meet both intelligence and military needs? Furthermore, how can the coordination of availability and tasking be similarly ensured across both intelligence and defense platforms and needs? What steps should be taken first, and what resources will be needed?

For combat, the military space architecture needs to function in "real time" as part of a kill chain as well as to support intelligence preparation of the battlefield. It needs redundancy and resiliency to assure critical mission capabilities despite mishap or hostile action. It needs to be used in training, exercises, and coalition activities. Its design must therefore be rooted in the operations and development planning of the fighting forces, and it likely will require different satellites and architectures, an acquisition system that is responsive to the strategy, and new relationships among service, departmental, and national organizations. Achieving this will require developing methods to evaluate alternatives (for example, supplemental satellites vs. national reconnaissance components vs. remotely piloted aircraft vs. piloted aircraft) in terms of overall combat effectiveness. Making a military space architecture work effectively will require procedures and standards to ensure cooperative interfaces between military and other national security space systems and activities.

The military perspective, however, is still seriously underdeveloped. Mission assurance has been a constant concern, beginning with the earliest Corona launches. But deciding how to protect which assets against which threats has become highly complex because of the variety of potential threats today, the enormous challenge to earlier thinking presented by cyber warfare, the difficulty of tracing satellite functions to combat capabilities, and the perceived plethora of work-arounds and alternatives to space support. Tactical reconnaissance is similarly unformed: space programs for military reconnaissance and surveillance have largely entailed efforts to

U.S. Air Force (Jim Gordon)



GPS satellite on display at Space and Missile Systems Center, Los Angeles Air Force Base

extract warfighting support from systems designed for other purposes and operated by another community, and so to date they have been ancillary to force development plans and programs, even where the space contribution was important.

Three years ago the commander of Air Force Space Command called on the defense and intelligence space communities to shift from the "one size fits all" approach—"to shift from a suboptimized 'satellite, reconnaissance, intelligence, and warfighting, one each' approach—to a new architecture that accommodates the needs of both, with platforms that are purpose-designed for specific war fighter or national intelligence needs, and, in my view, that makes individual satellites more affordable and easier to produce."[22]

Answering this call is even more urgent today as national leaders look for ways to reduce budgets without sacrificing near-term military strength. Budget cutters can find space programs to be irresistibly attractive targets. Terminating or delaying these programs offers disproportionately large near-term savings compared with other major programs because so much of their life-cycle cost occurs during initial acquisition. Doing so is also appealing because it may have little or no effect on near-term military capabilities; acquisition of major new satellites can take years. Meanwhile, most legacy systems in orbit continue operating well beyond their expected design lives.

What makes space systems most vulnerable to budget sacrifice, however, is analytic vacuity—a continuing inability to explain military space in terms of enhancements to joint fight performance. Yes, the military space capability envisioned in this paper will require DOD to do more for mission assurance and tactical reconnaissance. Whether it will cost more than continuation of the legacy programs will depend on the results of future detailed assessments of space and the joint fight. But the first step is analysis, not procurement, and it is needed now. A continuing inability to explain military space in terms of enhancements to joint fight performance can only dim the prospects for military space systems and for making future combat forces as strong as they should be. **JFQ**

NOTES

[1] The National Space Policy 2010 issued by the White House embodied this approach to mission assurance, emphasizing the maintenance of mission-essential functions. See "National Space Policy of the United States of America," The White House, June 28, 2010, 9. The Defense Department and Intelligence Community's subsequent National Security Space Strategy (unclassified summary, January 2011) does not, however, and simply treats all space capabilities as equally important.

[2] James P. Mullins, *The Defense Matrix: National Preparedness and the Military-Industrial Complex* (San Diego, CA: Avant Books, 1986), 93.

[3] E.C. "Pete" Aldridge, while Under Secretary of the Air Force and Director of the National Reconnaissance Office, frequently responded to allegations that spy satellites were "gold plated" with the fact that "we have never flown capability that was not needed."

[4] Amrom H. Katz, "Preliminary Thoughts on Crises: More Questions Than Answers," mimeo., March 1972, 7.

[5] Beyond technical compatibility and operational familiarity, work on problems of legal, institutional, and domestic political relations at home and abroad would be needed at the outset.

[6] Indeed, government "departments and agencies" are directed to "work jointly to acquire space launch services and hosted payloads arrangements that are reliable, responsive to United States Government needs, and cost-effective" ("National Space Policy," 5). Geosynchronous commercial communications satellites might be useful as platforms for situational awareness, selected communications, research and development testing, or other purposes, depending on corporate business plans and fears of extortion. Better understanding of liability, technical compatibility, security, and related issues is needed. The Defense Department moved ahead with hosted payloads soon after the space policy was released (Turner Brinton, "U.S. Military Wants to Streamline Hosted Payload Process," *Space News*, September 24, 2010) and issued a solicitation for "Commercial Flight of DoD Space Test Program (STP) Hosted Payloads (HPs)," Solicitation Number BAA-SMC-SD-011, on November 23, 2011. Meanwhile, the Air Force completed work on the CHIRP (Commercially Hosted InfraRed Payload) and launched it in September 2011 (see, for example, "SES-2 satellite with USAF hosted CHIRP completes testing," December 22, 2011, available at <www.airforce-technology.com/news/newsses-2-satellite-with-usaf-hosted-chirp-completes-testing>). The continued interest in military hosted payloads was emphasized in the keynote address to the hosted payload summit delivered by Deputy Assistant Secretary Greg Schulte on October 4, 2011 ("Hosted payloads are one of the ways to assure space capabilities . . . [and] are one way the U.S. government might address impending budget constraints." Other agencies, of course, are pursuing these options as well; see, for example, "Hosted Payloads," in the *Space Commerce* publication of the National Oceanographic and Atmospheric Administration, Department of Commerce, available at <www.space.commerce.gov/general/commercialpurchase/hostedpayloads.shtml>.

[7] Even then, they can do virtually nothing against a total space negation attack. The United States has far more to lose than any other country if space becomes unusable; satellites and their products have become central to civil, scientific, and commercial activities, while providing critical force multipliers for military operations. A "scorched space" attack, not so unthinkable after the attacks

of 9/11, would hurt the United States more than any other country.

[8] Amrom H. Katz, "Some Ramblings and Musings on Tactical Reconnaissance," (Santa Monica, CA: RAND, March 1963), 1. As Katz went on: "If anyone wants to argue with this definition, let him write his own paper." The distinction between reconnaissance and surveillance is without effect on the subject of the present paper, and so references to space-based reconnaissance or tactical reconnaissance are intended to include surveillance functions as well. The distinctions are presented clearly in the Air University space handbook; see Brian Crothers et al., "U.S. Space-Based Intelligence, Surveillance, and Reconnaissance," chapter 13 of the *AU–18 Space Primer* 2d ed. (Maxwell Air Force Base, AL: Air University Press, 2009), available at <http://space.au.af.mil/au-18-2009/au-18_chap13.pdf>.

[9] Robert Perry, *Management of the National Reconnaissance Program*, 1960–1965 (Chantilly, VA: National Reconnaissance Office History Office, Second Printing, 2001).

[10] See remarks by then–Lt. Gen. Thomas S. Moorman, Jr., quoted in "The JDW Interview: Lt. Gen. Thomas S. Moorman, Jr.," *Jane's Defense Weekly*, February 9, 1991, 200. See also Robert L. Butterworth, "Space Systems and the Military Geography of Future Regional Conflicts," Report No. 14 (Center for National Security Studies, Los Alamos National Laboratory, January 1992).

[11] The GRAB and Poppy programs, while perhaps appearing initially to be exceptions, illustrate the point. For example, "Intelligence derived from the GRAB and Poppy systems supported a wide range of applications during the Cold War. It provided clues to locations and capabilities of Soviet radar sites, characteristics and locations of Soviet air defense equipment, ocean surveillance information for Navy commanders, and a more complete picture of the actual Soviet military threat." Crothers et al., "U.S. Space-Based Intelligence, Surveillance, and Reconnaissance," 175. Also see Dwayne A. Day, "A flower in the polar sky: the POPPY signals intelligence satellite and ocean surveillance," *The Space Review*, April 28, 2008, available at <www.thespacereview.com/article/1115/1>.

[12] "The important factor to recognize in this relationship [between strategic and tactical surveillance and reconnaissance operations] is that the function being supported determines if it is strategic or tactical, not the command that performs the mission or trains the crews. Neither is it the department nor agency that funds the platform." And later: "While the Air Force is satisfying the surveillance and reconnaissance needs of the Army, it must also do the same for its own forces and possibly for the National Command Authorities and strategic planners. Some of the information will be of use to all organizations, but it is a mistake to believe there is a high degree of overlap. The fine detail required for targeting weapons is unnecessary for strategic planning. The technical information required to satisfy a research and development question may go far beyond the needs of a combat soldier or airman who only needs to know what is where, when, and how many." See George E. Daniels, "An Approach to Reconnaissance Doctrine," *Air University Review* (March–April 1982), available at <www.airpower.au.af.mil/airchronicles/aureview_toc/AUReview1982/AUReview1982Mar-Apr.htm>.

[13] A former deputy director of the National Reconnaissance Office (NRO) summarized the event this way: "In 1995 the NRO had a funding crisis. The NRO was found to have accumulated $3.8 billion in forward funding (i.e., unused margin) across all NRO programs. The timing could not have been worse. The U.S. was involved militarily in Bosnia during a period of declining defense budgets. The discovery that a government agency had amassed $3.8 billion was greeted in Congress with both outrage and a sense of relief. There was outrage that the funds had been accumulated, but there was a sense of relief these newly identified funds could be reallocated to solve a funding gap related to ongoing military operations in Bosnia. At the same time, Director of Central Intelligence (DCI), John Deutch, publicly fired the incumbent NRO Director and Deputy Director (DNRO and DDNRO), and installed Keith Hall as the New DNRO with a mandate to get the NRO back on firm financial footing;" Dennis Fitzgerald, "Commentary on: Kohler's 'Recapturing What Made the NRO Great—Updated Observations on "The Decline of the NRO,"'" *National Reconnaissance: Journal of the Discipline and Practice* (2005), 59.

[14] Report of the Commission to Assess United States Space Security Management and Organization ("Rumsfeld Commission"), January 11, 2001, 79.

[15] "[Space-based radar], in fact, could become the poster child of horizontal integration development. The Air Force is grinding away on a concept of operations for space radar, and officials say they will get it right, with major implications for combat operations. 'The same radar wave front that is collected for intelligence information can be vitally important to the warfighter,' said [Under Secretary of the Air Force and Director of National Reconnaissance Office] Peter B. Teets." Robert S. Dudney and Peter Grier, "New Orbit for American Space Power," *Air Force Magazine*, February 2004, 43–44.

[16] Amy Butler, "USAF Eyes 'Disaggregation' for Future Sats," *Aviation Week and Space Technology*, April 25, 2011. The formal document is DOD Directive 5105.23, signed on June 28, 2011, by Secretary of Defense Robert M. Gates.

[17] As argued by, for example, then–Brigadier General Katherine E. Roberts, "Reflections on the Integration of Black and White Space," *High Frontier* 4, no. 4 (August 2008), 17–19.

[18] "If there is only one outcome, or if there are multiple outcomes but they are indistinguishable, the event is a demonstration, not an experiment. If the meaning of the outcome is determined only after the experiment is over, then it is an exploration, not an experiment." Brian McCue, "Wotan's Workshop: Military Experiments Before the Second World War," Occasional Paper, (Alexandria, VA: Center for Naval Analyses, October 2002), 4–5. Of similar interest is McCue, "The Practice of Military Experimentation" (Alexandria, VA: Center for Naval Analyses, February 2003), 5. An exercise is different still, and would be used for example to test the effectiveness or readiness of an operational force.

[19] The current lexicon includes six phases of conflict: shape, deter, seize initiative, dominate, stabilize, and enable civil authority. See Chapter III, Part C, of Joint Publication 5–0, *Joint Operation Planning*, August 11, 2011.

[20] One well-known example of improving space support is the Air Force initiative to mitigate the "sky-challenged" terrain in Afghanistan by providing quick access to more accurate GPS data, which significantly improved accuracy for the Small Diameter Bomb. See the account of Talon Namath by Brig. Gen. Jay Raymond, available at <www.marshall.org/pdf/materials/763.pdf>.

[21] This board of outside luminaries would be quite different from the Overhead Reconnaissance Advisory Group mentioned in the recent defense/intelligence memorandum, though the two certainly need not be incompatible. The Group as of mid-November had not yet held its first meeting.

[22] General C. Robert Kehler, commander, Air Force Space Command, notes for keynote address to GEOINT 2008 Symposium in Nashville, Tennessee, October 30, 2008. The gist of Kehler's remarks was reported in Colin Clark, "Intel, AF Sats Must Go Separate Ways—Kehler," *DoD Buzz*, available at <www.dodbuzz.com/2008/11/16/intel-af-sats-must-go-separate-ways-kehler/>.

Special operations forces sniper with ISAF provides security for road maintenance team in Kapisa Province, Afghanistan

U.S. Air Force (Joseph Swafford)

The Regional Special Operations Headquarters
Franchising the NATO Model as a Hedge in Lean Times

By **ARTHUR D. DAVIS**

In any problem where an opposing force exists and cannot be regulated, one must foresee and provide for alternative courses.

—Sir Basil H. Liddell Hart,
The Strategy of the Indirect Approach, 1954.

For better and worse, 2011 was a banner year for U.S. domestic and foreign policy in the fight against violent extremists. The United States saw the end of Osama bin Laden and North Korean's Kim Jong-il. Spring came to flower in parts of the Middle East, leading to the collapse of dictatorial regimes in Tunisia, Egypt, and Libya. The United States observed the 10th anniversary of the attacks of 9/11 while Congress debated the scope and size of cuts to discretionary spending in the wake of the largest budget deficit in history. The last combat troops crossed the Iraqi border with Kuwait, signaling the end of an 8-year campaign. And while these changes in many respects are promising, our nation still faces, in the words of Defense Secretary Leon Panetta, "a complex and growing array of security challenges across the globe."[1] Coupled with these complex and irregular threats is our rising national debt, which in itself creates a significant impact on our nation's ability to defend itself. The current fiscal reality will necessitate tackling these challenges with a military that is smaller in size and reorganized to capitalize on regional partnerships to share the security burden.

The Security Threat

As stated in President Barack Obama's June 2011 *National Strategy for Counterterrorism*, "the preeminent security threat to the United States continues to be from al-Qaeda and its affiliates and adherents."[2] The death of al Qaeda's leader in May 2011 did not reduce the threat of this far-flung organization. With affiliate organizations in the Pan Sahel, Horn of Africa, and Southeast Asia, and a growing interest in Central and South America, al Qaeda is a global hydra that threatens U.S. interests on all fronts.

Outside of the larger terrorist threat that al Qaeda inspires, countering the proliferation of weapons of mass destruction (WMD) and securing access to maritime trade routes are also areas of significant concern for the United States and its allies. With the distributed nature of these threats and the elusive hunt for terrorist leadership and support functions, Washington has acknowledged a greater-than-ever need to enable partner states to counter the threats. The 2010 Quadrennial Defense Review (QDR) highlights the need to "build the defense capacity of allied and partner states."[3] Such activities include multilateral and bilateral training venues, sales and financing of defense articles, and exchange and educational programs targeted at promoting greater capacity and capability to counter security issues. Important to note is the QDR's emphasis that "for reasons of political legitimacy as well as sheer economic necessity, there is no substitute for professional, motivated local security forces protecting populations threatened by insurgents and terrorists in their midst."[4]

The Budget Threat

Admiral Michael Mullen, former Chairman of the Joint Chiefs of Staff, said

Colonel (S) Arthur D. Davis, USAF, was the National Defense Fellow for Special Operations and Low Intensity Conflict Analysis at the Naval Postgraduate School during the 2011–2012 academic year and is assigned as Deputy Chief, Special Operations and Personnel Recovery Division, Headquarters United States Air Force, in Washington, DC.

in 2010 that the "single biggest threat to our national security is our debt."[5] The financial crisis and subsequent recession that came about in 2008 caused the Nation's deficit to spike significantly in the wake of emergency spending through stimulus programs, increased unemployment benefits and social expenditures, and the Troubled Asset Relief Program. In April 2011, as the Department of Defense (DOD) was working its fiscal year 2012 budget request, Secretary of Defense Robert Gates directed the Service Secretaries to identify more than $350–400 billion in spending cuts and efficiencies over the next 10 years.[6] While the Nation's recovery effort remained relatively flat, and with the coming end to major operations in Iraq and Afghanistan, DOD became a prime target for fiscal restraint as the administration tackled a nearly $1.5 trillion deficit.

Over the summer of 2011, Congress was forced to consider legislation to increase the debt ceiling to meet government outlays in the coming fiscal year. A compromise was reached in August that raised the debt ceiling while working to slow growth of the national debt: the Budget Control Act. One of the measures to curb the deficit was a requirement to cut projected defense spending by $487 billion over the next decade.[7] As he prepared to unveil his projected defense budget for 2013, Secretary of Defense Leon Panetta announced that he would meet this spending reduction by retiring older aircraft and ships, delaying several acquisition programs, and reducing the Nation's ground forces by 100,000 Soldiers and Marines.[8] With the size and scope of cuts to the defense budget over the coming years, now more than ever the United States must look to cooperation with friends and allies to ensure that security is not compromised in these lean times.

This article briefly examines past and present defense policy to frame the current emphasis on building and sustaining partner-nation security capacity. An examination of the newly formed North Atlantic Treaty Organization's (NATO) Special Operations Headquarters (NSHQ) will show that this organization is a regional partnership capable of conducting operations to counter terrorism and build partner-nation capacity in the defense of the NATO Alliance. As a case study, this article will apply the NSHQ model in the western Pacific to conduct military assistance, counterterrorism, and humanitarian assistance missions in a region of increasing importance to U.S. foreign and military policy. Special operations forces (SOF), through their regional focus and habitual training relationships with partner nations, are uniquely suited to these tasks. Franchising the NATO model of a coalition SOF headquarters with deployable air and ground forces can provide a hedge against declining defense budgets while ensuring that regional partners are vested in the collective security of their regions against nontraditional threats.

Defense Policy in Review

Past Quadrennial Defense Reviews have stressed the need to build and sustain forces capable of winning two major regional conflicts in overlapping timeframes against peer or near-peer adversaries. A large part of this strategy was formed as a result of the breakup of the Soviet Union. This strategy was designed to dissuade military entrepreneurship counter to U.S. and aligned international partners' interests either regionally or globally. This environment-shaping strategy involved military deployments, military-to-military contacts, and arms transfers and assistance programs to bolster partner-nation capabilities and reassure allies of U.S. participation in regional security. In these instances, the United States took more of a leading role both in terms of policy- and goal-setting and in providing substantial fiscal support. While the United States sought to address security issues through a multinational approach, the trend has been to play, in the words of defense analyst Carl Conetta, an "ever more prominent role as the convener, governor, and quartermaster of joint action."[9]

with the size and scope of cuts to the defense budget over the coming years, now more than ever the United States must look to cooperation with friends and allies

However, the current QDR emphasizes that "America's adversaries have been adopting a wide range of strategies and capabilities. . . . It is no longer appropriate to speak of 'major regional conflicts' as a sole or even primary template for sizing, shaping and evaluating U.S. forces."[10] In a recent *Joint Force Quarterly* article, Paul Davis and Peter Wilson emphasize that the distributed nature of today's threats requires the ability to "surveil, strike, punish from afar, and insert small, networked ground forces."[11] This strategy could certainly involve the use of SOF supported by capably trained indigenous forces and enabled by air and sea mobility and fires support as well as intelligence, surveillance, and reconnaissance assets. The challenge to planners at the Pentagon will be to find the right mix of more costly conventional deter-and-defeat resources and small, less-expensive networked forces that can engage in irregular warfare, counterinsurgency, stabilization, and humanitarian assistance mission sets, usually with other nations involved.

The European Model: Can an Answer Be Found in NATO?

The North Atlantic Treaty Organization came into being as a result of a rising and belligerent Soviet Union in the wake of World War II. Largely blossoming out of the Truman Doctrine of 1947, which sought to "support free peoples who are resisting attempted subjugation by armed minorities or by outside pressure," and fueled by the Marshall Plan, which provided funds to repair a war-torn continent, a transatlantic Alliance was formed to provide for a collective defense.[12] This "Transatlantic Bargain" encompassed 10 Western European states, Canada, and the United States and sought to counter Soviet expansionist ambitions while ensuring a stable security environment to bolster European democracy and foster economic growth.[13] Today, the Alliance includes 28 member nations. NATO also engages in security cooperation and multilateral initiatives with 37 countries from Eastern Europe, the Euro-Atlantic area, the Gulf region, and Asia.[14] The overarching premise for the Alliance revolves around a defense partnership to ensure collective security for Europe and the North Atlantic region. But outside of a few organic assets that include a command and control architecture and an airborne surveillance aircraft wing, NATO does not own its own military forces and relies on member states to provide them.

Following the collapse of the Soviet Union, many questioned the continuing need for NATO. However, throughout the 1990s, the Alliance became involved in

defense matters outside of their charter area to include operations in Bosnia and Kosovo. In the 1999 NATO Strategic Concept, Alliance political leadership stressed that future threats would be increasingly "multidirectional and often difficult to predict,"[15] thus opening the door for a defense strategy that lay beyond the borders of Europe. As of January 2012, NATO is involved in five ongoing missions to include stabilization in Kosovo, antiterrorism in the Mediterranean, counterpiracy in the Gulf of Aden, support for the African Union, and training and assistance missions in Afghanistan. It recently concluded Operation *Unified Protector* in Libya, implementing United Nations Security Council Resolution 1973 against Muammar Qadhafi's attempt to put down a popular uprising against his dictatorial regime.

as early as 1995, NATO realized that its special operations forces were inadequate for the security environment following the breakup of the Soviet Union

The Transatlantic Bargain—Redux

The Transatlantic Bargain between the United States, Canada, and the European member states has been renegotiated several times since the Alliance's inception. Throughout these incarnations, the United States shouldered much of the burden for defending Europe from possible Soviet aggression. But over the next 40 years, Washington saw a more capable military emerging from the ashes of War II and sought to have NATO shoulder more of the burden for its own defense. As the Cold War ended, the greatest threat to the Bargain was how the Allies would work together to share the security burden beyond NATO's borders. During the 1990s, many nations sought to capitalize on the "peace dividend" that followed the loss of the greater Soviet threat, and individual defense spending plummeted.[16] Though the Alliance did engage in several operations during this period, the majority of the heavy lifting was accomplished by the United States both in terms of equipment and in manpower. In fact, as highlighted in Defense Secretary Robert Gates's last address to NATO before leaving office, the United States provides 75 percent of NATO's budget, up from 50 percent during the Cold War.[17]

As NATO prepared for its 2012 summit in Chicago, the topic of collective defense—supported both with resources and with resolve—promised to be prominent in the discussions. Previous iterations of the Transatlantic Bargain involved a very active U.S. role in terms of assets and capabilities. Burden-sharing among the member nations has always been a stated objective. However, while the United States saw this as a contract that involved each nation doing its part, most European countries saw this as a compact that did not translate necessarily into a specific commitment.[18] Today's Bargain will be more about restructuring the current arrangement to emphasize new and evolving threats from transnational terrorism, cyber attack, and weak and failing states without a leading U.S. role. While the United States will never abandon the Bargain, it is clear that NATO should continue to prioritize future security objectives and develop a clear path to resourcing them. NATO Secretary General Anders Fogh Rasmussen's "Smart Defense" approach to burden sharing is a good start.

Smart Defense

Secretary General Rasmussen, recognizing significant decreases in defense spending among member nations, stated that a fundamental challenge facing Europe and the Alliance is "how to avoid having the economic crisis denigrate into a security crisis."[19] Throughout the past decade, member nation defense spending has fallen to roughly 1.7 percent of gross domestic product as compared to the current U.S. level of 4.8 percent. These numbers could continue to decline as austerity measures force further belt-tightening across the Alliance. Rasmussen stressed that the threat of terrorism and failed states will only increase and that investing in homeland defense and retrenching will not counter these threats.[20]

The Secretary General's Smart Defense approach is about "building security for less money by working together and being more flexible while encouraging multinational cooperation [and] combining resources to build capabilities that can benefit the Alliance as a whole."[21] This approach has already proven itself in the form of the long-standing airborne surveillance capability the Alliance operates through the NATO Airborne Early Warning and Control Force and through its newly formed Heavy Airlift Wing consortium, which employs a fleet of shared C-17 transport aircraft in Papa, Hungary. In 2006, the Alliance embarked on a NATO SOF Transformation Initiative (NSTI) to standardize another critical enabler of Alliance security in this time of unconventional threats.

NATO SOF Headquarters: The Vision

As early as 1995, NATO realized that its special operations forces were inadequate for the security environment following the breakup of the Soviet Union. In Bosnia and Kosovo, SOF were either not assigned to the overall commander or were working in a stovepiped arrangement that disallowed unity of effort on the battlefield. NATO SOF were again deployed to provide counterterrorism support for the 2004 Olympic Games in Athens but were not under a unified command and control structure or part of the overall intelligence architecture, instead reporting back through their own national command structures. And in 2006, as part of the International Security and Assistance Force (ISAF) in Afghanistan, significant differences in SOF capability and interoperability, as well as a dearth of special operations capable aircraft, led the NATO Military Committee to look for a solution.

During the NATO Riga summit in 2006, ministers of defense from 23 countries agreed to form NSTI, which would create a NATO SOF Coordination Center (NSCC). This center would be responsible for increasing each member nation's SOF ability to train and operate together as well as standardizing and improving equipment capabilities with the United States, as the Framework Nation.[22] In March 2010, the NSCC was reflagged as a headquarters and placed under the command of a 3-star general or flag officer reporting directly to the Supreme Allied Commander. Though still in its early stages of development, the NSHQ will eventually provide NATO senior leadership with a mature allied and partner network of SOF able to rapidly generate a special operation ground task unit with organic command, control, communications, and intelligence assets.

NSHQ is designed to provide a coherent long-term stewardship and direction for member nation and allied SOF. The missions expected to be conducted by SOF trained and led by NSHQ include direct action, either unilaterally or as part of a larger conventional force, military assistance to partner nations and other security forces outside of Europe, and humanitarian assistance following natural disasters anywhere in the world. To accomplish these missions, the headquarters seeks to move beyond the current ad hoc construct into a partnership that transforms these multinational SOF units from acquaintances to kinship. The "failure is not an option" political demand of many SOF missions requires a high degree of cohesiveness among both maritime and ground forces and their aviation enablers. This has led the commander, NSHQ, Lieutenant General Frank Kisner, USAF, to recommend both an increased deployment capability for NATO ground SOF and a standing air operations capability.[23]

the current reality within NATO is that no one nation possesses the capability to conduct the full scale of SOF missions unilaterally in an environment of uncertainty and unconventional threats

From Vision to Reality

From the outset, the headquarters primary lines of operations were to advise NATO leadership on matters related to the employment of capable special operations forces and coordinate and synchronize force generation and development of tasks in support of NATO operation; and to enhance interoperability and standardization through a Federation of NATO SOF Training Centers.

To execute this vision, the headquarters maintains a staff of 149 officer, enlisted, and civilian personnel drawn from the 23 participating nations under a memorandum of understanding (MOU).[24] Based in Mons, Belgium, NSHQ fulfills this first line of operation by providing ongoing assessments of member and partner-nation SOF participating in the ISAF special operations training mission in Afghanistan. NSHQ also provides in-garrison and deployable assessment teams to advise member nations on improving special operations capabilities from the tactical to strategic level. Lastly, the command maintains an ever-expanding NATO secure communications network to ensure connectivity and intelligence sharing across all of NATO SOF. In the future, NSHQ will form the core of a combined joint special operations component command able to field a deployable joint special operations task force headquarters to provide command and control of SOF either independently or as part of a larger NATO mission to ensure unity of effort and execution.[25]

However, as important as the primary line of operation is to the evolution of deployable and capable NATO SOF, the second tasking, providing standardization and training, is the command's current focus. The NATO SOF Training and Education Program, based at nearby Chièvres Air Base, provides a course of instruction that includes the doctrinal employment of SOF as well as programs in such areas as intelligence, forensics, air operations integration, and technical exploitation. The command is diligently working to increase this training capability by adding course offerings from among the partner nations' civilian and military academic institutions as part of a training federation. To ensure that SOF activities are standardized, NSHQ has authored the Allied Joint Doctrine for SOF, Allied Command Operations Force Standards for SOF, and SOF Evaluation as well as manuals and handbooks covering a range of topics to include special air warfare, SOF task group architecture and employment, and medical concerns for SOF. None of these existed prior to the arrival of the NSHQ.

As the Framework Nation for NSHQ, the United States supports the lion's share of the fiscal and personnel burden for this headquarters. Though the member nations are responsible for sharing costs, Washington maintains a vast majority of the budget responsibility through U.S. Army and U.S. Special Operations Command (USSOCOM) lines of accounting. NATO common funding is not assured and must be requested on a case-by-case basis. USSOCOM remains committed to the continuing evolution of NSHQ and will assume all responsibility for funding the U.S. portion of the contribution account in the coming years. Additionally, USSOCOM is seeking to expand both the training mission and deployable SOF architecture within NATO in an effort to expand their SOF network.[26]

As all of the NATO partners face resourcing constraints, a comprehensive SOF resourcing model epitomizes the NATO Secretary General's Smart Defense initiative. The current reality within NATO is that no one nation possesses the capability to conduct the full scale of SOF missions unilaterally in an environment of uncertainty and unconventional threats. The NSHQ and its mission to standardize and train SOF to work jointly follows the SOF truth that emphasizes that capable SOF cannot be created after emergencies occur. By creating joint employment doctrine; standardizing training, tactics, and procedures; and promoting a true culture of interoperability and unity of command, NSHQ is working to field capable NATO SOF for any contingency or military assistance mission. The benefits of interdependence among NATO SOF units should include enhanced worldwide mobility and operational proficiency in all NATO missions. With U.S. support, NSHQ will include capable air component enablers that will habitually train and deploy globally with ground and maritime forces.

Application: The Pacific

The administration's shift to a more Asia-centric foreign policy was extremely evident in the November 2011 East Asia Summit. President Obama attended it for the first time since he came to office. The summit, consisting of the traditional Association of East Asian States (ASEAN) plus Russia, Australia, China, India, Japan, South Korea, and New Zealand, is primarily a forum to promote security and prosperity in the region.[27] Asia-Pacific is becoming more and more crucial to the United States as its own economy continues to stagnate while China, India, and several other nations in the area continue to grow. While past administrations have had episodic participation in trade and security dialogue in the region, the Obama administration has placed ASEAN-led institutions such as the East Asian Summit and ASEAN Regional Forum (ARF) at the heart of its foreign policy agenda in Asia.[28] Secretary of State Hillary Clinton, in a recent article in *Foreign Policy*, noted that the "United States has emphasized the importance of multilateral cooperation,

for we believe that addressing complex transnational challenges of the sort now faced by Asia requires a set of institutions capable of mustering collective action."[29]

A Trans-Pacific Bargain?

Over the past decade, the region has increased collaborative efforts to counter transnational terrorism. Although no NATO-like entity exists, the ASEAN Regional Forum has taken on a greater security dialogue, and traditional U.S. alliances with powers such as Australia and Japan have strengthened and sought new members to form a collective security environment. Many nations have significantly increased their defense spending, with China and India being the most notable. Though trade is still at the forefront for most efforts in the region, securing trade routes, environmental and resource security, combating piracy, the risk of weapons of mass destruction proliferation, and countering extremist elements have risen to the top of most agendas.

Early in the evolution of ASEAN, many of its members were militarily aligned to Western governments stemming from precolonial arrangements or other bilateral agreements. Internal security cooperatives among several ASEAN states existed but were primarily bilateral and meant to secure shared borders. With the collapse of the Soviet Union, ASEAN, like NATO and the European Union, adjusted to a security environment that was more nebulous than that of the previous two decades. With a nuclear North Korea and the Taiwan Strait as potential flashpoints, and China's rising military and economic power countering a waning Japan and distracted United States, ASEAN was forced to look at developing a more formal security arrangement. The ASEAN Regional Forum was established in 1994 to form a single East Asian security agreement aimed at addressing the numerous security concerns in evidence after the Cold War and ensuring that the United States remained engaged in the region.[30] The forum thus formed the underpinnings of an arrangement or bargain structure similar to what the United States maintains with NATO. Though not specifically stated, this "Trans-Pacific Bargain" was the necessary first step toward a regional military cooperative that is still evolving.

The U.S. experience in NATO over the past 60 years can prove a useful point of departure when looking at a Trans-Pacific bargain. Like NATO, ASEAN shares a common sense of regional values and norms. By seeking to carry these into a security regime, the ASEAN Regional Forum should avoid the identification of a singular threat that characterized much of NATO's existence vis-à-vis the Soviet Union. This forum represents an opportunity to extend ASEAN's distinctive cooperative security and political culture of noninterference, equality, and sovereignty to all Asia-Pacific nations as the only multilateral forum covering the region with a clear security role.[31] Within the forum, the larger powers, China, Japan, and the United States, although they are members, have ceded formal leadership to the ASEAN nations, reflecting the necessary independence and regional importance of their continued support to a more stable security environment. Though the United States still maintains many bilateral agreements with members of ASEAN, the importance of supporting a larger security construct like the ARF in the form of a SOF-centric multilateral coordination and advisory organization cannot be overstated.

a comprehensive SOF resourcing model epitomizes the NATO Secretary General's Smart Defense initiative

The Pacific Regional Special Operations Headquarters

As demonstrated in Afghanistan, SOF are uniquely suited to partnering with conventional security forces. Special operations forces are traditionally a more mature capability that is inherently joint in nature and able to exploit multiple facets of any combat environment. These forces are utilized in wide-ranging roles and missions to include training and advising local security forces, setting conditions for successful humanitarian assistance missions, and performing direct action raids and special reconnaissance to counter WMD proliferation or irregular threats. The Defense Department is currently reviewing its military posture and options worldwide and will seek to add greater strategic depth across the Pacific region.[32] While there is a permanent or rotational presence of U.S. forces in the region, SOF presence remains relatively small by comparison under the command and control of Special Operations Command–Pacific (SOCPAC).

Although SOCPAC helps orchestrate the training and operations of several national SOF units, it is a U.S.-led, manned, and resourced headquarters. The SOF assigned to the command routinely interact with regional partners. However, there is not a significant number of partner-nation personnel assigned to SOCPAC, and the assigned personnel usually function in a liaison capacity. Taking the next step toward a truly integrated partner-nation SOF construct along the lines of NSHQ would provide forward basing of U.S. SOF in nontraditional areas with a greater array of partners to share the security burden. In terms of perception and legitimacy, a regional partnership in which the United States is an equal partner vice leading entity will ensure that each member gets an equal say in security policy and execution. The regional SOF headquarters will ensure standardization and manage redundant assets. By producing common training practices, ensuring equipment commonality, and reducing the number of forces and capabilities that a nation must produce and maintain, the headquarters will allow many nations to have a greater involvement in regional security concerns without shouldering the financial burden of a standing professional special operations component.

Making It Work

As in Europe, Central and South America, and the Middle East, U.S. SOF maintain a continuous presence in the form of a Theater Special Operations Command in the Pacific. SOCPAC provides a lean but potent SOF land, maritime, and air capability to assist in meeting the component commander's regional security requirement. However, in contrast to NATO, the ARF as a group is not as mature militarily, making any cooperative military venture a tenuous proposition at best. But the United States has a long tradition of bilateral security and assistance relationships with many ASEAN and regional partners that can aid in furthering this security construct by acting as a bridging agent between the states. Fostering a culture of military cooperation among SOF and other regional security forces can bring these forces together and eventually meld them into a cooperative working arrangement for the greater security good. USSOCOM is working diligently to increase

their forward presence to gain access to a global SOF network of capable allies and the Pacific region is the next logical area in which to focus. Establishing a regional SOF coordination entity or headquarters structure along the NSHQ model would further this effort. Though this might seem counterintuitive to the "ASEAN Way" of conflict management and regional security norms,[33] transnational and unpredictable threats to regional security have brought more focus on developing a security community not unlike NATO. Through the creation and sustainment of a training entity, nations that might have not normally worked together could join their efforts for the common good with the United States in a supporting vice supported role.

This indirect approach is not necessarily new. U.S. SOF have been present across the globe for decades providing advice and assistance to partner-nation forces. In any given year, USSOCOM conducts military assistance engagements in more than 70 countries. These persistent engagements strengthen our partners and aid in the creation of a hedge against unforeseen threats. Yet there is more that can be accomplished by expanding this to include multiple partners in a combined effort to increase security capital across a region. "Burden sharing" has been a part of the political and military lexicon for decades. However, with shrinking defense budgets and a threat environment more suitable for smaller, networked special operations forces, the United States should look to redefining its concept of burden sharing with an eye toward building truly capable partners that can act with or without significant U.S. support.

By leveraging a combined SOF headquarters able to organize, train, equip, and possibly deploy special operations forces to combat regional threats or provide humanitarian assistance and civic action, the United States can maintain a forward presence and assure its partners and allies that it will not allow belligerent actors or nations to impinge on the freedoms we all expect in a democratic world. Admiral William McRaven, USSOCOM commander, testified before the House Armed Services Committee recently that "the future of USSOCOM is building up the Theater Special Operations Commands and regional special operations networks."[34] SOF is representative of what the Defense Secretary calls for in his latest defense initiative to "develop innovative, low cost and small footprint approaches to achieve our security objectives."[35] **JFQ**

NOTES

[1] Secretary of Defense Leon Panetta, "Statement on Defense Strategic Guidance," press conference, Pentagon, Washington, DC, January 5, 2012.

[2] The White House, *National Strategy for Counterterrorism* (Washington, DC: The White House, June 2011).

[3] Office of the Secretary of Defense (OSD), *Quadrennial Defense Review Report* (Washington, DC: OSD, February 2010), 26.

[4] Ibid., 27.

[5] Travis Sharp, "The Sacrifice Ahead: The 2012 Defense Budget," Center for New American Security, February 2011, available at <www.cnas.org/2012defensebudget>.

[6] Major General Duane A. Jones, HAF A4/7, address, Air Force Fellows Orientation, Washington, DC, August 5, 2011.

[7] David J. Berteau and Ryan Crotty, "Super Committee Fallout and the Implications for Defense," Center for Strategic and International Studies, December 2, 2011, available at <http://csis.org/print/33923>.

[8] Elisabeth Bumiller and Thom Shanker, "Pentagon Plan Includes Base Closings and Smaller Raises," *The New York Times*, January 26, 2012, available at <www.nytimes.com/2012/01/27/us/pentagon-proposes-limiting-raises-and-closing-bases-to-cut-budget.html>.

[9] Carl Conetta, "The Pentagon's New Mission Set: A Sustainable Choice?" Project on Defense Alternatives report, Task Force on a Unified Security Budget (Washington, DC, October 23, 2011), 2, available at <www.comw.org/pda/fulltext/111024Pentagon-missions.pdf>.

[10] Quadrennial Defense Review, 42.

[11] Paul K. Davis and Peter A. Wilson, "The Looming Crisis in Defense Planning," *Joint Force Quarterly* 63 (4th Quarter 2011), 18.

[12] Stanley R. Sloan, *NATO, The European Union, and the Atlantic Community* (New York: Rowman and Littlefield Publishers, Inc.), 14.

[13] North Atlantic Treaty Organization, "What Is NATO," online brochure, available at <www.nato.int/welcom/brochure_WhatIsNATO_en.pdf>.

[14] Ibid., 6–7.

[15] Ibid., 13.

[16] Sloan, 86.

[17] *The Wall Street Journal*, "Transcript of Defense Secretary Gates's Speech on NATO's Future," *WSJ.com*, June 10, 2011, available at <http://blogs.wsj.com/washwire/2011/06/10/transcript-of-defense-secretary-gatess-speech-on-natos-future>.

[18] Mark D. Ducasse, ed., *The Transatlantic Bargain* (Rome: NATO Defense College, 2012), 13.

[19] Anders Fogh Rasmussen, "NATO After Libya, The Atlantic Alliance in Austere Times," *Foreign Affairs* (July/August 2011), 3.

[20] Ibid., 2–3.

[21] Ibid., 5.

[22] North Atlantic Treaty Organization Special Operations Coordination Center (NSCC), *Special Operations Forces Study*, NATO white paper (Mons, Belgium: NSCC, December 4, 2008), 3.

[23] Lt Gen Frank Kisner, USAF, "Special Air Warfare and a Coherent Framework for NATO SOF Aviation," briefing, NATO Special Operations Headquarters Commanders Conference, Mons, Belgium, November 16, 2011.

[24] Department of Defense of the United States of America to the North Atlantic Treaty Organization NATO SOF Coordination Center Participants, memorandum of understanding, October 9, 2009.

[25] NSCC, *Special Operations Forces Study*, 34.

[26] Admiral William H. McRaven, "Q&A with Admiral William H. McRaven," *Special Warfare* (April–June 2012), available at <www.soc.mil/swcs/swmag/archive/sw2502/sw2502QAAdmiralWilliamMcRaven.html>.

[27] Council on Foreign Relations, "The U.S. Should Stay Relevant in Asia," available at <www.cfr.org/asia/us-should-stay-relevant-asia/p26546>.

[28] David Capie and Amitav Acharya, "The United States and the East Asia Summit: A New Beginning?" *PacNet*, no. 64 (November 14, 2011), available at <http://csis.org/files/publications/pac1164.pdf>.

[29] Hillary Clinton, "America's Pacific Century," *Foreign Policy* (November 2011), 61.

[30] Erik Beukel, *ASEAN and ARF in East Asia's Security Architecture*, DIIS Report 2008:4 (Copenhagen: Danish Institute for International Studies, 2008), 29.

[31] Ibid., 30.

[32] Andrew Davies and Benjamin Schreer, "*Whither U.S. Forces? U.S. Military Presence in the Asia Pacific and the Implications for Australia*," Policy Analysis Report Number 87 (Canberra: Australia Strategic Policy Institute, September 8, 2011), 1.

[33] The ASEAN Way, as described by Gillian Goh's article "The ASEAN Way; Non-Intervention and ASEAN's Role in Conflict Management," published in the Spring 2003 issue of the *Stanford Journal of East Asian Affairs*, is a set of formally adopted principles found in Article 2 of the ASEAN Treaty of Amity and Cooperation. These principles include respect for sovereignty and territorial integrity, noninterference in internal affairs, settlement of disputes by peaceful means, and a renunciation of the threat or use of force. Beyond the political context, the ASEAN Way represents a set of values that all East Asian states share that eschews formal negotiation in favor of personal contacts and quiet negotiation outside of the legalistic systems of ASEAN.

[34] U.S. Congress, House, *Future of U.S. Special Operations Forces*, Hearing before the House Armed Services Committee, 112th Cong., 1st sess., September, 22, 2011.

[35] Department of Defense (DOD), *Sustaining U.S. Global Leadership: Priorities for 21st Century Defense*, Office of the Secretary of Defense (Washington, DC: DOD, January 2012), 3.

U.S. Air Force

NO ONE AT THE CONTROLS

LEGAL IMPLICATIONS OF FULLY AUTONOMOUS TARGETING

By JEFFREY S. THURNHER

Autonomous robots on the battlefield will be the norm within twenty years.

—P.W. Singer, *Wired for War*[1]

MQ-9 Reaper takes off in Afghanistan

Major Jeffrey S. Thurnher, USA, is a Member of the Judge Advocate General's Corps and is serving on the Faculty in the International Law Department at the U.S. Naval War College.

Robots and unmanned systems have proven incredibly valuable on the battlefield during the war on terror and are likely to play a larger and more sophisticated role for militaries in the future. From 2000–2010, the number of U.S. unmanned aerial vehicles (UAVs) proliferated from fewer than 50 to over 7,000, with similarly astounding increases among land- and sea-based unmanned systems.[2] Despite overall reductions in upcoming U.S. defense budgets, expenditures for unmanned systems are projected to grow.[3] All branches of the U.S. military are poised to rely more heavily on unmanned systems in the future.[4] Not only are the numbers of these systems increasing but so are their capabilities. Technology has advanced so rapidly in the past few years, particularly regarding artificial intelligence, that the creation of fully autonomous systems appears a distinct possibility in coming years. The potential deployment of fully autonomous lethal systems raises significant legal and ethical concerns. These concerns, including whether such systems would even comport with the Law of Armed Conflict (LOAC), have yet to be definitively resolved. The technology, however, continues to race forward regardless. Therefore, operational commanders should begin examining the legal and the command and control implications of using such lethal autonomous robots (LARs) as they help steer the future development and doctrine of unmanned systems.[5] While the use of LARs will arguably be deemed permissible under LOAC in most circumstances, prudent operational commanders should still implement additional control measures to increase accountability over such systems.

Technological Advances May Make LARs Possible

Operational commanders need to be aware of recent technological advances and the extent to which the military is poised to incorporate them into future unmanned systems. While LARs may seem incredibly futuristic at first blush, the technological gap is quickly narrowing. In fact, the former chief scientist for the U.S. Air Force even contends that technology currently exists to facilitate "fully autonomous military strikes."[6] Several recent technological breakthroughs, particularly those involving artificial intelligence, highlight how attainable these systems are becoming.

The past few years have witnessed tremendous technological breakthroughs in artificial intelligence. Two highly publicized examples showcase its extraordinary potential. The first involves the IBM supercomputer system known as "Watson." The Watson supercomputer is best known for competing and winning against human competitors on the *Jeopardy* television game show during several special episodes which aired in February 2011. The uniqueness of Watson stemmed from the way it learned to identify the answers to the trivia questions. To attempt to replicate the complex human thought process, Watson was designed with more than 100 statistical algorithms. These helped Watson rapidly sort through multiple databases of stored information. They essentially helped Watson learn—statistically speaking—which words were most likely associated with which answers.[7]

U.S. Air Force (Donald R. Allen)

Unmanned aerial systems lead pilot controls ScanEagle UAV during exercise for aeromedical evacuation and ground medical components

Watson marked an enormous advance in artificial intelligence both in the number of algorithms embedded into it and in the statistical methods it used in solving problems. The extraordinary technology showcased in the supercomputer will likely begin appearing in other computer systems and could be adapted to assist LARs in the future.[8] This is but one recent breakthrough in artificial intelligence.

A second technological breakthrough came from Google with its driverless car. Google funded a team of researchers to design vehicles that could drive without human controllers on city streets and public highways. The researchers, most of whom are part of Stanford University's Artificial Intelligence Laboratory, created seven vehicles that navigated California's freeways and streets accident-free for approximately 140,000 miles with only sporadic human assistance.[9] The sophisticated artificial intelligence in these vehicles was able to "sense anything near the car and mimic the decisions made by a human driver."[10] This cutting-edge technology represented a tremendous leap forward in artificial intelligence. The potential military use of systems capable of autonomous navigation is clear. In fact, this Google project was an extension of an earlier Stanford University project that won the 2005 Defense Advanced Research Projects Agency (DARPA) Grand Challenge competition. That Pentagon-funded competition offered a $2 million prize to the team that could develop an autonomous vehicle capable of navigating itself over a 130-mile desert course.[11] The Google version of the vehicle represents a marked improvement over the one that won the DARPA prize, and possesses the advanced artificial intelligence capabilities that the military will likely incorporate in future unmanned systems.

The true breakthrough of systems like Watson and the Google car is the way in which they adapt and learn. These systems essentially are able to learn from their own mistakes.[12] The branch of artificial intelligence used in these systems is called "machine learning."[13] The computers can recognize patterns in data and accurately make decisions or perform functions based on those observed patterns.[14] It is akin to humans learning through examples.[15] Machine learning is helping computer developers tackle problems "once thought too complex for computers."[16]

Any future development of LARs will rely heavily on such types of artificial intelligence reasoning capabilities. Machine learning computers will likely help future LARs attain the necessary behaviors to make critical decisions about whether and how to engage and destroy a target. The U.S. military has wisely positioned itself to incorporate these new technological breakthroughs into the next generation of its unmanned systems.

The Department of Defense (DOD) is at the vanguard of developing new unmanned technologies. DARPA is the "primary player in the world of funding new research in . . . robotics."[17] It sponsors research on future technologies, and is currently focused heavily on robots and unmanned systems.[18] Other government entities, such as the Office of Naval Research (ONR), are funding efforts to develop robots that can act independent of humans.[19] These DOD organizations helped create the vast numbers of unmanned systems that were deployed to Afghanistan and Iraq over the past decade of fighting.[20] The organizations are now poised to develop even more sophisticated systems.

DOD is already developing doctrine and tactics for incorporating autonomous systems into the overall force

As technology advances, many cutting-edge DOD unmanned systems are taking greater advantage of these artificial intelligence improvements and are being designed with more autonomous features. In the U.S. Navy, close-in weapons systems such as the Phalanx found on *Aegis*-class cruisers and other ships now possess upgraded software enabling them to autonomously find, track, and destroy enemy antiship missiles.[21] ONR is developing systems for the U.S. Navy such as the Biomimetic Autonomous Undersea Vehicle (BAUV), which is capable of conducting long-term underwater surveillance. BAUV can recognize changes in the environment and make adjustments autonomously to maintain its position in the water for many weeks.[22] The Navy is also developing "mine-hunting" autonomous mini-submarines.[23]

The Navy is not alone in pursuing unmanned systems with autonomous features. The U.S. Air Force has designed its Global Hawk UAV systems to include autonomous flight options.[24] Rather than directly controlling the aircraft's every move, human operators merely designate patrol areas for the platform. The system then navigates itself to those areas using Global Positioning System satellites.[25] The Air Force is also researching the use of Proliferated Autonomous Weapons, which are systems of small robots that could be flown autonomously to attack targets as a swarm.[26]

The U.S. Army has been developing a series of unmanned vehicles capable of autonomous operations. Some future Army counter-battery systems may be able to autonomously destroy incoming artillery and missile barrages at speeds faster than humans could possibly perform.[27] Other Army unmanned ground systems are being designed to move around the battlefield autonomously, such as the Crusher Unmanned Ground Combat Vehicle. The Crusher possesses advanced artificial intelligence capabilities and may serve as an unmanned reconnaissance, supply, or fire support vehicle.[28] It represents a potential prototype of the next-generation autonomous robotic ground fighting vehicle.[29]

In anticipation of these autonomous features becoming more widely available, DOD is already developing doctrine and tactics for incorporating autonomous systems into the overall force. Military organizations such as DARPA, ONR, and the U.S. Army Research Laboratory have been working diligently on the so-called warfighters' associate concept, which will partner humans and robots to work as "synergistic teams."[30] The expectation is that robots on the battlefield will form the bulk of detachments, such as infantry units that would be comprised of 150 human soldiers working alongside 2,000 robots.[31]

Operational commanders need to be aware not only that these technological breakthroughs will make autonomous features more readily available but also that there will be a growing need for unmanned systems to become more autonomous. There are several key reasons for the growing need. First, requiring a man-in-the-loop for all unmanned systems is prohibitive both in cost and personnel. It takes scores of people, from pilots to technicians to intelligence analysts, to operate a single tethered UAV.[32] Impending budget constraints may cause the

overall size of the uniformed force to shrink in coming years. Autonomous unmanned systems, which are comparatively less expensive and require fewer human supervisors, will be expected to fill the capability gaps.[33] Second, future battles will likely occur at such a high tempo that human controllers may not be able to direct drone forces to rapidly counter enemy actions.[34] Essentially, a force in the future that does not have fully autonomous systems may not be able to compete with an enemy who does. Many nations, including China, are already developing advanced systems with autonomous features.[35] Third, adversaries are improving satellite communications jamming and cyber-attack capabilities, and, as a result, systems tethered to a human controller may be incredibly vulnerable.[36] Without a constant connection to a human operator, tethered systems are incapable of completing their missions.[37] Thus, in general, future weapons systems will be "too fast, too small, too numerous, and will create an environment too complex for humans to direct."[38] One likely solution will be unmanned systems that are much more autonomous than those that presently exist.

the systems would be programmed to recognize who the enemy is and what objects belong to that enemy

Although the United States is developing a variety of autonomous features for many of its unmanned systems, the Nation remains committed, at the moment, to having a human remain in the loop for lethal targeting decisions.[39] One of the main reasons the United States has not yet fully embraced lethal autonomous targeting is the legal uncertainty associated with robots making those life and death decisions.[40] Deciding whether LARs are permissible under LOAC remains a hotly contested issue.

LOAC Would Permit Fully Autonomous Targeting Under Most Circumstances

LOAC has proven flexible, and has evolved and adapted over time due to advances in both weapons technology and military tactics.[41] Many weapons systems were initially outlawed only to be accommodated later, once the technology proliferated to other nations and international norms conformed.[42] LOAC is essentially derived from customary international practices and international treaties, but thus far there is neither international consensus nor an international treaty about autonomous targeting.[43] Internationally, the debate over whether LARs should be lawful is highly contentious.[44] Any examination of the lawfulness of LARs must begin with the aspect of LOAC known as jus in bello (justice in war), which focuses on determining the practices allowed and prohibited in war.[45] The jus in bello is comprised of four bedrock principles: military necessity, distinction, proportionality, and unnecessary suffering or humanity.[46] With a careful analysis of these and other foundational LOAC principles, the use of LARs will likely be deemed permissible in the vast majority of circumstances.

LOAC is not designed to hinder the conduct of war but is instead intended to ensure combatants properly direct violence toward the "enemy's war efforts."[47] The principle of military necessity helps to achieve that goal. Military necessity requires combatants to focus their military efforts and attacks on those items with a military objective or those offering a "definite military advantage."[48] Thus, force may only be used when it will help the belligerent win the war.[49] Belligerents are expected to examine whether an "object of attack is a valid military objective" before engaging a particular target.[50] One normally looks to an object's nature, location, use, or purpose to make that decision.

Given those parameters, LARs would need to be able to make the determination that a potential target meets the criteria as a valid military objective. While this decision-making process might be complex, forces utilizing unmanned systems would be able to greatly influence this process and likely ensure compliance with the LOAC principle. Even though a system is designed to operate autonomously, it would presumably be given specific orders from its headquarters about what types of missions it would be directed to accomplish. Leadership would most likely program LARs to only engage specific targets or at least specific types of targets. In essence, the systems would be programmed to recognize who the enemy is and what objects belong to that enemy. As long as the types of targets and missions assigned to LARs are valid military objectives, the LARs would be in compliance with the principle of necessity when engaging those targets.

The issue becomes more complicated if the target is not on a preset list. Such a situation might arise with a "target of opportunity" or in response to an emergency situation. The most likely emergency situation is one in which friendly forces are being attacked and LARs are dispatched to provide assistance. In those circumstances, the military necessity prong would be relatively easy to meet as part of a unit self-defense argument. Operational commanders may still want to limit LARs from engaging targets in such emergency situations.

The jus in bello principle of distinction requires belligerents to distinguish between combatants and civilians.[51] It applies to both real persons and tangible objects.[52] The intent is to minimize the harm to civilians and their property.[53] Commanders have the affirmative duty to distinguish between these before ordering an attack.[54] This principle is intended to prohibit indiscriminate attacks.

LARs would have the same requirements to distinguish as any other member of the force. They need to be able to discern between civilian and military objects and personnel. To make this distinction, LARs should be able to rely on uniforms and other distinctive signs. Given the advanced image recognition technology expected to be incorporated into LARs, the systems will likely be capable of recognizing this distinction consistently.[55]

As the United States and others have learned during the past decade of fighting, however, enemies do not always wear uniforms or use distinctive marks. In such uncertain cases, civilians are safeguarded "unless and for such time as they take a direct part in hostilities."[56] Determining if and when a civilian is taking direct part in hostilities can often be most difficult. Similar to humans, LARs would have a hard time making this distinction.[57] However, LARs possess one advantage over humans in this regard. They are not constrained by the notion of self-preservation. Thus, LARs could be programmed to sacrifice themselves to "reveal the presence of a combatant."[58] LARs could easily be ordered to hold fire until they are fired upon. In so doing, the use of LARs could greatly help a belligerent

U.S. Navy (Joseph M. Buliavac)

ScanEagle UAV launches from USS *Comstock* in Gulf of Aden

distinguish combatants from noncombatants on a complex battlefield. Belligerents would still need to satisfy the other foundational principles, including proportionality.

Proportionality requires belligerents to weigh the military advantage of their attack against the unavoidable collateral damage that will result.[59] An attack is lawful as long as it is not expected to cause collateral damage that would be "excessive" in relation to the military advantage.[60] Thus, collateral damage is permitted but only in an amount that would not be deemed excessive. It is vital to recognize that the balancing decision is made in anticipation of the attack rather than with the actual amount of collateral damage caused after the fact.[61]

This proportionality determination equates to a judgment call, which has always belonged to a human. Traditionally, the call has been compared against what a "reasonable person" or a "reasonable commander" would do in such a situation. As long as a similarly situated person would be expected to make a comparable determination of what is excessive under the circumstances, the decision to strike would be deemed lawful.[62] Advances in artificial intelligence notwithstanding, it remains unclear whether a robot's determination of excessiveness could be considered sufficient given such a standard.[63]

Even if the proportionality standard represented an obstacle, many workarounds might still enable commanders to lawfully employ LARs on the battlefield. Operational commanders could use LARs in situations where a higher amount of collateral damage might be acceptable. Normally, attacks directed against high value targets or against a declared hostile force in a high-intensity conflict might fall into this category.[64] Similarly, a commander could designate a limit for the amount of expected collateral damage that is permissible during a specific mission. Thus, if LARs determine that the expected number of civilian casualties exceeds the predetermined acceptable limit, they would not be permitted to engage the target without supplementary human approval. Beyond proportionality, the United States must also ensure LARs do not cause unnecessary suffering.

The last jus in bello principle is unnecessary suffering or humanity. When examining the lawfulness of LARs, this principle should not prevent their use as long as standard munitions and tactics are used in these robots.[65] LOAC requires belligerents to prevent unnecessary suffering when conducting attacks. To comply, belligerents cannot use any weapon or ammunition that is calculated to cause such harm.[66] Instead, they must only use lawfully designed weapons and ammunition and employ them in a lawful method of warfare. All U.S. military weapons and ammunition have been designed with these considerations in mind. As a result, the United States does not field unlawful munitions per se, such as hollow-point rounds or warheads filled with glass.[67] In this case, LARs equipped with standard weapons and ammunition and used in accordance with U.S. doctrine would likely be deemed to comply with the principle of unnecessary suffering.

Overall, as explained in the preceding paragraphs, LARs would arguably be in compliance with all four foundational jus in bello principles in the vast majority of circumstances.[68] Commanders should, therefore, be confident in their ability to utilize LARs, especially when supplemented with additional control measures. This opinion on the lawfulness of LARs is by no means universal, however. Many legal commentators argue that LARs should be banned under international law.

There are several strong counterarguments for why LARs might not be permissible under LOAC. First, many critics argue that LOAC assumes a human is ultimately making the weighty life and death decisions. It would, therefore, be morally wrong to completely remove humans from these targeting decisions. Accordingly, LARs operate outside

the bounds of the applicable international laws and norms.[69] Second, other critics contend that the systems should be deemed illegal because their use could lead to a total lack of accountability for attacks on civilians. They assert that there is no human who can be held accountable for a breach committed by an autonomous system.[70] Those critics contend that there is a "visceral human desire to find an individual accountable."[71] Third, other critics argue that the fact that a system is technologically possible may not mean it is lawful. They contend that some weapons systems are simply too dangerous and thus risk causing too much unnecessary suffering. They argue that other systems, such as lasers with the ability to blind soldiers on a battlefield, are technologically possible but have been banned from war for being too abhorrent.[72] They contend that LARs should suffer a similar fate. Fourth, still other critics contend that LARs fail the proportionality test for some of the reasons that were discussed above. In particular, they argue that robots will not be able to "holistically weigh" the proportionality test.[73] While LARs may be able to determine if the number of expected civilian casualties exceeds some predetermined limit, the proportionality test requires a greater sense of what is excessive.

While those critics provide compelling reasons to doubt the lawfulness of LARs, their counterarguments can be rebutted with a deeper examination of the many prevailing theories on the law. The first counterargument questioned whether LOAC is designed to handle life and death decisions made by robots vice humans. LOAC is indeed a flexible and robust body of law. It has adapted to numerous technological changes, such as the development of submarines and helicopters and nuclear weapons.[74] Although the development of LARs represents a significant advancement in warfighting, it is not so drastic a change as to warrant throwing out the existing body of international laws. LOAC can evolve to encompass LARs and provide necessary and sound guidance to their use. The second counterargument focused on the lack of accountability. Contrary to the opinions of those critics, LOAC does not require that a human be held personally accountable for any mistakes or violations that may occur on the battlefield. While the need to hold someone accountable might be "visceral," it is not definitively required by law. Instead, international law demands that states not absolve themselves of liability with respect to a grave breach of the laws of war.[75] Therefore, the state would likely be responsible for any breach related to LARs.[76] Such a framework essentially exists today if, for instance, a sophisticated mine exploded incorrectly and injured a civilian or some civilian property. The lack of a human to hold accountable does not undermine the lawfulness of the weapons system.[77]

With respect to the third counterargument regarding abhorrent weapons, LARs can easily be distinguished from blinding lasers and other banned weapons. As opposed to those weapons where the weapon itself is at issue, the unique feature of LARs is autonomous control.[78] LARs are expected to use the same types of conventional munitions found on manned military systems, and the lethality of LARs would not differ substantially from that of other weapons systems. Thus, LARs would not cause the same type of unnecessary suffering as blinding lasers. Thus, it seems less likely that LARs would be deemed abhorrent under international law.

The fourth counterargument dealt with proportionality and the requirement for a holistic approach. As was discussed above, the proportionality judgment call is normally assumed to be a human decision. While it is not clear whether a robot's determination will be deemed holistic enough for the critics, the commander's judgment, as evidenced by his orders to LARs about acceptable levels of collateral damage, may be sufficient to encompass that holistic examination. Furthermore, there is actually no specific LOAC requirement for the judgment call to be holistic. International law merely requires belligerents to balance the military advantage against the expected collateral damage. Thus, critics are expanding the notion of proportionality beyond what is legally required.

In general, such strong counterarguments highlight just how complicated and unresolved these legal issues remain. Given this complexity, prudent operational commanders should enact additional control measures when utilizing LARs.

Prudent Additional Control Measures for Commanders of LARs

Even though LARs will likely be technologically possible and permitted under LOAC in the future, operational commanders would be wise to plan carefully for how and when to use such systems. There may be situations in which using LARs might actually prove disadvantageous and unnecessarily risky. If an operational commander ever doubts the effectiveness or lawfulness of using LARs in a particular situation, he either should not deploy them or should implement additional control measures to further protect the unit and the commander from LOAC violations. The following additional control measures will assist operational commanders in their employment of LARs systems.

First, operational commanders need to ensure that all LARs have the proper rules of engagement (ROE), tactical directives, and other national caveats embedded in their algorithms. Moreover, commanders must ensure that any revisions to the ROE or


U.S. Navy (Kimberly K. Fritz)

Transducer Evaluation Center pool at Space and Navy Warfare Systems Center Pacific tests autonomous robotics designed by international student engineers

directives are rapidly inputted into and incorporated by the LARs. Unmanned underwater systems, particularly those without regular communications with the headquarters, may prove to be the most challenged in this arena. For LARs that cannot make such adjustments while deployed, commanders need to ensure those systems can be recalled and then reprogrammed quickly.

Second, commanders should limit when and where LARs are employed to avoid potential proportionality issues. Geographically, LARs are best suited to engage targets in areas where the likelihood of collateral damage is reduced, such as underwater or in an area like the demilitarized zone in Korea. Regardless of geography, LARs might be appropriate when the target is one of particularly high value. In such situations, a commander may have fewer proportionality concerns or might at least be able to quantify the amount of acceptable collateral damage. Utilizing LARs only in specific geographic environments or when pursuing high value targets would alleviate many of the critics' proportionality concerns and best protect operational commanders.[79]

Third, operational commanders should carefully examine the type of conflicts where they might deploy LARs. They would be wise to use LARs predominantly during high-intensity situations where the ROE are status-based, meaning there is a declared hostile force to attack. Those declared hostile forces would then be more easily recognizable, eligible targets for LARs. LARs are less appropriate in counterinsurgency or irregular warfare situations, where "the blurring of the lines between civilian and military is a commonplace occurrence."[80] Similarly, commanders may also want to restrict LARs in emergency situations where the proposed target is not already on a preset list of targets. In such irregular fights and in emergency situations, the legal authority to engage with lethal force is more often conduct-based and thus contingent upon an enemy demonstrating a hostile intent or engaging in a hostile act. Given the higher degree of difficulty in identifying targets and the greater distinction concerns, the best approach may be to avoid using LARs under these circumstances. Prudent commanders should only use LARs in appropriate situations and recognize when it is best to resort to manned systems instead.

Lastly, LARs should be required to have some version of a human override, sometimes referred to as software or ethical "brakes."[81] The systems should be able to be shut down or recalled immediately upon a commander's order.[82] Commanders should also establish triggers for when LARs must seek human guidance before engaging a target. For instance, when a LARs system identifies expected collateral damage greater than a predetermined acceptable limit, it could be forced to seek guidance from the command before engaging that target. Commanders would need to establish protocols and support structures to facilitate quick decisionmaking for these potential targets. In these circumstances, human decisionmakers need a high degree of clarity about what situation the robot is facing. This oversight would not be effective if the human operator were merely a rubber stamp to approve an engagement. With prudent additional control measures such as these, commanders can more safely employ LARs on the battlefield and better protect themselves and their commands.

commanders need to ensure that all LARs have the proper rules of engagement, tactical directives, and other national caveats embedded in their algorithms

Conclusion

The United States will likely face asymmetric threats in military campaigns of the future. Whether the threat is the substantial jamming and cyber-attack capabilities of the People's Republic of China or the legions of swarming Iranian patrol boats, LARs may provide the best way to counter it.[83] LARs have the unique potential to operate at a tempo faster than humans can possibly achieve and to lethally strike even when communications links have been severed. Autonomous targeting technology will likely proliferate to nations and groups around the world. To prevent being surpassed by rivals, the United States should fully commit itself to harnessing the potential of fully autonomous targeting. The feared legal concerns do not appear to be an impediment to the development or deployment of LARs. Thus, operational commanders should take the lead in making this emerging technology a true force multiplier for the joint force. Operational commanders who establish appropriate control measures over these unmanned systems will ensure their LARs are effective, safe, and legal weapons on the battlefield. **JFQ**

NOTES

[1] P.W. Singer, *Wired for War: The Robotics Revolution and Conflict in the 21st Century* (New York: Penguin Press, 2009).

[2] Raul A. "Pete" Pedrozo, "Use of Unmanned Systems to Combat Terrorism," in *U.S. Naval War College International Law Studies* 87, ed. Raul A. "Pete" Pedrozo and Daria P. Wollschlaeger, 217 (Newport, RI: U.S. Naval War College, 2011).

[3] Jack Browne, "UAV Markets Robust Despite Declining Spending," *Defense Electronics*, February 15, 2012, available at <http://rfdesign.com/military_defense_electronics/uav-markets-robust-despite-declining-spending-0215/>.

[4] W.J. Hennigan, "New Drone Is Pilotless, So Who's Accountable?" *Los Angeles Times*, January 26, 2012, available at <http://articles.latimes.com/2012/ jan/26/business/la-fi-auto-drone-20120126>.

[5] The LARs (lethal autonomous robots) label is intended to encompass land-based, aerial, and surface and subsurface unmanned systems.

[6] Werner J.A. Dahm, "Killer Drones Are Science Fiction," *The Wall Street Journal*, February 15, 2012, 11.

[7] Clive Thompson, "What Is I.B.M.'s Watson?" *The New York Times*, June 16, 2010, available at <www.nytimes.com/2010/06/20/magazine/20Computer-t.html?fta=y>.

[8] Jim Fitzgerald, "IBM's Supercomputer Watson Hired to Handle Health Insurance Claims," *The Star-Ledger* (Newark, NJ), September 13, 2011; Edward Larkin, "Siri, Watson, and Artificial Intelligence's Big Year," *London School of Economics Beaver Newspaper*, October 11, 2011, available at <http://edwardandlarkin.com/2011/10/11/siri-watson-and-artificial-intelligences-big-year/>.

[9] John Markoff, "Google Cars Drive Themselves, in Traffic," *The New York Times*, October 9, 2010, available at <www.nytimes.com/2010/10/10/science/10google.html>.

[10] Ibid.

[11] Ibid.

[12] Public Broadcasting Service (PBS), "Smartest Machines on Earth," *NOVA*, September 14, 2011, available at <www.pbs.org/wgbh/nova/tech/smartest-machine-on-earth.html>.

[13] Victoria Nicks, "Machine Learning Types—Unsupervised Learning," *Suite101.com*, March 6, 2010, available at <http://victoria-nicks.suite101.

com/machine-learning-types---unsupervised-learning-a218298>.

[14] Ibid.

[15] PBS.

[16] Ibid.

[17] Singer, 140.

[18] Ibid.

[19] Ibid., 143.

[20] David Axe, "One in 50 Troops in Afghanistan Is a Robot," *Wired.com*, February 7, 2011, available at <www.wired.com/dangerroom/2011/02/1-in-50-troops-robots/>.

[21] Ronald C. Arkin, *Governing Lethal Behavior in Autonomous Robots* (Boca Raton, FL: Chapman & Hall, 2009), 7.

[22] Singer, 144.

[23] Ibid., 225.

[24] Dave Majumdar, "Source: AF to Kill Block 30 Global Hawks," *Military Times.com*, January 25, 2012, available at <www.militarytimes.com/news/2012/01/dn-af-to-delete-global-hawk-012512w/>; Sydney J. Freedberg, Jr., "HASC Orders DoD to Fly Block 30 Global Hawks," *AOL Defense.com*, April 25, 2012, available at <http://defense.aol.com/2012/04/25/hasc-orders-air-force-to-fly-its-block-30-global-hawks-260-mil/>.

[25] Singer, 36.

[26] Ibid., 232.

[27] Ibid., photo section.

[28] W. Wayt Gibbs, "A New Robot Rolls, and a New Prize Is Set," *Scientific American*, May 15, 2006, available at <www.scientificamerican.com/article.cfm?id=a-new-robot-rolls-and-a-n&page=1>.

[29] Defense Advanced Research Projects Agency, "News Release: Crusher Unmanned Ground Combat Vehicle Unveiled," April 28, 2006, available at <www.rec.ri.cmu.edu/projects/crusher/Crusher_Press_Release_DARPA.pdf>.

[30] Singer, 132; Michael J. Barnes and A. William Evans III, "Soldier-Robot Teams in Future Battlefields," in *Human-Robot Interactions in Future Military Operations*, ed. Michael Barnes and Florian Jentsch, 9 (Burlington, VT: Ashgate Publishing Company, 2010).

[31] Singer, 133.

[32] *Defense Update*, "RQ-1A/MQ-1 Predator UAV," *Defense Update*, n.d., available at <http://defense-update.com/products/p/predator.htm>.

[33] Armin Krishnan, *Killer Robots: Legality and Ethicality of Autonomous Weapons* (Burlington, VT: Ashgate Publishing Company, 2009), 2.

[34] Darren Stewart, "New Technology and the Law of Armed Conflict: Technological Meteorites and Legal Dinosaurs?" in *U.S. Naval War College International Law Studies* 87, ed. Raul A. Pedrozo and Daria P. Wollschlaeger, 275 (Newport, RI: U.S. Naval War College, 2011).

[35] Ibid., 276–277, 281; Arkin, 10, 44; Brendan Gogarty and Meredith Hagger, "The Laws of Man over Vehicles Unmanned: The Legal Response to Robotic Revolution on Sea, Land and Air," *Journal of Law, Information and Science*, 19 (2008), 90–91.

[36] Krishnan, 38–39.

[37] Jan Van Tol et al., "AirSea Battle: A Point-of-Departure Operational Concept," Center for Strategic and Budgetary Assessments, May 18, 2010, 33–34, available at <www.csbaonline.org/wp-content/uploads/2010/05/2010.05.18-AirSea-Battle.pdf>.

[38] Singer, 128.

[39] Department of Defense, *FY2009–2034 Unmanned Systems Integrated Roadmap* (Washington, DC: Government Printing Office, April 6, 2009), 27.

[40] Ibid., 24; Dahm, 11.

[41] Stewart, 272.

[42] Krishnan, 90.

[43] Ibid.

[44] Ibid., 89; Peter Finn, "A Future for Drones: Automated Killing," *The Washington Post*, September 19, 2011, available at <www.washingtonpost.com/national/national-security/a-future-for-drones-automated-killing/2011/09/15/gIQAVy9mgK_story.html>.

[45] Krishnan, 90.

[46] Stewart, 272.

[47] U.S. Navy, Marine Corps & Coast Guard, *The Commander's Handbook on the Law of Naval Operations*, Naval Warfare Publication (NWP) 1-14M/Marine Corps Warfighting Publication (MCWP) 5-12.1/Commandant Publication (COMDTPUB) P5800.7A (Washington, DC: Headquarters Department of the Navy, July 2007), 5-2.

[48] Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts, 8 June 1977, 1125 U.N.T.S. 3, art. 52 [hereinafter AP I]. See also Ryan J. Vogel, "Drone Warfare and the Law of Armed Conflict," *Denver Journal of International Law and Policy* 39, no. 1 (Winter 2010), 115.

[49] Krishnan, 91.

[50] *Commander's Handbook*, 5-2.

[51] Ibid., 5-3; AP I, art. 48.

[52] Pedrozo, 249.

[53] Chris Jenks, "Law from Above: Unmanned Aerial Systems, Use of Force, and the Law of Armed Conflict," *North Dakota Law Review*, no. 85 (2009), 665.

[54] *Commander's Handbook*, 5-3.

[55] Krishnan, 95.

[56] AP I, art. 51(3).

[57] Singer, 402.

[58] Arkin, 46.

[59] *Commander's Handbook*, 5-3.

[60] AP I, art. 51(5)(b).

[61] Pedrozo, 248.

[62] David E. Graham, "The Law of Armed Conflict in Asymmetric Urban Armed Conflict," in *U.S. Naval War College International Law Studies* 87, ed. Raul A. Pedrozo and Daria P. Wollschlaeger (Newport, RI: U.S. Naval War College, 2011), 304.

[63] Krishnan, 92.

[64] Author's notes, Unmanned Maritime System Legal Workshop, March 20, 2012, U.S. Naval War College Center for Naval Warfare Studies Conference.

[65] *Commander's Handbook*, 5-3.

[66] Ibid.

[67] Graham, 305.

[68] AP I, art. 57; Stewart, 287; Jenks, 668.

[69] Kenneth Anderson and Matthew Waxman, "Law and Ethics for Robot Soldiers," *Policy Review* (forthcoming, 2012), 11, available at <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2046375>.

[70] Stewart, 290.

[71] Ibid., 291.

[72] Singer, 408.

[73] Stewart, 283 and note 38.

[74] Krishnan, 90.

[75] Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field, August 12, 1949, 6 U.S.T. 3114, 75 U.N.T.S. 31, art. 147.

[76] Krishnan, 105.

[77] Anderson and Waxman, 12.

[78] Krishnan, 97.

[79] Ibid., 162.

[80] Stewart, 286.

[81] Barnes and Evans, 23.

[82] Krishnan, 163.

[83] Tony Capaccio, "Pentagon's Iran Buildup Calls for Lasers, Spy-Plane, Sensors," *Bloomberg News*, March 19, 2012, available at <www.bloomberg.com/news/2012-03-19/pentagon-s-iran-buildup-call-for-adding-laser-weapons.html>.

U.S. Navy (Daniel Viramontes)

ANY SENSOR, ANY SHOOTER

Toward an Aegis BMD Global Enterprise

By JOHN F. MORTON *and* GEORGE GALDORISI

John F. Morton is a Senior Analyst with Gryphon Technologies. Captain George Galdorisi, USN (Ret.), is Director of the Corporate Strategy Group at PAWAR Systems Center Pacific.

Guided-missile cruiser USS *Monterey* under way in Mediterranean

The Aegis ballistic missile defense (BMD) system aboard the USS *Ticonderoga* (CG-47) guided-missile cruisers and *Arleigh Burke* (DDG-51) guided-missile destroyers has become a primary high-end enabler for U.S., allied, and partner maritime forces as they execute the full range of operational tasks in regions where threat vectors are accelerating and proliferating. Warship-focused Aegis BMD and its foundation, the Aegis Combat System, serve as the flexible and adaptive capability to provide "regionally concentrated, credible combat power," as articulated in the national maritime strategy.[1]

Ballistic missile defense is a mission that involves all the Services, and regional BMD is a mission that increasingly supports the U.S. geographic combatant commanders. Aegis BMD is only one component of the larger national ballistic missile defense system (BMDS). This article focuses primarily on Aegis BMD, particularly current and planned roles supporting the combatant commands. Importantly, Aegis BMD is the centerpiece of the Phased Adaptive Approach (PAA), the four-stage framework for regional ballistic missile defense announced by President Barack Obama in 2009.

Proven Aegis BMD capability directly supports or will support the three operational imperatives identified in the national maritime strategy, as well as those implicitly or explicitly stated in the national security and military strategies:

- secure the United States from direct attack
- secure strategic access and retain global freedom of action
- strengthen existing and emerging alliances and partnerships and establish favorable security conditions.[2]

Aegis BMD is evolving into a global enterprise as the system migrates from the U.S. Navy to allied navies. As such, the system is becoming the interoperable "glue" that binds the United States and its regional allies and partners into a credible combat force and, by extension, into a credible deterrent. Here, too, the maritime strategy states, "Integrated maritime operations, either within formal alliance structures (such as the North Atlantic Treaty Organization [NATO]) or more informal arrangements (such as the Global Maritime Partnership initiative), send powerful messages to would-be aggressors that we will act with others to ensure collective security and prosperity."[3]

In the Middle East and Asia, the United States, its allies and partners, and naval joint and combined commanders are contending with the high-end threats posed by accelerating Iranian and North Korean ballistic missile and weapons of mass destruction development. In addition, naval commanders in the Western Pacific now must counter antiaccess/area-denial capabilities such as China's development of the Dong-Feng 21D "ship-killer" ballistic missile.

With Aegis BMD going global in the face of such regional high-end challenges, U.S. coalition partners increasingly have the option to "plug into" Aegis. The question then becomes the extent to which their naval assets—sensors and shooters—should be able to provide *and* receive BMD capability. Our maritime partners are making calculations based on their perceived national interests, threat assessments, and the inevitable budget tradeoffs that must be made in the midst of the ongoing worldwide debt crisis and concomitantly flat or declining defense budgets.

Aegis BMD builds upon the success of the Navy's Aegis Combat System

An Advancing Capability

Funded by the Missile Defense Agency (MDA) and Navy, Aegis BMD builds upon the success of the Navy's Aegis Combat System with its more than 60 years of missile research, development, and testing; real-world performance; and some $50 billion invested in technologies, systems, and ships. Aegis entered the U.S. fleet in 1983 as a blue-water air defense system to defeat massed raids of Soviet naval aviation antiship cruise missiles. In 1991, the Strategic Defense Initiative Organization, the predecessor to MDA, provided the initial funding for the first Aegis BMD capability for area-wide and theater missile defense.

Since then, regular upgrades have provided increased capabilities at every step of Aegis development—guided by its trademark "build a little, test a little, learn a lot" philosophy. The 2011 configuration of Aegis BMD, which was operationally certified in 2009, teams the Aegis 3.6.1 weapon system with the Standard Missile-3 Block 1A missile. The other two major shipboard components for Aegis BMD are the AN/SPY-1 S-band radar system and the Mk 41 vertical launching system (VLS). Phased upgrades of these components have given the Aegis BMD system the ability to counter short- to intermediate-range ballistic missile threats both in the lower and upper tiers of the atmosphere.

The Navy in mid-2011 had 21 Aegis BMD–capable warships: 5 cruisers and 16 destroyers. Sixteen of these BMD ships were in the Pacific supporting U.S., Japanese, and allied efforts to counter the ballistic missile threat presented by North Korea. Five were in the Atlantic to support the expanded NATO requirements vis-à-vis Iran. The commitment of the Nation and the Navy to Aegis BMD is clear, with 94 Aegis-capable ships planned for by 2024.[4]

MDA and the Navy are also developing the Aegis Ashore program, a key component that comes online in Phase II of the European PAA (EPAA), the four-phase regional PAA for the NATO area of responsibility. Initial deployments in Europe will occur later in the decade. In Phase 1 (2011 timeframe), existing sea-based Aegis missile defense ships and radars were deployed to defend against short- and medium-range ballistic missiles in Southern Europe. In Phases 2 (2015 timeframe), 3 (2018 timeframe), and 4 (2020 timeframe), Aegis SM-3 missiles will be successively upgraded to provide coverage against medium- and intermediate-range missiles. By Phase 4, the Block IIB variant of the SM-3 should have an intercept capability against some intercontinental ballistic missiles as well.[5]

In March 2011, the United States and NATO began EPAA Phase I implementation with the deployment of the Aegis cruiser USS *Monterey* (CG-61) to the Mediterranean.[6] Armed with SM-3 Block IA interceptors, the ship arrived on station with an immediate capability to track and intercept short- and medium-range missiles that comprise the Iranian ballistic missile threat to NATO territory and populations. While other Aegis BMD ships have deployed to the Mediterranean since 2009, *Monterey* was the first sustained 6-month deployment of such a ship specifically to support the EPAA.

Aegis integrated weapons system aboard USS *Hopper* launches RIM-161 SM-3 Block IA during exercise Stellar Avenger

As part of EPAA Phase II, Aegis Ashore is a relocatable, land-based Aegis BMD system that, together with the shipboard Aegis BMD, will provide the near-term deterrent framework against regional threats to Europe from short- and medium-range ballistic missiles. Aegis Ashore will reduce the Navy's need to maintain multimission Aegis BMD ships on station that would otherwise constrain their availability for other BMD and general purpose naval missions. In the NATO area, these conjoined elements of the PAA are the U.S. contribution to the NATO territorial missile defense mission and requirement adopted at the Alliance's November 2010 Lisbon Summit.[7]

In May 2011, the United States and Romania agreed on the site for the first Aegis Ashore. That site will include one land-based SPY-1 radar and a relocatable and modified Mk 41 VLS capable of housing and launching 24 SM-3 Block IB missiles.

C2BMC-enabled Aegis BMD

Both Aegis and Aegis-compatible ships plug into MDA's Command, Control, Battle Management, and Communications (C2BMC) element, which enables them to share and receive enhanced capability. Operational since 2004, C2BMC provides layered missile defense by linking regional, theater, and national commands into a single network, providing capability for battle management, planning, situational awareness, and sensor networking—the four major components for ballistic missile defense. C2BMC also links with orbital platforms such as space-based infrared satellites, which generate initial early warning data that fuse with data coming from ground-based sensors, such as the directional AN/TPY-2 X-band radar.

The C2BMC application relies on the Link 16 tactical data exchange network to ensure that sensor and shooter systems have the interoperability required for accepting and sharing target and tracking data. Link 16 is on all Aegis cruisers and destroyers and permits all elements of the national BMDS to accept and share data with other tactical platforms. U.S. allies in the U.S. Pacific Command area of responsibility, Republic of Korea, and Japan rely on Link 16 and their Aegis systems for accepting and sharing information in their missile-defense constructs. In Europe, NATO's missile defense committee is monitoring systems development to ensure interoperability there as well.

Link 16 will network the two relocatable TPY-2s planned for Europe and space-based satellites and airborne sensors with Aegis BMD ships, the Aegis Ashore system, and the air operations and C2BMC command center in Ramstein, Germany. Altogether, this network will expand the coverage area to allow missiles to engage on remotely obtained sensor data. Extending the range for intercepts will enable full-theater missile defense across Southern Europe—a major step toward the NATO territorial missile defense that was agreed upon at Lisbon. C2BMC will link the TPY-2s and the U.S. Army's Terminal High-Altitude Air Defense and Patriot batteries under the NATO missile defense framework. The system will also network with the Ground-based Midcourse Defense system that provides missile defense for North America against intercontinental ballistic missiles.

C2BMC enables a missile defense framework that leverages "any sensor, any shooter, at any phase of missile flight in any region, against any size and type of attack."[8] C2BMC and Link 16 enable TPY-2 radars to provide sensor data to shipboard SM-3 interceptors to allow an Aegis BMD ship to cue its sensors. With the addition of the launch-on-remote (LoR) capability, Aegis BMD ships will be able use this data to launch their interceptors. And these interceptors—no longer constrained by the range of the Aegis radar to detect an incoming missile—can be launched sooner and fly farther.

Existing Aegis BMD–equipped ships already embody the LoR capability, as demonstrated by the 25th Aegis BMD flight test FTM-15 on April 15, 2011. This was the first LoR test of the system against an intermediate-range "separating target"—a warhead separating from its booster missile. FTM-15 featured the Aegis BMD system installed in the guided-missile destroyer USS *O'Kane* (DDG-77) firing a Standard Missile-3 Block IA missile in response to remote sensor data provided by a forward-based TPY-2 radar. This pitted for the first time an in-service SM-3 Block 1A missile against an intermediate-range (1,800–3,400 miles) modified Trident I/C-4 ballistic missile target called the LV-2. This test was well beyond the expected capability of the current version of Aegis BMD, Version 3.6.1, which was developed to counter only short- and medium-range ballistic missiles. The LV-2 had flown in two previous BMD live-fire tests but was not hit until FTM-15.

The flight test thus used technologies and systems that are at sea and in service *today*. There were no changes to *O'Kane*'s BMD suite for the test. Thus, FTM-15 proved an intercept capability against a PAA Phase III intermediate-range ballistic missile (IRBM) threat using a current, though enhanced, PAA Phase I Aegis BMD architecture. Under the PAA, LoR is to have full operational capability during Phase II. MDA had planned for LoR capability to come online in 2015 with the next spiral upgrades to the Aegis 4.0.1 system software and SM-3 IB. The successful FTM-15 intercept demonstrates that the SM-3 IA, supported by a forward sensor and C2BMC architecture, can process forward cueing already, thus giving *Monterey* and other Aegis BMD ships on Phase I deployments an initial LoR capability to intercept an IRBM.[9]

The latest Aegis BMD flight test, FTM-16, occurred September 1, 2011. The

primary goal was to engage a separating ballistic missile target with the Aegis BMD 4.0.1 Weapon System and the SM-3 Block IB missile, the block upgrade to the SM-3 Block IA.[10] The shooter, the guided-missile cruiser USS *Lake Erie* (CG-70), had on board the 4.0.1's upgraded Aegis BMD signal processor along with a two-color infrared sensor in the SM-3 IB seeker. FTM-16 was the first flight test of the Block IB. Unfortunately, the test yielded no intercept despite *Lake Erie* having successfully detected and tracked the target and guided the SM-3. Although the test result was disappointing, FTM-16 highlighted the difficulties and complexities of the ballistic defense mission. In accord with the Aegis philosophy, the Navy and MDA will glean important information from FTM-16, incorporate it, and continue to advance Aegis BMD capabilities.

FTM-16's secondary objective was to test the capability of the FTM-16 participants, which along with *Lake Erie* included the Space and Naval Warfare Command and the Space Tracking and Surveillance System, to exchange Link 16 tracks and simulated engagement status messages. FTM-16 thus served as the second test of the LoR concept for linking an Aegis ship to remote sensor data to increase the coverage area. Certification of BMD 4.0.1 and the Block IB was scheduled for early 2012, after which the system would be ready to be used and supported by the operational forces, thus providing another initial LoR capability.

The next step after LoR is the engage-on-remote (EoR) capability, where the interceptor uses tracking data from remote off-board sensors to destroy a missile threat. EoR, scheduled for PAA Phase III deployment, advances LoR by providing an organic track to the interceptor late in its flight. To the extent that LoR and EoR can provide enhanced capability to the Block IA, IB, and IIA interceptors, these missiles—supported by a C2BMC-netted sensor framework—have the potential to provide territorial and even homeland missile defense in some circumstances.

The addition of LoR capability enables Aegis BMD shooters to launch interceptors earlier in the target missile's trajectory. The goal is to enable a shooter to launch off a track of a forward-based sensor in the system. Ultimately, EoR will enable the shooter to complete the intercept. LoR thus facilitates layered defense, a critical capability for the intercept of longer range and fast-flying missiles. When launch-on-remote and engage-on-remote become operational, the Aegis system can reach farther into the joint and combined arenas. The enhanced network integration of Aegis BMD and MDA's BMDS legitimizes the concept of "any sensor, any shooter" and thus extends the battlespace as well as the area defended.

when launch-on-remote and engage-on-remote become operational, the Aegis system can reach farther into the joint and combined arenas

Linking Aegis BMD and Regional Framework Capabilities via C2BMC

Similar to MDA and the Navy's approach with Aegis and Aegis BMD, NATO has built its theater ballistic missile command and control system upon its air defense capability—calling the system Active Layered Theater Ballistic Missile Defense (ALTBMD). NATO is now expanding ALTBMD to meet its territorial missile defense requirement, which was announced at Lisbon.[11] Alliance members are not building and deploying systems in isolation. Instead, they are providing opportunities for regional and global partners to participate in an integrated, networked territorial missile defense effort that leverages prior investments and investment decisions. Under the expanded ALTBMD framework, the European Allies will operate systems for lower layer, terminal defense for theater-deployed forces. Leveraging its contribution, the U.S. Aegis BMD will operate upper layer (high-altitude) missile defense systems.

Aegis BMD and the MDA's C2BMC element have been fully involved in ALTBMD testing. In December 2010, Aegis BMD participated in the ALTBMD integration test bed at the NATO Consultation, Command and Control Agency facilities in The Hague, providing sensor support to initial lower tier ALTBMD efforts. Aegis BMD is completing lower tier activities as it prepares for the upper tier ALTBMD efforts yet to be planned. A month after beginning its EPAA Phase I deployment in spring 2011, *Monterey* made a port visit to Antwerp, Belgium, where it participated in initial testing of links between Aegis BMD and ALTBMD. In August, NATO conducted the first operational test of the links across ALTBMD, C2BMC, and Aegis BMD to validate ALTBMD's ability to track a target missile. This test was the first time that ALTBMD and Aegis were formally linked and proved their command, control, and communications compatibility. Follow-on efforts will aim to make those links permanent, with a second test scheduled to occur prior to ALTBMD initial operational capability in 2012.[12]

Aegis BMD Global Enterprise

Aegis open architecture provided by the Aegis BMD 5.0 system software upgrade will make it easier for allies and partners to integrate new weapons systems and sensors into the Aegis system—and C2BMC. Aegis BMD officials have been working with foreign shipyards on innovative approaches for reconfiguring Aegis to fit on several classes of foreign ships. Worldwide, seven shipyards have installed Aegis and the SPY-1 radar aboard seven different ship classes. In mid-2011, more than 20 percent of the global Aegis fleet was non-American. Five allies had their navies actively participating in Aegis—Japan, Korea, Spain, Australia, and Norway.

This global effort started in the 1980s with a foreign military sales (FMS) relationship with Japan. The Japanese Maritime Self-Defense Force (JMSDF) was the first foreign navy to construct Aegis warships. The JMSDF currently operates four *Kongo*-class destroyers. The lead ship of the class was commissioned in 1993. In 2000, the JMSDF won approval for two improved units, known as the *Atago* class. The lead ship of that class was commissioned in 2007.

Sharing the U.S. interest in building ballistic missile defenses in light of an increasing regional threat, Japan also decided in 2003 to upgrade its *Kongo*-class destroyers with an Aegis BMD capability. U.S. FMS packages subsequently went to upgrade all four ships with this capability, along with

inclusion of SM-3 Block IA missiles. Japan eventually decided to upgrade its *Atago*-class ships with Aegis BMD as well. That upgrade enables the JMSDF to meet the tenets of its New Defense Program Guidelines, which call for a total of six Aegis BMD–equipped ships to defend the country from missile threats in conjunction with U.S. Navy warships.[13]

Aegis BMD has worked closely with Japan since 1999 to design and develop advanced components for the SM-3 missile. The United States and Japan signed a memorandum of agreement in 1999 to cooperate in the development of the SM-3 Block IIA, with Japan contributing both funding and know-how. The Japanese technical contribution included activities in the areas of the kinetic kill vehicle, second-stage propulsion, and the missile's nose cone. In 2010, the Japanese government relaxed its decades-long arms embargo to allow for the U.S. export of the SM-3 Block IIA to other countries such as U.S. European Allies.[14]

South Korea has announced plans to build six 5,600-ton KDX-IIIA Aegis-equipped destroyers beginning in 2019 that will join its three *Sejon-Daewan* KDX-III destroyers scheduled for service by 2012. High-level discussions have taken place to provide South Korea an Aegis BMD capability on its KDX-III class ships. In 2011, South Korea declared that it was establishing a defensive system to combat air-breathing (aircraft and cruise missile) and ballistic missile threats from North Korea. Scheduled to be in place by 2015, the Korean Air and Missile Defense System will be built around the capabilities inherent in its Aegis-equipped destroyers and its modified Patriot Advanced Capability-3 ground-based interceptors.

In Europe, Aegis has been included in a commercial relationship with Spain that has extended to an enterprise among the Spanish, Australians, and Norwegians.[15] The Spanish navy has been operating four Aegis-equipped *Alvaro de Bazan* (F100) air defense frigates built by the Navantia shipyard in Ferrol, Spain. A fifth F100 was under construction in mid-2011. Navantia has partnered with the Australian government to construct three Royal Australian Navy *Hobart*-class air defense destroyers at the ASC Shipbuilding facility in South Australia. The Australian Ministry of Defence wants to use Aegis to link other maritime assets into an integrated architecture while stipulating that the system must have the capability of adding BMD in the future. In 2004, Australia signed a memorandum of understanding with the United States that provides for a 25-year framework for missile defense cooperation. Navantia also has a commercial enterprise with Norway that put the Aegis system aboard their Royal Norwegian Navy *Fridtjof Nansen F310*–class frigates. In 2011, Norway received the last of five frigates of the class that is a somewhat less capable but still potent version of Spain's F100.

Although their navies have no Aegis warships, other NATO Allies, specifically the United Kingdom, the Netherlands, Denmark, and Germany, have destroyers and frigates with combat systems that can contribute to a broader, Aegis-centered naval BMD architecture. In 2003, the British signed a memorandum of understanding with the United States that led to a follow-on 2006 joint study on a potential Type 45 guided-missile destroyer BMD capability. The Netherlands and the United States have been assessing the potential of Dutch naval combat systems for a BMD capability with SM-3 missiles that could be integrated onto ships equipped with a SMART-L surveillance radar and the Advanced Phased Array Radar (APAR). The German navy also operates three frigates fitted with SMART-L/APAR and the VLS missile launcher. Additionally, Germany has assigned a BMD liaison officer to the Aegis BMD staff to further German understanding of BMD-related issues. This summer, NATO pursued ideas for cooperative SM-3 procurement for use on German and Dutch frigates. In turn, these ships would further explore how they could provide sensor support to the long-range sensor network under the EPAA.[16] Finally, Denmark has plans to construct comparably equipped patrol frigates, suggesting another avenue for migrating the BMD capability to NATO navies.

Aegis BMD's flight test program has engaged allied participation both in missile tracking and interceptor launches. The JMSDF has progressed furthest in this regard, closely integrating its activities with its American counterparts. The destroyer *Kirishima* was the first foreign warship to participate in a U.S. Aegis BMD flight test in the June 2006 FTM-10. In December 2007, the *Kongo* became the first ship of an allied navy to successfully engage a ballistic missile target during the JMSDF's first flight test mission, designated Japan JFTM-1. Between 2007 and 2010, four separate JMSDF ships launched SM-3 missiles at medium-range, separating-warhead targets.[17] These tests, involving JMSDF guided-missile destroyers, demonstrated the promise of a broad-based coalition enterprise linking several navies' Aegis capabilities to address shared operational requirements. Japan's involvement has

U.S. Navy (Daniel Viramontes)

Standing watch aboard guided missile cruiser USS *Monterey*, Black Sea

potential for the Aegis BMD, given Aegis procurements that presage potential partnering opportunities for mutual self-defense and greatly enhanced interoperability.

Aegis BMD will continue to pursue spiral upgrades to advance capabilities—both afloat and ashore

The Netherlands' LCF *Tromp* (F 803) was the first European FTM participant. The ship's modified SMART-L/APAR tracked the ballistic missile target during the December 2006 FTM-11. The Spanish navy's *Mendez Nunez* (F 104), outfitted with BMD software, tracked a ballistic missile target in the June 2007 FTM-12.

The Course Ahead

"The Joint Chiefs of Staff are coming to realize that the Navy's approach to improving Aegis command and control has applicability to the broader BMD system," notes former Deputy Chief of Naval Operations for Naval Warfare Vice Admiral J.D. Williams, who made possible the introduction of a BMD capability into Aegis in the early 1990s. "The Navy, for its part," he continues, "recognizes that its Aegis BMD system needs access to off-board sensor data generated by systems that are outside its control through the improved command and control structure."[18]

The United States and its allies and partners have Aegis and Aegis-compatible assets that offer a variety of in-service and projected capabilities to support and enhance regional ballistic missile defense. As the 2010 *Ballistic Missile Defense Review* put it:

Other allies already own or are working with the United States to acquire specific capabilities, such as naval vessels equipped with the Aegis defensive system that could be adapted to include a missile defense capability. . . . A primary U.S. emphasis is on ensuring appropriate burden sharing. The Administration recognizes that allies do not view the specifics of the missile threat in the same way, and do not have equal resources to apply to this problem, but there is general recognition of a growing threat and the need to take steps now to address both existing threats and emerging ones.[19]

Aegis BMD will continue to pursue spiral upgrades to advance capabilities—both afloat and ashore. LoR and EoR are two emerging Aegis capabilities that are leveraging MDA's C2BMC to expand the Aegis BMD battlespace and improve integration with allied and partner BMD efforts. Command and control interoperability is key to enabling allied and partner navies—with their Aegis and Aegis-compatible ships—to plug their sensors and shooters into this Aegis BMD capability to yield effective, robust, and overlapping regional defense. Command and control interoperability makes for cost-effective burdensharing, especially in this era of declining defense budgets.

In the end, the truly global Aegis BMD enterprise is about networking and leveraging assets—existing or potential—to create the necessary allied and partner synergies for a resilient missile defense framework that is any sensor, any shooter. **JFQ**

NOTES

[1] *A Cooperative Strategy for 21st Century Seapower* (Washington, DC: U.S. Navy, U.S. Marine Corps, and U.S. Coast Guard, October 2007), 7.

[2] Ibid., 3.

[3] Ibid., 6.

[4] See Clarence Robinson, "A Sea Change in Ballistic Missile Defense," in *The Year in Defense: Spring 2010 Naval Edition* (Tampa, FL: Faircount Media, 2010). Robinson quotes Rear Admiral Frank Pandolfe, then-director of the Surface Warfare Division (N86), Office of the Chief of Naval Operations: "Over time we will have a much larger and more capable BMD force, with all 62 destroyers already built or under construction as BMD-capable units." See also, "Navy Aims for 94 BMD-Capable Ships by 2024, Lays Out Plans to Congress," *Inside the Navy*, June 20, 2011.

[5] Missile Defense Agency (MDA), *At Sea . . . on Patrol! Aegis Ballistic Missile Defense Program Review 2011* (Washington, DC: MDA, January 2011), 5.

[6] Michael Fabey, "Aegis-Equipped Ship Provides BMD Protection," *Aviation Week & Space Technology*, March 28, 2011; "NATO Dignitaries Visit USS Monterey, Learn About PAA, BMD Capabilities," Pentagon Brief, April 1, 2011, available at <http://pentagonbrief.blogspot.com/2011/04/nato-dignitaries-visit-uss-monterey.html>.

[7] North Atlantic Treaty Organization (NATO), "Missile Defence," available at <www.nato.int/cps/en/natolive/topics_49635.htm>.

[8] Henry S. Kenyon, "Missile Defense Command System on Target," *Signal Magazine*, January 2007, available at <www.afcea.org/signal/articles/anmviewer.asp?a=1241>.

[9] Amy Butler, "Pentagon Mulls Hurdles to Early Missile Intercept," *Aviation Week & Space Technology*, June 13, 2011, available at <www.aviationweek.com/Article.aspx?id=/article-xml/AW_06_13_2011_p40-330498.xml>.

[10] MDA, "Aegis Ballistic Missile Defense FTM-16 Fact Sheet," August 22, 2011.

[11] NATO.

[12] Amy Butler, "NATO Eyes IOC for BMD Shield Next Spring," *Aviation Week & Space Technology*, August 17, 2011, available at <www.aviationweek.com/Article.aspx?id=/article-xml/asd_08_17_2011_p01-01-360132.xml>.

[13] Japan Ministry of Defense, Defense of Japan 2011 (Provisional Translation), Part III, chapter 1, 23, available at <www.mod.go.jp/e/publ/w_paper/pdf/2011/09_Part3_Chapter1.pdf>.

[14] "Govt sets terms for missile interceptor transfer," *The Yomiuri Shimbun*, July 29, 2011, available at <www.yomiuri.co.jp/dy/national/T110728006799.htm>.

[15] MDA, *At Sea*, 25.

[16] Butler, "NATO."

[17] MDA, *At Sea*, 25.

[18] J.D. Williams, *Improving Aegis Ballistic Missile Defense Command and Control*, Heritage Special Report SR-89 (Washington, DC: The Heritage Foundation, May 2, 2011), 11, available at <http://thf_media.s3.amazonaws.com/2011/pdf/sr0089.pdf>.

[19] MDA, *At Sea*, 32. The success of Aegis BMD afloat and the promise of Aegis Ashore have also garnered interest from a wide range of nontraditional partners such as India. See Amy Kazmin and Farhan Bokhari, "New Delhi Weighs Up U.S. Missile Shield," *The Financial Times*, January 8, 2009, available at <www.ft.com/intl/cms/s/0/1331a926-dce4-11dd-a2a9-000077b07658.html#axzz1t5WCBvtg>.

U.S. Air Force (Benjamin Wiseman)

RESPONSIVE CLOSE AIR SUPPORT

By JOHN J. SCHAEFER III

Colonel (S) John J. Schaefer III, USAF, is a 2012 graduate of the Industrial College of the Armed Forces and is currently serving as the Deputy Director of the NATO Combined Air Operations Center at Larissa, Greece.

A-10C Thunderbolt II is first aircraft designed to provide close air support of ground forces

In May 2011, International Security Assistance Force Commander General David Petraeus said the responsiveness of close air support (CAS) in Operation *Enduring Freedom* (OEF) went from "great to exceptional" in the previous year. He further stated, "The traditional standard had been 12 minutes from the time assets are requested to when they are on station. Recently the average response time has fluctuated around eight minutes."[1] This reduction applied specifically to "troops in contact" (TIC) situations where ground forces request CAS. Ground forces request CAS when their organic assets cannot handle the situation. In practical terms, this means aircraft are normally responding where ground forces are receiving accurate fire. Four minutes can seem like an eternity to a soldier in the middle of a complex ambush. Aircraft arriving even a few seconds earlier can make the difference between life and death.

Numerous agencies and people contributed to this success story, but a great deal of credit belongs to three U.S. Air Force (USAF) captains and a Royal Air Force flight lieutenant[2] at the Air Support Operations Center (ASOC) in Kabul. Their leadership as Fighter Duty Officers (FDOs) in charge of their respective shifts in the ASOC directly resulted in the increased responsiveness that General Petraeus lauded. They motivated their crews of highly skilled Airmen to reduce the historically acceptable 12-minute response time to TIC situations. Command and control of airpower in a complex combat environment is not easy, yet they saw the potential for improved support to the coalition's fielded forces and fought to provide it. As the campaign in Afghanistan enters its drawdown phase, an examination of how they achieved this dramatic decrease is appropriate.

Fundamentally, improved responsiveness happened because these Airmen left no rock unturned in their pursuit of better supporting their comrades in arms. No single line of effort produced this change. Multiple lines of effort simultaneously contributed to success. Of note, some great ideas did not come to fruition due to technical, bureaucratic, financial, and other barriers. Other initiatives turned out not to be great ideas after all. Five lines of effort, however, proved particularly fruitful.

Build Relationships Based on Trust

A quick survey of the doctrinal Theater Air Control System/Army Air-Ground System (TACS/AAGS)[3] shows that the system is a network of relationships. Each agency has an important role in the overall success of the system. The fielded version of the system in Afghanistan is far more complex than the doctrinal model. Geography, coalition command structures, the presence of civilian air traffic in the battlespace, and equipment shortfalls all contribute to the nondoctrinal aspects of the command and control structure. Multiple regional commands led by different Services and nations introduce even more boundaries and relations that are not depicted on any hierarchical organizational chart. In effect, an ad hoc command and control network is overlaid on the basic doctrinal framework. The result is that personal relationships serve as vitally important "grease" to keep the command and control structure functioning smoothly.

improved responsiveness happened because Airmen left no rock unturned in their pursuit of better supporting their comrades in arms

Relationships are better built face to face. A phone call or email can start a relationship but nothing replaces actually meeting counterparts and seeing firsthand where they work. The four officers mentioned above traveled widely throughout the area of operations (AOR) and forged relationships that repeatedly helped shorten CAS response times. Building a relationship in person allows both sides to understand each other's environment, capabilities, and limitations. Details as simple as knowing seating arrangements in the Combined Air Operations Center (CAOC) can slice minutes off response times. When a phone is busy during a TIC situation, knowing which of your contacts is close enough to tap the busy party on the shoulder and speed the process can save lives. Cultivating close relationships across organizations requires time and effort but it pays off when the chips are down.

From the ASOC perspective, three relationships stand out in importance:

ASOC—Fires relationship. First, the ASOC relationship with the corps staff (particularly the corps fires staff) is exceptionally important in creating the flexibility to meet the ground force commander's (GFC) intent. Establishing personal relationships leads to mutual understanding of each organization's capabilities, limitations, and purpose. Once ASOC and fires personnel establish a relationship that facilitates open exchange of priorities and compromises required to achieve given priorities, both parties can work together to best achieve the commander's intent. A strong personal relationship with fires officers allows FDOs to explain the compromises involved in fulfilling a particular air support request when they predict excessive impact to achieving the commander's intent. Each situation will be different, but having open lines of communication at the personal level allows for quick, intelligent adjustments to air support requests and aircraft taskings. Time spent building a good relationship assures both sides that each is working to maximize their assets' contribution to the common effort.

ASOC—Combined Air Operations Center relationship. These two organizations interface at multiple points. While numerous publications detail the formal structure of this relationship, strong personal relationships allow each organization to maximize its contribution to the fight. The most important interface is between the ASOC director and the chief of combat operations (CCO). The ASOC director commands the ASOC and is responsible for the actions of all ASOC crews. The CCO directs operations on the CAOC floor to ensure effective use of airpower assets. This relationship sets the tone for all other interactions. Frequent dialogue between these individuals allows each to provide direction to their organizations that speeds the exchange of information required to reduce CAS response times. As with any two distinct organizations, friction will occasionally develop as each strives to achieve its own mandates, but strong personal relationships allow both sides to move beyond these instances to expedite CAS response times. The FDOs' relationships with the numerous CAOC desks they deal with fall under the umbrella of this larger relationship. Routine communication between the FDO and multiple duty officers (DOs)—for example, CASDO, Tanker DO, and others—at the

CAOC keeps both sides in the loop when changes in the plan are emergent. When these relationships are mutually trusting, time is not wasted trying to figure out why a change is being made. Instead, time and effort is focused on finding the best solution to the challenge at hand. Good ASOC/CAOC relationships at the DO level allow peers to share workload and anticipate each other's moves when time is of the essence.

ASOC—Marine Aviation Command and Control System (MACCS) relationship. Future campaigns may or may not result in the TACS/AAGS and MACCS working as neighbors. However, the lessons learned by working along this boundary apply whenever two similar, but not identical, command and control systems interface. While internal communications and relationships are important, relationships along and across seams and borders cannot be overlooked. Actions occurring at borders between command and control systems are potentially sources of significant delays if the people operating both systems are not familiar with each other. Due to cultural and Service differences, these relationships may initially require more effort to cultivate, but they are absolutely worth it.

The addition of Regional Command Southwest (RC-SW) in 2010 significantly changed command and control relationships for both ground and air forces in Afghanistan. The ASOC and elements of the MACCS experienced predictable growing pains during this transition. Working relationships were lukewarm at best through early 2011. Philosophical differences regarding the best way to integrate airpower into ground operations, high turnover rates, and different definitions of the same terminology all contributed to less than optimal CAS response times along the boundary between the U.S. Marine Corps (USMC) and USAF command and control systems. Numerous telephone-brokered agreements improved the flow of airpower assets between the two systems but significant improvement eluded both sides until Airmen visited RC-SW and Marines toured the ASOC in Kabul. ASOC personnel learned how aircraft are handed off inside the MACCS system; this allowed them to contact the right agency to quickly recall Combined Forces Air Component Commander (CFACC) assets into the TACS system in response to immediate CAS requests. Conversely, Marines saw the impact that an unreliable air picture had on ASOC operations and they were able to frame future requests in a manner that expedited responses. However, the most important outcome of these exchanges was mutual trust. Parochial mistrust disappeared once operators on both sides clearly saw that each desired to provide the best possible airpower support to fielded coalition forces. The time and effort spent to build relationships across the command and control seam paid huge dividends and allowed for the codification of procedures that mutually benefited all parties.

U.S. Air Force (Rebecca Garland)

Air Force air liaison officer calls in A-10C II Thunderbolts for close air support in Afghanistan

U.S. Army (Jason Fetterolf)

Marine AH-1W Super Cobra during close air support training, Kuwait

The Air Tasking Order Is a Baseline

A cautionary declaimer is in order before describing the role of ASOC in executing the CAS portions of the air tasking order (ATO) in OEF. The following discussion details how the FDOs managed the ATO to achieve the GFC's intent but the extent of their actions should not be extended to other mission types. The actions they took and the mindset that accompanied their actions were very effective in the OEF context. The same types of actions in other missions areas or in a broader campaign could have significant negative operational and strategic impacts.

Command and control of airpower in a CAS-centric environment is art aided by science. The ATO is built using inputs from the ground component and therefore positions airpower assets to contribute to achieving the GFC's objectives. In a CAS-centric air campaign, the plan laid out in the ATO provides the palette FDOs use to meet the GFC's intent. Just as ground forces continuously modify their actions during execution in response to weather, enemy actions, logistics delays, and myriad other factors, FDOs modify the CAS plan after the ATO is published. Changes made after ATO publication are not made in a vacuum nor are they indicative of flaws in the process used to produce an ATO. Ground forces routinely cancel, reprioritize, or reschedule operations that the ATO supported with dedicated CAS missions. FDOs are normally collocated with the corps staff, which enables the relationships described above, and allows them to coordinate in real time to adjust the flow of CAS assets. The systems used by both ground and air planners to build the ATO are extremely complex and represent a scientific way to account for as many factors as possible when allocating scarce resources. FDOs apply art to the CAS portion of the ATO in order to actively manage a four dimensional mosaic of CAS assets throughout an ATO cycle.

In practice, FDOs started "reflowing" 20 to 80 percent of the CAS ATO each night to better support evolving ground forces actions. All elements of the TACS did not initially receive this notion well. The magnitude of change produced significant heartburn in some quarters, but the immediate drop in response times shielded the FDOs from backlash. Luckily, success is hard to argue with, and their results afforded them the leeway to refine the process until it produced the 33 percent reduction in response times lauded by General Petraeus. The ATO serves as an important baseline for CAS operations. It sets the bounds of flexibility available to FDOs charged with executing it to support the GFC. For example, FDOs need to know what CAS assets they have to work with at any given time. Any changes to the plan must consider the number of distinct assets available. Likewise, careful study of the ATO may reveal that availability of tanker assets is actually the constraining factor during a particular timeframe. FDOs must work within the limits imposed by the ATO, but they should have considerable leeway to apply operational art within those constraints.

Active Pursuit of Improved Situational Awareness

The ASOC requires situational awareness across the span of its area of operations to effectively command and control CAS. The quality of decisions and the rapidity with

which they are made is directly related to the extent of the ASOC's situational awareness. By the fall of 2010, a series of relocations, difficulties associated with release of classified information on coalition networks, and a variety of significant technical issues resulted in the ASOC operating with an unreliable air picture and virtually no ground picture. Numerous workarounds enabled the ASOC to perform its mission. However, these workarounds had two nontrivial impacts. First, they introduced delays into the decision-making process. Second, parts of the ASOC mission were outsourced to other command and control agencies because the ASOC did not always have enough information to make good decisions. Immediate efforts to improve situational awareness enabled the FDOs to reclaim their mission and produce quicker response times.

The issue was not the lack of a common operating picture for the theater. While traveling and establishing relationships throughout the AOR, the FDOs discovered myriad operating pictures at all organizational levels. Interestingly, some of the most complete pictures were available to organizations that did not use or need them to accomplish their missions. Those organizations had the good fortune of available bandwidth, highly skilled interface control personnel, favorable line-of-sight geography, and the right mix of equipment to display high quality real-time overlays of ground and air forces.

Fortunately, Joint Interface Control Officers across both the Army and Air Force are passionate about what they do. At every turn, they worked with the datalink managers at ASOC to apply impressive knowledge and ingenuity toward resolving the issue. The story of how the ASOC collaborated with numerous agencies to improve its access to situational awareness is impressive, but the more important story is what the FDOs did once they had access to the information they needed. The ASOC cannot maximize the advantage it gains from sitting at the intersection of the Army and Air Force command and control systems unless it has good situational awareness of the operations of both components.

Gaining better situational awareness enabled faster CAS response times, but the bulk of the improvement came from how the FDOs used the information—not from simply having a better picture. The improved common operating picture allowed the ASOC to evolve from a processing node to an active node of the TACS. Rather than waiting for an immediate CAS request to arrive from the field, then consulting with adjacent agencies to determine the appropriate reaction, ASOC crews used their improved situational awareness and the relationships they forged across the campaign to develop a "feel" for their AORs. They began to recognize enemy trends in particular geographic areas, the engagement patterns and tactics of coalition forces, and the likelihood of TIC situations arising from different types of missions. For example, given two air support requests of equal priority, ATO planners must choose which to support based on the information they have available at the time. After the ATO is published, ground forces may generate a mission near the unsupported request that is of lower priority but has a high likelihood of developing into a TIC situation. FDOs can use their knowledge of the battlespace to switch support to the high priority task closer to the new mission. This reduces response time if their intuition about the new mission is correct, while providing the same level of support to ground forces. Armed with this heightened feel for the situation, FDOs began to anticipate events and either develop contingency plans or reposition assets. Because their scope of responsibility was limited to the CAS realm, the feel they developed falls short of "Napoleon's coup d'oeil," but it certainly contributed to reducing CAS response times. They did not always get it right, but their ability to make the right trade-offs improved rapidly over time. Combining high quality situational awareness with a network of relationships allowed the FDOs to get further ahead of the game and make decisions that put the right assets in the right place at the right time.

Joint Interface Control Officers across both the Army and Air Force are passionate about what they do

Decide and Take Action

Command and control of CAS assets is not for the timid. FDOs need to be decisive and start the process of moving aircraft as quickly as possible when a TIC situation is declared. Ideally, the FDO makes a decision and communicates it directly to the appropriate CAS assets, who then immediately start moving in the correct direction while coordinating the required clearances. The FDO arrives at a pairing decision using the considerable resources resident in his crew, his feel for the battlespace, and the network of relationships available to him because he is collocated with the supported command.

In Afghanistan, CAS aircraft work in assigned areas that can take several minutes to transit, so they usually have time and space to start toward their assigned tasking and attain new airspace clearance before reaching the limits of their current airspace. Excessive consultation introduces delays that result in casualties. Some of the previously described technical difficulties had resulted in an atmosphere where command and control agencies other than the ASOC operated as if the decision to pair assets against a particular CAS request was a collaborative one. Armed with better situational awareness, the FDOs began using their positional authority to expedite CAS response times. Execution of the FDO's decision may well require a collaborative effort but the decision belongs to the FDO. When collaboration is required to notify the assigned aircraft, time spent debating the decision rather than executing it can prove fatal for the Soldiers who requested CAS.

Increased use of datalink technology reduced the need for collaboration to notify aircraft of their assignments and correspondingly reduced opportunities for this type of delay. ASOC datalink managers were physically located in the midst of the conversation that produces a CAS aircraft tasking. They quickly became so adept at listening to the conversation while simultaneously preparing the ensuing message traffic that the message was digitally sent as the FDO uttered the final syllable of the order. By involving fewer middlemen in a CAS tasking, faster response times are achieved. However, cutting intermediaries out of the execution chain must not be confused with cutting them out of the loop. Because their decisions sometimes affect multiple operations across the area of operations, the ASOC strove to inform the entire command and control system of their decisions as quickly as possible.

In practice, notification of both the aircraft and the entire system often occurred simultaneously by using electronic chat rooms and the datalink architecture.

While this simultaneous notification is admirable, all stakeholders must remain focused on the fact that *pairing CAS aircraft to troops in contact situations is combat command and control not peacetime air traffic control*. Nevertheless, worries about aircrews exceeding their authorized clearances while rushing to respond to their CAS taskings are overblown for two reasons. First, geography and airspeed usually conspire to prevent this conflict from arising as aircrews are rarely at the edge of their assigned airspace at the precise second they receive a tasking. In the rare instances when this occurs, highly trained and disciplined CAS aircrews flying the most sophisticated aircraft in the world can safely expedite their arrival overhead in a TIC situation. Their onboard systems, coupled with years of experience and their own situational awareness, minimize any risk they assume. Second, commanders at all levels, from the CFACC to aircraft commanders, take appropriate risks in combat. They do so within the limits of very clear guidance. That guidance, not a peacetime air traffic control mindset, should determine how much risk they assume. Everyone involved with CAS needs to operate with the appropriate urgency and willingness to assume risk consistent with their commander's guidance.

strong situational awareness and communications capacity enable decentralized execution of airpower through the ASOC

Relentless Debrief

The final line of effort discussed in this article applies to any attempt to improve a system. Changing large systems is not a simple endeavor, and one should learn along the way. The FDOs constantly debriefed their crews' performances as they developed new procedures and mindsets to reduce response times. No aspect of their operation was immune to examination. They set an atmosphere that allowed everyone in their crews to contribute to the improvement process. Some of the most significant lessons learned (and subsequent improvements) arose from examining events with response times under 5 minutes. Successes produce as many lessons as failures. Careful examination of decisions after the actions are complete may reveal a technique to achieve the same result while introducing fewer perturbations into the system.

The FDOs' debrief process was particularly effective for two reasons. First, they made sure they shared their knowledge with all the ASOC crews through formal handover briefs and immediate updates to their operating procedures. This effort ensured lessons *learned* rather than just lessons *observed*. Second, when their actions caused friction with outside agencies, they diligently collected the facts and then worked with the appropriate agency to explore better ways to accomplish the task that caused the conflict. Leading change is sometimes a messy process, but taking the time to thoroughly debrief and document required changes both internally and externally contributes to success and ensures that the change endures.

Conclusion

This article highlighted several lines of effort that produced a significant reduction in CAS response times in Afghanistan. Mutual trust arising from strong relationships throughout the command and control system enabled faster actions from all parties. Common predeployment training is the ideal way to establish these relationships. When that is not possible, command and control units should visit adjacent organizations during the deployment process. The FDOs described above altered their routes into theater to visit the CAOCs and the Control and Reporting Centers, then trekked to the MACCS in the early stages of the deployment. The relationships forged in these initial visits paid significant dividends throughout the deployment. Using high fidelity situational awareness to apply operational art to the CAS portions of the ATO improved the effectiveness, efficiency, and response times for CAS operations. In future operations, the command and control system must prioritize providing situational awareness and communications capability to forward elements. That is often more difficult than providing the same capabilities to rear elements, but it allows those closest to the decisionmakers on the GFC's staff to capitalize on that proximity to provide shorter CAS response times. Strong situational awareness and communications capacity enable decentralized execution of airpower through the ASOC. Conversely, concentrating situational awareness tools and communications ability in rear elements leads to less responsive centralized execution. Empowering FDOs to make decisions and immediately begin executing them reduced response times by eliminating unnecessary postdecision collaboration. Experience showed that combat-seasoned aviators with a broad understanding of the entire command and control system performed best in the FDO role. Time invested in training to familiarize FDOs with adjacent command and control agencies allows them to step into their critical role with confidence. They must arrive in theater with a clear understanding of their role in the command and control system and the confidence to make tough decisions quickly. Robust predeployment training scenarios are the best way to develop this confidence and lead to rapid intuitive decisions that reduce CAS response times. Lastly, taking the time to debrief each engagement thoroughly and document lessons learned built a culture of continuous improvement that incrementally improved response times. Lessons learned must be codified in order to outlast the tenure of those who experience them. While future conflicts will present different challenges, the remarkable improvement in CAS response times that these Airmen generated and how they accomplished it should not be forgotten the next time our country finds itself involved in a conflict. **JFQ**

NOTES

[1] "From Great to Exceptional," *Airforce Magazine.com*, June 1, 2011, available at <www.airforce-magazine.com/Features/airpower/Pages/box060111petraeus.aspx>.

[2] The author remains incredibly impressed with the leadership and dedication to improving response times displayed by Captains Timothy Scariano, Dave Kelley, Timothy Swierzbin, and Flight Lieutenant Phil Druce.

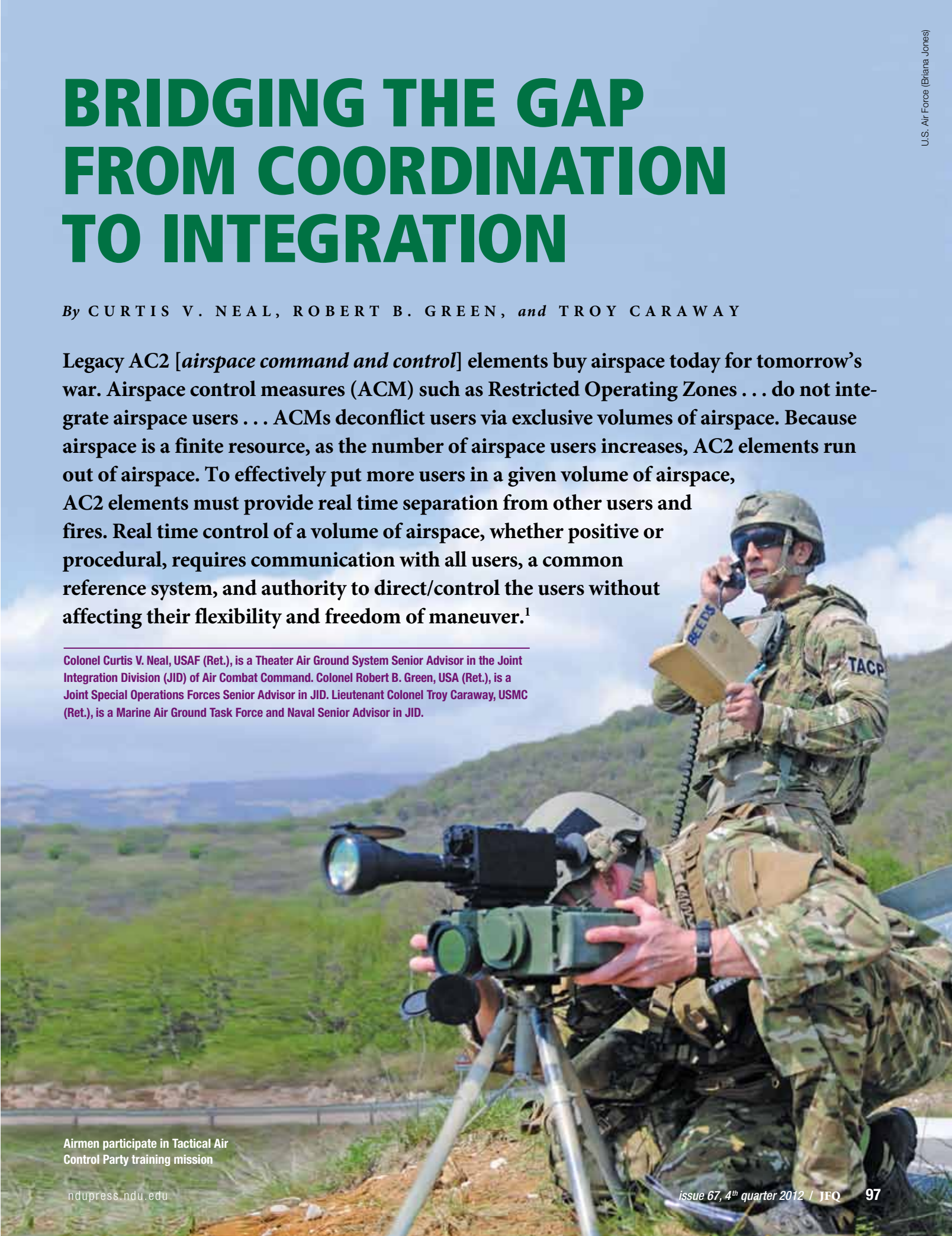
[3] Joint Publication 3-09.3, *Close Air Support* (Washington, DC: The Joint Chiefs of Staff, July 8, 2009).

BRIDGING THE GAP FROM COORDINATION TO INTEGRATION

By CURTIS V. NEAL, ROBERT B. GREEN, *and* TROY CARAWAY

Legacy AC2 [*airspace command and control*] elements buy airspace today for tomorrow's war. Airspace control measures (ACM) such as Restricted Operating Zones . . . do not integrate airspace users . . . ACMs deconflict users via exclusive volumes of airspace. Because airspace is a finite resource, as the number of airspace users increases, AC2 elements run out of airspace. To effectively put more users in a given volume of airspace, AC2 elements must provide real time separation from other users and fires. Real time control of a volume of airspace, whether positive or procedural, requires communication with all users, a common reference system, and authority to direct/control the users without affecting their flexibility and freedom of maneuver.[1]

Colonel Curtis V. Neal, USAF (Ret.), is a Theater Air Ground System Senior Advisor in the Joint Integration Division (JID) of Air Combat Command. Colonel Robert B. Green, USA (Ret.), is a Joint Special Operations Forces Senior Advisor in JID. Lieutenant Colonel Troy Caraway, USMC (Ret.), is a Marine Air Ground Task Force and Naval Senior Advisor in JID.



U.S. Air Force (Briana Jones)

Airmen participate in Tactical Air Control Party training mission

In the past, when faced with a large number of competing airspace users and limited command and control capabilities, it has generally been easier to deconflict competing demands for airspace by implementing procedural control methods that placed heavy emphasis on the increased use of airspace and fire support coordinating measures. Prior to Operations *Enduring Freedom* and *Iraqi Freedom*, military operations demonstrated little need for the much more difficult real- or near real-time deconfliction and integration of airspace and fires.

Beginning about 2004, emerging military capabilities and ongoing operations in Iraq began to provide insight into how future military operations would increasingly challenge our current airspace control abilities. These included large numbers of manned military, civil aviation, other government agency, special operations, and coalition aircraft, as well as rapidly expanding numbers of unmanned military aircraft of all sizes. In addition, combat operations demanded increasingly large volumes of responsive ground-based fires that had to be integrated into the airspace.

In a 2007 Joint Urgent Operational Need Statement, Lieutenant General Raymond Odierno, Commander, Multi-National Corps–Iraq, stated, "The joint community and the U.S. Army are not equipped to manage or adequately deconflict airspace of high-traffic density." As a result of these challenges, the way the U.S. military controls airspace during joint operations began to fundamentally change. In 2006, the Army began fielding an organic airspace command and control (AC2) capability comprised of over 1,600 trained operators with dedicated AC2 cells at corps, division, and brigade levels, all linked through the tactical airspace integration system. In 2007, the Army also began a migration from a division-centric force toward a more expeditionary brigade-centric force, with the Brigade Combat Team becoming the primary combined arms building block unit of the Army. Today, the divisions employ brigades to fight battles and engagements while corps conduct large-scale land operations, employing divisions as part of a joint campaign, executing operational-level actions to achieve strategic effects.[2]

To maintain responsiveness and flexibility, the Air Force, in coordination with the Army, made a decision to increase the number of Air Support Operations Centers (ASOC) from 6 Cold War–legacy ASOCs aligned with each Army corps to 10 ASOCs, aligned and collocated with the 10 active Army divisions. Each ASOC is responsible for the coordination and control of air component missions requiring integration with other supporting arms and ground forces.[3] Three additional ASOCs will remain non-aligned. While still functionally unique, the aligned ASOCs are being integrated with the division Tactical Air Control Party (TACP) as part of each division's Air Support Operations Squadron. The ASOC realignment is scheduled to be complete by fiscal year 2015.

A New Approach

This new ASOC alignment makes it possible to improve the integration of joint airspace control and joint fires at the division level through an organizational concept called the Joint Air Ground Integration Cell (JAGIC). The JAGIC is the result of a 6-year Army–Air Force Integration Forum effort, spearheaded by Air Combat Command's Joint Integration Division and the U.S. Army Training and Doctrine Command (TRADOC) Fires Center of Excellence Joint and Combined Integration Directorate. It has been exercised in multiple Army–Air Force warfighting experiments and exercises and resulted in increased air-ground effectiveness during each event.[4]

to maintain responsiveness and flexibility, the Air Force, in coordination with the Army, made a decision to increase the number of Air Support Operations Centers

The JAGIC is created by organizing the ASOC operations crew, division TACP personnel, the Division Fires Support Element, AC2, air and missile defense, and aviation personnel into a single integrated cell within the division Current Operations Integration Cell.[5] The important point is that the JAGIC is simply an integrating cell[6] created from Air Force and Army personnel already supporting, or assigned to, the division headquarters (HQ). No additional manpower is required to form the JAGIC, and it does not replace any current division cells or command and control nodes. Quite simply, the JAGIC improves the way these elements integrate organizationally and procedurally to conduct operations in a more efficient, linked, and situationally aware manner.

Unlike most military capability improvements based on new systems and technology, the JAGIC is based on organizational and procedural changes that emphasize proximity and teamwork by collocating Theater Air Control System (TACS) personnel with their ground element counterparts. By doing so, the JAGIC builds Soldier-Airman relationships, improves communication effectiveness, and increases situational awareness and understanding. Essentially, the JAGIC creates a joint decision-oriented command and control organization resulting in faster decisions based on better information that increases effectiveness while decreasing risk.

The JAGIC is neither a staff nor a planning cell, but is composed of those personnel directing and monitoring the current fight through the arrangement of operators performing related functions in close physical proximity. Such an arrangement not only integrates the air and ground component operators, but also collocates the decisionmaking authorities from the land and air components with the highest levels of situational awareness, that is, the senior air director and deputy fire support coordinator, while building habitual relationships to support the maneuver commander's concept of operations. This arrangement also ensures support of joint forces air component commander (JFACC) objectives and intent and requirements of joint force commander (JFC)-designated authorities such as Airspace Control Authority and area air defense commanders.

While procedural control methods will remain a mainstay of airspace and fires integration for the foreseeable future, the integration of personnel from both Services who are directing and monitoring ongoing operations permits dynamic coordination, activation, and deactivation of airspace and fire support coordination measures rather than "buying airspace today for tomorrow's war." When the JAGIC is empowered with the means and authority to pass control instructions directly to the airspace users, mutually supporting operations can rapidly be integrated, conflicts can be resolved on the fly, and real-time coordination of competing requests can either be resolved through the use of flexible, informal control measures or by direct coordination requiring no control measures at all. For the airspace user, the JAGIC provides a

single "center" for coordinating requests and resolving joint airspace conflicts within the division area of operations.

While the overarching function of the JAGIC is to fully integrate joint airspace control and joint fires at the division level, it executes integrated tactics, techniques, and procedures (TTP) to support numerous joint processes including direction and monitoring of fires and effects, command and control of some volume of airspace overlying the division area of operations, rapid attack of emerging targets, interdiction coordination, improved friendly force identification, increased situational awareness for air defense, and synchronization and integration of tactical intelligence, surveillance, and reconnaissance, electronic warfare, information operations, and airlift assets.

The design and manning of the JAGIC is such that a subset of the JAGIC, called a Joint Air Support Element (JASE), can be task-organized and sent forward to extend control and integration of air operations in High Density Aircraft Control Zones, support displacement operations, or extend support to a subordinate maneuver unit for named operations of limited duration. The JASE will normally be provided in coordination with an Army tactical aviation control team. The JASE and Army control team effectively extend the JAGIC capability forward of the division when needed.

As noted earlier, corps conduct large-scale land operations, employing divisions as part of a joint campaign, executing operational-level actions to achieve strategic effects.[7] The corps TACP will remain the JFACC's primary liaison for providing advice, planning, synchronization, and integration of airpower at the operational level in support of corps operations. When a corps is designated as a joint force land component command or joint task force, it may receive an Air Force Joint Air Component Coordination Element, in addition to the corps TACP, to better integrate joint air operations with corps operations.[8]

As the Services have moved forward with JAGIC development and implementation, some have questioned its origins and purpose. The most common criticism is that the JAGIC was developed as a solution for the challenges the TACS faced as it adapted to irregular warfare operations and therefore does not have universal application.

The JAGIC concept actually evolved out of three experiences that occurred during recent major combat operations. The first was the development of air coordination elements by U.S. Air Forces Central and special operations forces during early operations in *Enduring Freedom*.[9] The second was the integration of a joint air coordination element with a special operations joint fires element during early operations in *Iraqi Freedom*, which resulted in a small JAGIC-like cell integrating air operations and joint fires in real time.[10] The third was the V Corps and 4th Expeditionary Air Support Operations Center experience in *Iraqi Freedom* during early 2003, in which the V Corps commander, Lieutenant General William S. Wallace, noted, "The critical ingredient in successful focusing of joint fires lay in the organization of the main command post to place the [all source collection element], the [Fires and Effects Coordination Cell] and the ASOC in close proximity for current operations."

Just as the Army has evolved over time, so has the TACS. Prior to 1965, ASOCs were aligned with each Field Army headquarters, but over time close air support coordination and control problems became apparent. In September 1962, a new concept for improved joint air-ground coordination was approved in principle and the respective Army and Air Force chiefs of staff approved the new system in 1965.[11] Among the revisions to the TACS, the ASOC was renamed the direct air support center (DASC) and located at the corps level. During the Vietnam War, up to six of these centers supported the American and Vietnamese corps, each working directly for the 7th Air Force Tactical Air Control Center collocated with the Military Assistance Command, Vietnam.

The Way Ahead

In September 2008, the Army–Air Force Board, General Officer Steering Committee, approved development and staffing of the JAGIC Tactical Operating Concept for the Air Force and Army chief of staff signatures. The Tactical Operating Concept is currently in final coordination at the Air and Army staff. The October 2008 CORONA (Air Force four-star conference) approved JAGIC development as one of a series of measures designed to enhance the TACS. The concept was subsequently briefed at the Army–Air Force Warfighter Talks in February 2009, where it was well received.

In the interim, a JAGIC concept of employment containing detailed TTP has been developed by the Air Force Command and Control Integration Center, working together with Air Combat Command's Joint Integration Division and the TRADOC Fires Center of Excellence Joint and Combined Integration Directorate.

Relocation and alignment of ASOCs with 25th Infantry Division and 1st Infantry Division is complete, and the 82nd Airborne Division ASOC alignment is happening in fiscal year 2012. As the ASOCs relocate to their aligned divisions, Air Combat Command's Joint Integration Division and TRADOC Fires Center of Excellence Joint and Combined Integration Directorate are contributing a joint training team to provide education, training, and exercise support for JAGIC implementation.

the Tactical Operating Concept is currently in final coordination at the Air and Army staff

An ongoing revolution in military operations has transformed airspace into the new high ground. All the Services are rapidly fielding new and more dynamic capabilities to exploit this environment. Past practices of deconflicting operations primarily through procedural control methods are proving to be insufficient for current and future operations as both the use of and the users of airspace proliferate and often limit and restrict, rather than enable and enhance responsive, integrated operations. While new systems and technologies will enhance airspace and fires integration in the future, today the JAGIC is demonstrating a very real capability to improve integration at the division level using existing personnel and systems. **JFQ**

NOTES

[1] Center for Army Lessons Learned, Air Force Office of Lessons Learned, Operation *Iraqi Freedom*–Operation *Enduring Freedom* Airspace Command and Control Collection and Analysis Team Initial Impressions, 2006.

[2] Field Manual (FM) 3-94 (initial draft), *Echelons Above Brigade* (Washington, DC: Headquarters Department of the Army, October 28, 2011), 3-2, paragraph 3-1 [sic].

[3] Joint Publication (JP) 3-09.3, *Close Air Support* (Washington, DC: Joint Chiefs of Staff, July 8, 2009).

[4] Warfighting experiments include the Fires Battle Lab Earth, Wind, and Fire 08 and 09, AFCIE (Air Force Capabilities Integration Environment) 10, AGILE (Air Ground Integrated Layer Exploration) Fire I, II, and III, Fort Leavenworth Mission Command Battle Lab Joint Forcible Entry Warfighting Experiment, and Austere Challenge 11.

[5] FM 5-0, *The Operations Process* (Washington, DC: Headquarters Department of the Army, March 2010), para. 5-22.

[6] Ibid., para. A-24.

[7] FM 3-94, 3-2, para. 3-1 [sic].

[8] The Joint Air Component Coordination Element is a component-level liaison that serves as the direct representative of the joint forces air component commander.

[9] Jody Jacobs, Gary McLeod, and Eric V. Larson, *Enhancing the Integration of Special Operations and Conventional Air Operations—Focus on the Air-Surface Interface* (Santa Monica, CA: RAND, July 2007).

[10] Robert B. Green, "Joint Fires Support, the Joint Fires Element, and the CGRS [Common Grid Reference System]: Keys to Success for CSJOTF-West," *Special Warfare*, April 2005.

[11] Concept for Improved Joint Air-Ground Coordination (Revised Tactical Air Control System), signed by the chief of staff, U.S. Air Force, March 19, 1965, and chief of staff, U.S. Army, April 28, 1965, 2.

Imperial War Museum

British troops raise Union Jack on Falkland Islands

THE FALKLAND ISLANDS CAMPAIGN OF 1982 AND BRITISH JOINT FORCES OPERATIONS

By RAYMOND E. BELL, JR.

The year 2012 marks the 30th anniversary of the 1982 British joint forces operations to recover the Falklands Islands in the South Atlantic Ocean from their Argentinean occupiers. Beginning as principally limited single-service operations by British air, naval, and marine elements, the campaign ended up as a major joint air-sea-land endeavor that turned out to be a "close run thing."

A review of this campaign merits a retrospective because of many factors—geographic, political, military, and even economic. But it is particularly salient from the perspective of how a successful joint military operation was conducted by the United Kingdom's armed forces over a vast distance with limited resources. This article revisits, in light of problems encountered and lessons learned, how the country's military establishment and its civilian counterparts were able on short notice to reoccupy a tiny British dependency

Brigadier General Raymond E. Bell, Jr., USA (Ret.), served in the New York Army National Guard and commanded the 5th Psychological Operations Group and 220th Military Police Brigade in the U.S. Army Reserve. He was on the staff and was a faculty member at the National Defense University from 1982 to 1985.

in a time-constrained, oncoming-winter operation. The focus must be on joint ground force combat while recognizing that the aerial and sea elements also played significant roles in obtaining the campaign's overall success.

Joint Participation

Combat began on April 25 with Royal Marine commando, Special Air Service, and Special Boat Squadron forces retaking Argentine-occupied South Georgia Island, located to the east of the Falkland Islands. This action was followed by the May 1 Royal Air Force (RAF) Vulcan bomber attack on Port Stanley's airfield; then on May 2, the British nuclear submarine HMS *Conqueror* sank the Argentine cruiser *General Belgrano.* Battle escalated as a British fleet consisting of some hundred ships to include frigates, destroyers, and two aircraft carriers sailed south and established a 200-mile Total Exclusion Zone around the Falkland Islands. The zone's purpose was to prevent further reinforcement of the Argentine force occupying East Falkland Island and to protect the British combat and logistics ships supporting the campaign.

The carriers with their helicopters and *Harrier* aircraft took up position well to the east of the islands to avoid attack by land-based Argentine naval and air force aircraft. British picket ships stood off the islands themselves both to shield the carriers and to intercept any Argentine aircraft that might try to interfere with ground operations on East Falkland Island where the bulk of Argentine forces were located.

In the meantime, diplomatic efforts to provide a peaceful solution to the crisis having failed, a British ground force had embarked in Great Britain and begun the 8,000-mile trek south to retake the islands. It was to be a major undertaking for a military establishment that was in the process of downsizing its expeditionary forces to concentrate on its North Atlantic Treaty Organization responsibilities.

Despite the turmoil engendered by the revamping of the British armed forces, in just over 3 weeks, from May 21 to June 14, a force of Royal Marine commandos, Army parachute troops, Nepalese Gurkha infantry, Special Air Service special forces, and guardsmen from Her Majesty's Coldstream Regiment of Foot Guards, as components of Royal Marine 3 Commando and 5 Infantry Brigade, "put boots on the ground" and retook the Falklands. The Royal Navy provided picket boat service, aerial coverage of the logistic support area, and gun support to the ground battle. The RAF, having sent long-range bombers against the islands' principal airfield, flew the *Chinook* helicopters transporting troops about the battle zone. The ground forces were staunchly backed by a joint combat and service support force. In addition to interservice aviation, artillery, and engineer participation, the service support establishment consisted of all manner of army, navy, and marine logistic elements to include Chinese-manned, contractor-operated logistics vessels. Backing the whole enterprise was the myriad of Royal Navy and commercially contracted ships, which often went in harm's way.

The Core Force

Initially led by Royal Marine Brigadier Julian Thompson commanding the Royal Marine commando brigade, and followed by the army brigade's commander Brigadier Anthony Wilson, the ground contingent had its task to oust the Argentineans occupying East Falkland Island cut out for it. The joint force slogged its way across peat bogs, flew over fields of rock, traversed craggy hills, and skirted the island by watercraft under abysmal weather conditions to confront a tenacious opponent entrenched around the island's capital and airfield at Port Stanley. The terrain combined with weather characterized by blowing snow, constant drizzle, squalls of freezing rain, and gusting wind to sorely try all combatants. Just as winter was setting in, the expeditionary force overcame Argentine resistance and the Falkland Islanders were able to assert their British affiliation once again.

The Falkland Islands (also known as the Malvinas) lay off the southeastern coast of Argentina within a relatively short distance of Antarctica and southern South America, where winter begins in June. Although ocean effects preclude much snow, other elements such as cold, fog, mist, and sleet are prevalent during winter. Any military operation involving combat on the islands requires a force habituated to fighting in harsh weather and on unforgiving terrain. British Royal Marine 3 Commando Brigade, around which the Falklands ground expeditionary task force was originally organized, frequently deployed to Norway on exercises and practiced in desolate regions in the United Kingdom. It was, of all British combat formations, the best suited for an expedition to the barren and inhospitable islands thousands of miles from the British Isles.

The primary elements of the commando brigade were three Royal Marine battalion-size infantry formations, 40, 42, and 45 Royal Marine Commandos. In support of these infantry organizations were commando-trained and -qualified personnel of the Royal Marines, Royal Navy, and British army. The Royal Marines contributed the brigade headquarters, signal squadron, and air squadron. Royal Navy doctors and medical technicians,

Imperial War Museum

Royal Marine commandos departing Teal Inlet on last leg of advance on foot to mountains

much as the U.S. Navy does for the Marine Corps, provided medical support as members of the Commando Logistic Regiment's Medical Squadron. The British army made a major contribution to the commando brigade in the form of 29 Commando Regiment, Royal Artillery, with three firing batteries of light 105mm cannon, 59 Independent Commando Squadron Royal Engineers (sappers), and the bulk of the Commando Logistic Regiment with transport, maintenance, and supply elements.

Royal Marine 3 Commando Brigade, a self-sufficient combat element, thus had the ability to operate as a separate entity. The brigade, however, was not large enough by itself to engage and defeat a numerically superior force such as Argentina had in the Falklands. It was, nevertheless, the ideal base upon which to forge an appropriate expeditionary force for the campaign.

Initial Force Augmentation

It was recognized early, therefore, that the commando brigade would have to be augmented if it was to accomplish an involved mission conducted so far from the United Kingdom. The initial infantry augmentation came from the British Parachute Regiment's 2nd and 3rd Parachute (2 and 3 Paras) Battalions. The airborne-qualified troops were also well conditioned to operate independently or as a component of a large force and had little trouble being integrated into the expeditionary commando brigade. The parachute unit leaders were resourceful and experienced, which made them a good match for their commando counterparts.

In support of the equivalent of five infantry battalions, the reinforced commando brigade included 3 and 4 Troops (platoons) of "B" Squadron, The Blues and Royals, with their light tracked-armored fighting vehicles. Each armored troop consisted of two *Scimitar*s and two *Scorpion*s, the former's principal armament being the 30mm high-velocity *Rarden* gun and the latter's a medium-velocity 76mm cannon. The armored troops came from one of Queen Elizabeth II's two royal household cavalry regiments, which are also charged with ceremonial horse-mounted duties in London. It was initially felt that the terrain on East Falkland Island would be inappropriate for tracked fighting vehicles as they would have to contend with rocky riverbeds, marshy ground, and jagged heights. As the U.S. Army discovered in South Vietnam, however, armor, in this case what amounted to light tanks, proved its value when deployed to the Falklands. There was no tank-versus-tank action in the islands, but the effective firepower and cross-country mobility provided by the light armored vehicles established that the supported infantry could easily have employed additional armor.

Also included in the task force was an enhanced "T" Battery (Shah Shiyah's Troop) 12 Air Defense Regiment, Royal Artillery, with *Rapier* and *Blowpipe* antiaircraft missiles. *Rapier* missiles were placed in the first landing waves to quickly protect the beachheads on the western shores of East Falkland Island against Argentine air activity. The task force leadership anticipated that the major threat to the initial landing would be by aircraft of the capable Argentine naval and air forces. The selected beachheads lay on the shores of Port San Carlos, Ajaz Bay, and San Carlos Water, which were surrounded by low-lying mountains. The missiles were emplaced on these heights so as to best engage any attacking enemy aircraft. *Rapier* effectiveness, however, was limited, although the gunners claimed 20 confirmed and probable Argentine aircraft kills. Argentine pilots attempted to bomb British ships and ground installations in the beachhead area from low altitudes, which meant the *Rapier*s launched from the mountaintops had to be fired down toward the water's surface. The *Rapier*s, designed to fire up into the sky, had to fire at negative elevations and had the tendency to fall off their pedestal mounts.

First Battle

The initial intent of the joint British ground effort was to establish a major presence in the form of a base of operations on East Falkland Island. Then through diplomatic efforts, the British government would try to persuade the large Argentine contingent on the island to return to the mainland. It quickly became evident that the Argentine force was going to stay on the Falklands because Buenos Aires insistently claimed sovereignty over the islands, which were so much closer to mainland Argentina than to Great Britain.

Once established on shore on May 21 and encountering minimum resistance, however, the British government quickly decided to launch an offensive against their foe, which was emplaced in great strength around Port Stanley on the east coast of East Falkland Island. For almost a week, Brigadier Thompson sought to build up an adequate logistical base to support anticipated ground operations. But in the meantime, the Royal Navy was suffering significant combat ship losses to Argentine air attacks, which made for bad press in the United Kingdom. All the while, the British Ministry of Defence (MOD), not aware of the logistical difficulties Thompson was facing, wanted the reinforced commando brigade to move swiftly against the final objective of Port Stanley.

Goose Green's capture caused a serious drawndown on the already limited supplies at the beachhead

The decision and prodding produced a dilemma for Brigadier Thompson because his brigade did not have sufficient logistical support or manpower to conduct the desired operation to invest Port Stanley. Nevertheless, pressure for a quick solution and rapid action from the commander of the naval task force and the British government in London made it imperative that some kind of attack be made. The MOD also soon realized that additional troops would be required to drive the Argentineans from the Falklands. As a result, the MOD dispatched an army infantry brigade, put together on an ad hoc basis.

Meanwhile, the Argentine air landing facility at the small community of Goose Green, a few kilometers southeast of the British beachhead, presented what appeared on the surface to be an easy objective to take. The capture of the installation could thus ease the pressure on Thompson to take the action demanded by the MOD and provide breathing space until the army brigade arrived. Two Para, with a minimum backup of fire and logistic support, was to perform the mission on May 27.

The army parachute battalion was led by Lieutenant Colonel H. Jones, who had prepared his men well for battle. For example, he doubled the number of light machineguns assigned to each section (squad), thereby greatly increasing his battalion's organic firepower. He also recognized that excellent

Imperial War Museum

Lifeboats carry British naval crew and soldiers to shore escaping RFA *Sir Galahad*, damaged by Argentine air strike

troop physical condition would be necessary in the islands' bleak environment, and on the trip south he saw to it that there was a great deal of conditioning in spite of cramped space on the ships.

Jones also stressed first-aid self-help for the wounded. In addition to the commando brigade's standard operating procedure of first-aid self-help, he issued a "puncture repair kit" made up of several elastic crepe field dressings used to put pressure on wounds to stop bleeding from exiting projectiles. With limited manpower he and other unit commanders did not want to detail men to carry litters or divert his paratroopers to assist their comrades when the troops could take limited care of themselves.

The May 28–29 attack on Goose Green was a success—but a costly one—and had an unfortunate impact on upcoming operations. Probably most importantly, Goose Green's capture exacerbated the logistic situation. It caused a serious drawndown on the already limited supplies at the beachhead. A special shortage was of larger caliber ammunition.

Lieutenant Colonel Jones, while personally leading a stalled attack to get it moving again, was killed by an Argentine machine-gunner. The foe's garrison with more than 1,400 men proved to be much larger than expected and was well dug in to resist an attack. Jones's death thus deprived the British of one of their most effective commanders.

An unforeseen challenge presented itself in the form of the large numbers of enemy prisoners taken at the objective. They became a major burden because they had to be taken care of properly according to the Geneva Convention. A large number of British personnel therefore had to be assigned prisoner-of-war duty, which tended to degrade overall operational effectiveness. There was also no place to keep the prisoners out of harm's way in the limited beach logistics area. As a result, they had to be evacuated to ships, which in turn were subject to Argentine bombing.

In the final analysis, the Argentine garrison at Goose Green represented no appreciable offensive threat to the British beachhead since the garrison's primary function was to service Argentine helicopters and light fixed-wing aircraft, not be a base for offensive operations.

The "Yomp" East and Reinforcements

Once the Goose Green garrison surrendered on May 29 and the additional British army infantry brigade was under way from Great Britain, Brigadier Thompson gave up ground command of the operation to Royal Marine Major General Jeremy Moore. On May 27, Thompson had dispatched 45 Royal Marine Commando and 3 Para east on foot over the tortuous terrain on what became known as the "yomp." Forty-two Royal Marine Commando was to be transported by *Chinook* helicopter, but the sinking of the modified container ship *Atlantic Conveyor* and the loss of three RAF heavy lift aircraft initially prevented the move. On May 31, however, a commando company was airlifted to Mount Kent in the center of East Falkland Island. On June 1, the remainder of the commando unit was flown by helicopter to nearby Mount Challenger, both mountains being unoccupied by the Argentineans.

The Blues and Royals armored fighting vehicles and the commando brigade's few light tracked vehicles accompanied the infantry in its trek across East Falkland Island. The armor proved fully capable of operating in the unfavorable terrain and greatly assisted in moving unit equipment, supplies, and weapons with their ammunition as well as personnel. The weather did not cooperate as the season advanced toward winter, but

the trek was made without serious incident. Supply of the columns, nevertheless, was a major challenge, and small watercraft from the British fleet skirted the island's shore bringing food and ammunition to forward logistic nodes. The first of these was established at Teal Inlet Settlement. Helicopters also moved the light artillery pieces, their crews, and ammunition to firing positions within range of the entrenched Argentineans.

While Thompson's Royal Marine 3 Commando Brigade, minus 40 Royal Marine Commando left behind to protect the beachhead, was in motion, 5 Infantry Brigade arrived in the battle zone. The brigade had a unique composition as it consisted of two battalions of Her Majesty's foot guards, the 1st Battalion Welsh Guards, and the 2nd Battalion Scots Guards, as well as the 1st Battalion 7th Duke of Edinburgh's Own Gurkha Rifles. The foot guard battalions, however, were not normal components of 5 Infantry Brigade as were the Gurkhas. Two and 3 Paras usually comprised the army brigade's combat elements so the brigade deployed to the Falklands as essentially an ad hoc organization.

The Gurkha riflemen were citizens of Nepal, and their participation in the British campaign had to be approved by the Nepalese government. Small in stature and tough in demeanor, the Nepalese had a ferocious reputation and were skilled with the curved native knife called the *kukri*. Word of their coming and their use of the kukri struck fear in the Argentine soldiers even before the Gurkhas arrived. The Gurkhas are known as world-class fighters and had fought for the British for decades. In World War II, Gurkha battalions fought on such battlefields as Burma. Over the postwar years, however, the number of battalions serving the British government declined significantly. Interestingly, the inclusion of the Gurkhas in the brigade added another dimension to the organization of the expeditionary force which was now not only a "joint" entity, but in reality a "combined" one as well.

Logistic Complications

The two foot guard infantry battalions were, along with the paratroopers and commandos, considered among the elite of British troop formations. For the guardsmen, it seemed almost a right instead of merely a duty to participate in the campaign. Unfortunately, from a logistic point of view, the foot guards' participation raised complications well before they arrived in the combat zone. They had many supply obstacles to overcome even before they came face-to-face with the Argentine forces. Among the challenges was the inadequate equipment they possessed to operate in the austere and blustering islands' environment. Some nongovernment cold weather gear, for example, had to be purchased from commercial sources. In another instance, the MOD issued the infantry brigade 2,000 pairs of arctic pants, but only 1,000 cold weather jackets. Not until the unofficial intervention by a member of the House of Lords whose son was a guardsman was the shortage rectified. The supply situation notwithstanding, the guardsmen's physical condition was adversely influenced by duty in ceremonial events around London and in a less demanding environment than was to be encountered in the Falklands, where proper weather attire and good physical condition were mandatory. Nevertheless, in the best British army tradition, the guardsmen, regardless of supply deficiencies and lack of physical condition readiness, went into battle determined to excel.

the guardsmen's physical condition was adversely influenced by duty in ceremonial events around London and in a less demanding environment than the Falklands

The British battle plan was relatively straightforward—move as quickly and directly as possible to engage and defeat the Argentinean forces dug in around Port Stanley. But a definitive logistics plan, however well conceived, could not take into proper account the execution challenges ahead that haste and poor management above brigade level were to cause. The result was near-chaos, and but for the resourcefulness and determination of logisticians, especially those in direct support of the troops on the ground, the final result can best be described as a "close run thing." The logistic operators of the British merchant marine, commercial entities, Royal Air Force, Royal Navy, British army, and Royal Marines had to overcome significant obstacles of terrain, weather, and gross mismanagement of resources more than effective and tenacious enemy opposition.

Right from the beginning of the campaign, haste resulted in guaranteed confusion. Had some tracking mechanism akin to present day bar coding been employed, identification of items required for combat operations such as ammunition, critical weapons systems, and food might have saved many hours of untangling the contents of loads on the various commandeered merchant ships. As it was, ships were loaded helter-skelter with items needed first on the battlefield being loaded first instead of last on the transports, making supplies and equipment, much of it being on the vessels' bottoms, not readily accessible. There was no organized manifest system, so logisticians seldom knew what was on what merchant ships when they arrived at the East Falkland Island beachhead for unloading. There were incidents where ships arriving to be unloaded had to be returned fully loaded to the logistics marshaling area because there was no need for their cargo at the time. Often complicating the situation was that the discharge of stores had to be made at night because Argentine aircraft were active over the beachhead during the day and the ships were inadequately armed to protect themselves. At the same time, *Rapier* and *Blowpipe* antiaircraft missiles emplaced to protect the ships and logistic nodes failed to receive high marks because of design features, sensitivity to climatic conditions, and tactical employment. As luck would have it, many of the attacking Argentine pilots in releasing their bombs at low altitudes did not allow sufficient time for the bombs to arm and explode.

The fastest way to move across the battlefield and carry a large load was by helicopter, and the best helicopter to perform such missions was the American-built CH-47, the *Chinook*, flown by RAF pilots. The Royal Air Force initially sent four CH-47 helicopters to the Falkland Islands, all on the converted container ship *Atlantic Conveyor.* Argentine aircraft sank the ship with a French-made *Exocet* missile, and all but one of the heavy lift aircraft as well as many *Wessex* helicopters were lost. The smaller Royal Navy *Wessex* and *Sea King* helicopters ended up carrying much of what turned out to be a major load. They and the single available *Chinook* nevertheless performed incredibly well. The helicopters often flew beyond their mandated operational hours under very challenging weather conditions, and their mechanics performed extraordinary feats under primitive conditions.

Heavily laden British soldiers wait to embark by helicopter

Imperial War Museum

The worst loss of personnel did not occur on the battlefield but in Bluff Cove at a supply distribution point behind the frontlines. Argentine aircraft attacked the two landing ships logistic *Sir Galahad* and *Sir Tristam*, which were carrying ammunition, vehicles, supplies, and soldiers of the Welsh Guards and medical personnel of 16 Field Ambulance. The sudden arrival of the Argentine aircraft caught Chinese crewman, many Welsh guardsmen, and medics on board *Sir Galahad* as the troops prepared to be ferried ashore. The loss of life, supplies, vehicles, and equipment was profound.

At the same time, the medical support provided by surgical teams of the Royal Navy, both those integral to the Commando Medical Squadron and attached, and the Royal Army Medical Corps personnel to include the parachute medics, was truly outstanding. For example, surgeons working in a makeshift operating theater in the Ajax main field medical dressing station, with two exploded bombs lodged in the roof, managed to save the lives of all the wounded who reached the facility. Medical personnel led by Surgeon-Commander Rick Jolly worked around the clock in the unsophisticated and grubby environment of an abandoned meat packing plant, as well as in rudimentary field locations. Of those initially treated ashore in the various medical field dressing stations only three died later on the hospital ship SS *Uganda.*

As the logisticians were bringing men, supplies, and ammunition while retrieving and treating the wounded, seven infantry battalions moved aggressively against their Argentinean foe. If their advance was hindered, it was less by Argentine resistance than by their own footwear. The government-issue direct molded sole boots, when immersed in salt water, retained the residual salt crystals, which became magnets for further moisture, so wet boots never dried out. The footwear failed to give personnel adequate protection and ended up causing many casualties. Ironically, the Argentinean troops were equipped with superb leather boots which became much sought after by British troops as spoils of war.

The resourceful British soldier and marine also learned to contend with the drinking water situation. Potable water was at a premium, and available groundwater had to be treated before it was drinkable. The fighting man soon learned that even when properly treated, his coffee mug often ended up with a bottom full of murky sludge. British combatants quickly learned to drink only the uppermost portion of fluid in a cup.

The combination of circumstances, physical environment, and mismanagement sorely tested all those men charged with

providing logistical support to task force personnel. From the most junior helicopter fuel replenishment technician to the most skilled surgeon, it was their exemplary performance that saved the campaign from disaster. That they came from all the British armed services and civilian support personnel sources spoke volumes for ultimate success.

Battlefield Success

The final attack consisted of a three-phase offensive. The first phase commenced the night of June 11 when the British overcame Argentine resistance on the three mountains, Two Sisters, Mount Harriet, and Mount Longdon. After a stiff fight, 45 Royal Marine Commando took Two Sisters, 42 Royal Marine Commando captured Mount Harriet, and 3 Para overran Mount Longdon. The medical field dressing stations had their hands full as overworked helicopters evacuated casualties after bringing forward ammunition, food, and even mail.

A Plethora of Problems

The British Falklands joint forces campaign was a success but at a price. Salient problem areas common to all aspects of the combat and logistical operations were many. For example, the loss of heavy lift rotary-wing aircraft, especially the three *Chinook*s and the six *Wessex* utility helicopters on the *Atlantic Conveyor*, severely taxed all manner of deliveries for the three armed services. The limited availability of Royal Navy and RAF *Harrier* combatant aircraft made air superiority over the large Argentinean air contingent problematical and resulted in severe loss of ships

the lack of unity of command from the British MOD down to the major combatants was strongly felt

The Phase I success of Royal Marine 3 Commando Brigade and 5 Infantry Brigade encouraged a fast implementation of a Phase II, but ammunition for the supporting artillery had become scarce. General Moore postponed the attack for a day, allowing the needed ammunition to be brought forward while unit commanders reconnoitered the terrain. The phase objectives were Wireless Ridge to be taken by 2 Para, Tumbledown Mountain by the Scots Guards, and Mount William by the Gurkha Rifles. The attacks went forward under harsh weather conditions of high winds and snow showers, which also hindered the helicopter evacuation of the wounded and the bringing up of ammunition and supplies. Capture of the terrain features placed the expeditionary force in commanding positions around the final Phase III objective of Port Stanley and its airfield.

The success of Phase III was assured by the Argentine defenders retreating into Port Stanley and its immediate environs. The final phase saw the British attacking from three directions in what became a rout. The Argentine resistance folded as the tank-supported infantry captured the last key defensive positions around the port town. That the collapse was quick was fortuitous because British supplies and especially readily available ammunition were becoming critical commodities. The Argentinean defenders had already begun to surrender in large numbers as the British advanced, and on June 14 the Argentine high command in the Falklands, with its troops hemmed in around Port Stanley, capitulated.

of the Royal Navy and complicated provision of logistical support to the ground forces. The lack of unity of command from the British MOD down to the major combatants was strongly felt by those charged with logistically supporting the troops and fighting the enemy.

There were, however, three problem areas that impacted seriously on joint land combat operations. First, there was a lack of adequate logistic infrastructure as the Commando Logistic Regiment, essentially a battalion with a few British army attachments, carried the entire burden of supporting eight infantry battalions, five artillery batteries, and a host of other units. Second, the inadequacy of equipment such as winter clothing for the army troops, to include an unsatisfactory combat boot, had a detrimental effect on the physical condition of all those men exposed to salt water. Finally, an ad hoc battle and logistic organization, equivalent in strength to a downsized infantry division, was literally assembled on the field of battle. The cobbling together of a joint ground combat force of commandos, paratroopers, guardsmen, Special Air Service troops, and Gurkha infantrymen with their supporting arms and services generated confusion and delays, thus severely taxing the accomplishment of the force's missions.

Lessons Learned

The campaign's ground lessons learned were fundamental. There was a need for a well-established, sound, and flexible command and control system as well as adequate logistics planning at the division level. The inadequate combat and logistical organization brought forth the realization that it is logistics that drives the battle. Resource management requirements needed closer attention, especially in the supply and distribution of ammunition and the availability of sufficient helicopters. The performance of equipment—not only of adequate clothing to include such mundane yet important items as boots, but also the ability of weapons systems to deliver fire and traverse terrain—required more appropriate consideration. Finally, operational procedures, to include combat loading of ships, required refinement and inclusion in standard operating documents.

The Argentine forces on the Falkland Islands outnumbered the British expeditionary force. But the Argentineans turned out to be no match for a joint task organization which, despite the challenges it faced, prevailed decisively. The outcome of the campaign in the long run, however, was basically decided by the professionalism, sturdiness, and tenacity of the British serviceman and his international partners. As a result, the Falkland Islands remain inhabited today by citizens loyal to the British crown. **JFQ**

Victory at Risk: Restoring America's Military Power: A New War Plan for the Pentagon
By Michael W. Davidson
Zenith Press, 2009
256 pp. $25.00
ISBN: 978-0-7603-3557-4

Reviewed by
JAMES CRICKS

In his first book, Michael Davidson, a retired Army National Guard major general, has issued a clarion call for the U.S. military to fundamentally change course or face the sobering prospect of losing our next war. As a decorated citizen-Soldier whose long service began with Vietnam, Davidson advocates a renewed emphasis on preparing for major conflicts while doubting the wisdom of the "war on terrorism." He reserves special criticism for the tenures of Defense Secretaries Robert McNamara and Donald Rumsfeld as periods of wrongheaded arrogance by civilian officials. His analysis of American military history since World War II provides an important backdrop for his argument that poor civil-military relations have led the United States to an extremely dangerous strategic position. Our force is exhausted and out of balance. Returning to the model of President Franklin D. Roosevelt and General George C. Marshall, where military advice was given greater weight, would be an important step toward crafting a sensible defense strategy devoid of political posturing. The solutions he offers are wide ranging and would require radical movement away from Afghanistan and current defense strategies.

The book is divided into three parts and begins with a survey of the current poor state of military readiness for conventional conflicts. Soldiers need more time, training, and resources. Our war plans are unrealistically optimistic and framed by Pentagon battles between the Services. The Army's funding bears little relation to its missions, and ground forces have been overtaxed. We have borrowed from long-term equipment modernization to the short-term costs of contingency operations. He does single out the special operations community for praise, complimenting their joint approach across the full spectrum of military operations.

The second and third parts of the book illustrate his key points about needed defense reforms. Based on his experience in key National Guard and Army Reserve positions, Davidson makes the case for a fundamentally different defense structure and a return to a citizen-soldier army. He assesses that the Pentagon has a "rush-to-war" mindset that favors the expensive Active-duty force when every major American war has been fought and won by citizen-soldier armies. Like Morris Janowitz and other Republican theorists, he views military service as a positive obligation that will increase the connection between the military and American people. We will have more time to build an army with broad-based national service now that the Cold War has ended. Although he acknowledges that the conventional warfight is extremely complex, his prescriptions are not as detailed as his strong historical examples. He does not discuss how an Army with more conventional combat National Guard forces would overcome the challenges of peacetime and postmobilization training that were apparent in roundout brigades during Operation *Desert Storm*. During that war, the Army's premobilization information on the proficiency of its roundout brigades overstated their capabilities and created significant capability shortfalls. With limited peacetime training, it is still likely the lack of opportunities for realistic training and constraints on the extent of collective training will limit Reserve units to lower levels of organization.

Like military analysts such as Colin Gray and Gian Gentile, Davidson prefers a shift in focus toward preparing for a major war. Standing forces would be used to contain crises and small wars. They would also serve as the base from which the citizen-soldier army would expand. Although he acknowledges the debilitating impact of engagement missions and our escalating workload, he would have deployed forces to Rwanda and Darfur. He still contends that we must apply more strict criteria to the application of military power in the defense of America. His willingness to consider new missions in Africa appears to be in contradiction with his opinion that we must more carefully expend our military resources.

He recommends that we begin by identifying our threats and then devising a strategy to meet those threats. Davidson identifies "expansive" China as an emerging threat with a modernizing force and an expanding navy. Major wars matter, so defeating conventional threats must be our core mission.

It is difficult to agree with Davidson's premise that all America's major wars came as surprises. Germany and Japan were vying for greater global roles before shots were fired in World War II. We may not have unambiguous warning of an impending conflict, but as in World War II, we will probably have strong indications of intense military competition.

Some of his harshest comments are aimed at Pentagon civilians stifling the sounder advice of generals and admirals. Secretary Rumsfeld decreased the likelihood of policy dissent and rethinking when policy changes were needed. The examples of Generals Marshall and Creighton Abrams provide keen insights into how courageous decisions could provide the basis for improved military capabilities. Military officers should have more forcefully presented their assessments directly to the President. Advocating more authority for the Chairman of the Joint Chiefs of Staff, he envisions senior generals and admirals defining the next defense strategy. Although he does not state it specifically, it appears he would question the necessity of the Chairman and Secretary of Defense both publishing strategies. As was the case with Goldwater-Nichols Department of Defense Reorganization Act of 1986, Davidson believes much of what needs to be fixed in the Pentagon will be fixed from outside.

It is hard to ignore the passion and thoughtful experience Davidson brings to the subject of defense reform. There is no doubt the role of the citizen-soldier should be redefined to better meet our post–Cold War requirements. General Craig McKinley, USAF, chief of the National Guard Bureau, has already discussed focusing on helping the Nation build partnership capacity worldwide. Somehow the linkage among the Department of Defense, Department of State, and U.S. Agency for International Development efforts must be fundamentally addressed in a whole-of-government approach. The Reserve components could be an important part of a solution, especially if they share Michael Davidson's desire to contribute fully to the defense of freedom. This important work enriches the reform debate and deserves to be studied by strategic planners as Americans consider the future of the military after current contingency operations. **JFQ**

James Cricks is a Joint, Interagency, and Multinational Operations Instructor at the U.S. Army Command and General Staff College.

Gangs, Pseudo-Militaries, and Other Modern Mercenaries: New Dynamics in Uncomfortable Wars
By Max G. Manwaring
University of Oklahoma Press, 2010
256 pp. $45.00
ISBN: 978-0-8061-4146-6

Reviewed by
NADER ELHEFNAWY

Famed counterinsurgency analyst Max G. Manwaring extends his research into the subject of "uncomfortable wars" in his newest book, *Gangs, Pseudo-Militaries, and Other Modern Mercenaries*. As Edwin C. Corr notes in the foreword, Manwaring focuses on the "asymmetrical, irregular . . . nonstate actors" he collectively terms *gangs*. Highly diverse in their size, sophistication, capacity and propensity for violence, relationships with state actors, and objects, these gangs range from old-fashioned guerrillas to paramilitary and vigilante organizations, from propaganda-agitator cells to criminal organizations of a great many kinds. However, they have in common their endeavoring to overthrow, capture, or simply weaken individual states or the state system as a whole to attain their goals, and in the process, their becoming the principal war-making entities of our era.

After establishing the issue and its importance in his preface, introduction, and first chapter (supplemented by John F. Fishel's historical survey of the issue in an afterword), Manwaring moves on to the five chapters of case studies of gangs that comprise the core of the book. These studies examine the impact of Argentine "*piqueteros*" on the country's domestic politics; the role of Colombia's gang problem in a security situation dominated by an "unholy trinity" of insurgent, paramilitary, and drug trafficker activity; Venezuela's "use of popular militias and other instruments of power" to develop a regional hegemony capable of challenging the United States; al Qaeda's activities in Western Europe; and Mexico's private armies, in particular the Zetas, respectively.

There is much to be said for Manwaring's study. While terrorism and guerrilla warfare and the like have long been the subjects of a vast literature, there has been little effort to examine many of the other kinds of nonstate actors he discusses in comprehensive ways. Additionally, as Manwaring himself points out, "strategic theory and action have played little part in the debate and actions involving contemporary irregular warfare as a whole." The book is refreshing on both counts, examining this underexplored territory in depth, and not only demonstrating the applicability of strategic literature, old and new (from Sun Tzu, Machiavelli, and Clausewitz, to Lenin and Mao, to Rupert Smith) to the subject, but also effectively applying it to individual case studies and the broader situation and charting out possible responses.

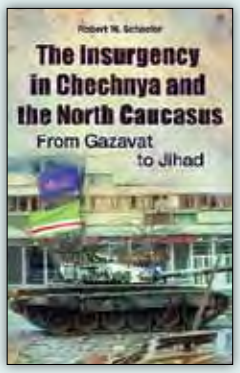
Unfortunately, the book suffers from a number of weaknesses. Some are comparatively minor, like a jargon-heavy prose style and a tendency to make extensive use of terms with multiple, politically charged, and contentious definitions in unconventional and unfamiliar ways (as with his use of *democratic socialism* and *neopopulism*), though I found that Manwaring always managed to make his essential points clear in the end. Another weakness is a propensity for understating the response of the United States and its allies to particular threats, as when the author suggests that Washington's support to Bogota has focused exclusively on the drug war (neglecting the country's insurgency), and claims that al Qaeda has been treated as a law enforcement problem.

A deeper issue is the book's methodology, about which I have some reservations. The most important of these is that all five of the case studies concern ongoing conflicts. That they are not resolved complicates their assessment in ways that would not be the case with wars or other situations where the analyst can examine ultimate outcomes. Related to this is Manwaring's tendency to emphasize the most grandiose aspirations of the actors he examines rather than actual events to date, and to take the feasibility of those aspirations as a given, rather than critically assessing the actors' capabilities to realize those aspirations. This is most pronounced in his assessment of Venezuela, though it is also prominent in his chapter on al Qaeda. (Manwaring classifies al Qaeda as a "hegemonic" actor. While such a classification may reflect its aspirations, this says nothing about its actual capabilities or their limits.)

Fortunately, the book's other three case studies are more solidly grounded, and the chapters on Argentina, Colombia, and Mexico are far more robust, lucidly elaborating the tangled domestic situations in those countries. Additionally, the concluding chapter distills the lessons of Manwaring's examinations and suggests an abstract but logical foundation for a theory to counter such actors emphasizing legitimate governance, the use of "soft" as well as "hard" power, and a unity of effort among the components involved (as war is now best thought of as a "sociopolitical matter," in which force is just one instrument). Manwaring also works to link such action with a proposed grand strategy that would move American policy from "short-term self-protection," "short-term compassion," and "cosmetics" conducted through "ad hoc, negative and reactive crisis management" responses strongly characterized by "military tactical-operational level" action to pursuit of "an organized and effectively enforced system of general international peace."

Most of this is a restatement of old principles, but the recognition that these principles apply to the irregular warfare conventional military and political theorists have regarded as beneath acknowledgement is one of Manwaring's principal contentions, and on the whole he is successful in demonstrating the point. As a result, the book usefully extends some worthwhile lines of recent thought and lays some foundations for future work, making it a meaningful if imperfect contribution to the underdeveloped literature on its subject. **JFQ**

Nader Elhefnawy has published widely on international security issues. He holds a degree in International Relations from Florida International University.



The Insurgency in Chechnya and the North Caucasus: From Gazavat to Jihad
By Robert W. Schaefer
Praeger Security International, 2010
303 pp. $59.95
ISBN: 978-0-313-38634-3

Reviewed by
JOHN W. SUTHERLIN

Winston Churchill famously remarked that Russia is "a riddle, wrapped in a mystery, inside an enigma." That would make Chechnya, by virtue of being inside Russia, nearly impossible to figure out. Yet Robert Schaefer attempts to do exactly that in one of the most important works on Chechnya's insurgency to date. His analysis is relevant to all such conflicts as Schaefer provides unambiguous recommendations on how to cope with all insurgencies. This is critical to the entire work since "insurgencies cannot be viewed like other conflicts because they are a fundamentally different type of warfare" (p. 2).

According to Schaefer, there are "four prerequisites" that must be present before a particular country sees an insurgency develop: lack of government control or illegitimate government (pp. 13–15), a common ideology (pp. 16–17), effective leadership for the insurgents (pp. 17–19), and a vulnerable population (p. 19). The last of these is most important to Schaefer. Insurgencies (and the counterinsurgencies) are fights over controlling populations and giving them something of value to fight for.

Next, Schaefer describes "common characteristics of insurgencies" (pp. 20–30). Many will read this section and others and wonder why the literature review is so light. Simply put, why is there so little provided to justify these claims? In many ways, this section is merely a foundation for the chapter on terrorism (pp. 31–48). Schaefer puts terrorism in the context of being one of many tools of insurgents. He then brings in the specific case study of Russia and Chechnya as an example of how the larger power has misread the smaller one and is, in fact, fighting the wrong kind of war. He firmly asserts, "The Chechen insurgency is alive and well and in better shape than it has been for much of the last 400 years" (p. 48). That is a long way away from what Vladimir Putin claims.

The next couple of chapters on Chechen history and the centuries-old conflict with Russia seem a bit out of place when first reading the book. This was a concern because *The Insurgency in Chechnya* has no consistent methodology, but employs a hodgepodge of histories, personal experiences, and a modest literature review to buttress Schaefer's contentions. Still, by the time chapter five is presented, Schaefer is back on solid ground. From 1980, the reader gets the sense that he could provide a minute-by-minute account of the Russian-Chechen conflict. He is able to tie the prerequisites and common characteristics sections with those on Chechen history and the Russian responses to provide a succinct summation: "To say that there had been a lack of government control in Chechnya prior to the declaration of independence would be a gross understatement . . . there was no Russian control" (p. 122). Thus, a political vacuum was fostered and external (that is, Turkey and Saudi Arabia) and Islamic extremists crammed the region with weapons and an ideology: "Wahhabism first entered the North Caucasus through Dagestan around 1986, although it would take another ten years before it would reach Chechnya" (p. 163).

When Schaefer reaches chapter eight on the Russian counterinsurgency (pp. 195–232), the reader will understand why earlier chapters were needed. Schaefer details Russia's counterinsurgency strategies and even provides a diagram (p. 201) to offer more explanatory power to his argument. But as he describes the Russian response, he is quick to point out why this has been inadequate to end the hostilities. When Russia sought to convince the "uncommitted population to support the war . . . it was effective in mobilizing those pro-Russian groups that lived in the North Caucasus region" (p. 204) and thus use counterinsurgency tactics against what it publicly called terrorists. It is only when Russia began using counterterrorism tactics that Chechens turned the tables.

However, Chechnya turned the tables internally (with locals) and internationally (using terrorist organizations that were willing to lend support or tactics in exchange for an Islamic-based agenda being adopted). Schaefer calls this the rise of the "Caucasus Emirate" (p. 233). Here, the objectives (at least in the short term) were distorted. With a religious ideology and external funding, Chechnya could remain relevant to the Russians and the world by "conducting well-planned attacks on high value targets" (p. 249). Furthermore, it could be a place where those leaving the fight in Afghanistan or Iraq could go and fight similarly using remarkably similar rhetoric.

But for how long? True, this conflict has been on and off for centuries. How important is it to the West? For Russia, it is vital that the West remain hooked to Caucasus natural gas and allow Russia to frame Chechnya as an internal matter with outside terrorists. This allows them a free hand, but will it work? Schaefer notes that each side has different objectives and is fighting a different war (p. 273). The Chechen insurgents remain elusive and "merely continue to move from one area to the next to avoid capture and attack government targets at will" (p. 281).

This impossible situation seems destined to continue because as long as there is just one insurgent, he can claim the righteousness of his cause and inflict damage to innocents. For Russia, every lost bridge, road, school, factory, or, in the worst case, human fatality to the insurgents is a nagging reminder that its legitimacy is being diluted and damaged.

Schaefer's work reflects the paradoxical world of insurgencies and counterinsurgencies using a real case study better than anything I have encountered lately. In terms of analyzing the North Caucasus region, there may be nothing as useful. Undoubtedly, there are lessons for U.S. policymakers here. Schaefer demonstrates that even mysterious riddle-laden enigmas can be understood. **JFQ**

John W. Sutherlin, Ph.D., is Associate Professor of Political Science and Co-Director of the Social Science Research Laboratory at the University of Louisiana at Monroe.

The Role of Multinational Joint Doctrine

By THE JOINT CHIEFS OF STAFF J7 JOINT EDUCATION AND DOCTRINE DIVISION

The nature of the challenges to the United States and its interests demand that the Armed Forces operate as a joint team, closely integrated with inter-organizational and multinational partners across the range of military operations.

—Joint Publication 1, *Doctrine for the Armed Forces of the United States*

The purpose of joint doctrine is to enhance the operational effectiveness of U.S. forces. It represents what is taught, believed, and advocated as what is right (that is, what works best). It also provides the national position for multinational doctrine and serves as a basis for multinational or interagency coordination during joint operations.

Whenever U.S. forces operate as part of a multinational force, they follow multinational joint doctrine and procedures to the extent that the guidance is consistent with U.S. law and policy. Joint Publication 1-02, *Department of Defense Dictionary of Military and Associated Terms*, defines *multinational doctrine* as "Fundamental principles that guide the employment of forces of two or more nations in coordinated action toward a common objective." Multinational doctrine enhances the interoperability of coalition forces and provides fundamental considerations used to determine command relationships and the assignment of missions, objectives, and tasks. In all cases, multinational doctrine must be well known, universally accepted, and commonly understood to be useful.

Allied Joint Doctrine Framework

Within the North Atlantic Treaty Organization (NATO), allied joint doctrine (AJD) provides the operational framework for operations conducted by Alliance members and partners, non-NATO nations, and other organizations. NATO policy guides AJD development by providing the baseline for the doctrinal principles or fundamentals. NATO's policy and doctrine developers strive to closely coordinate their efforts, ensuring that the relationship between NATO policy and military doctrine is consistent and mutually supportive.

NATO's doctrine is aligned within the AJD Architecture (AJDA). The AJDA is comprised of Allied Joint Publications (AJP) and supporting Allied Publications (AP). There are currently 45 approved AJPs and four APs in the AJD portfolio. The majority of AJPs (28) reside in the Operations series.

AJDA is organized into two levels. Level-one publications contain overarching doctrine, namely, NATO's "capstone" publication, AJP-01, *Allied Joint Doctrine*, as well as "keystone" publications AJP-2, *AJD for Intelligence, Counter-Intel, and Security*; AJP-3, *AJD for the Conduct of Operations*; AJP-4, *Allied Joint Logistics Doctrine*; AJP-5, *AJD for Operational-level Planning*; and AJP-6, *AJD for Communication and Information Systems*. Level-two publications contain supporting joint doctrine aligned to specific functional areas.

Allied Joint Doctrine Development

Current AJDA has more than doubled since 2005, expanding to include topics across the spectrum of military operations that now include AJP-2.1, *Intelligence Procedures*; AJP-2.7, *Joint ISR*; AJP-3.14, *Force Protection*; AJP-3.3, *Air and Space Operations*; AJP-3.4.9, *Civil-Military Cooperation*; AJP-3.10, *Psychological Operations*; AJP-3.5, *Special Operations*; AJP-4.0, *Allied Joint Logistics*; AJP-4.5, *Host Nation Support*; AJP-5, *Operational Level Planning*; and AJP-6, *Computers and Information Systems*. Six of the 28 member nations serve as AJD custodians, which is not to say that only six nations are contributing. Virtually every custodian team and working group includes contributions from all 28 member nations. Since 2009, NATO approved or will soon promulgate 10 new joint publications, among them doctrine for military support to stability and reconstruction, counter-intelligence, and counterinsurgency. Additionally, AJD development is under way for geospatial intelligence and stability policing. The AJP-2 series, currently consisting of six AJPs, is potentially expanding to include doctrine on signals

intelligence, imagery intelligence, measurement and signature intelligence, open-source intelligence, and collection coordination and intelligence requirements management.

Responsibility for the development, management, and standardization of AJD lies with the Allied Joint Operations Doctrine Working Group (AJODWG). The primary mission of the AJODWG is to enhance the interoperability and thus the effectiveness of NATO forces when planning and conducting joint operations through the provision of AJD, with the emphasis on doctrine at the operational level. The AJODWG consists of delegates from NATO member nations, the International Military Staff, and the two strategic commands (Allied Command Transformation and Allied Command Operations). The AJODWG has many responsibilities; however, its principal roll is to ensure that AJD conforms to NATO policy and guidance. The working group reviews proposals that identify doctrinal voids and recommends doctrine development to fill those voids. Additionally, the group ensures that AJD content is standardized in terms of layout, presentation, and format. The AJODWG is also responsible for harmonizing the AJDA—ensuring coherence and consistency with NATO policy across the level one keystone and capstone publications as well as vertically between the level-one and level-two publications.

The AJODWG meets in March and September annually at NATO Headquarters to review the AJDA to determine continued validity and, where necessary, recommend revision, consolidation, or cancellation of AJPs. In addition, the AJODWG identifies doctrinal voids, identifies and develops new doctrine proposals, and reviews lessons learned from recent operations, exercises, and experimentation for their potential for new or amended doctrine proposals to enhance interoperability.

Currently, the AJODWG is managing a number of doctrine initiatives. First, AJP-3.4.0, *Allied Joint Doctrine for Non Article 5 Crisis Response Operations*, is being reviewed as a potential thematic doctrine for AJP-3.4 series publications (*Stability and Reconstruction, Counterinsurgency, Peace Support, Non-Combatant Evacuation, Military Support to Civil Authorities, Civil Military Cooperation, and Stability Policing*). Second, while security force assistance (SFA) remains a relatively immature topic in NATO, there exists the potential for developing SFA doctrine. Third, recent and anticipated NATO policy changes will inform the eventual revision of AJP-01 and AJP-3, *AJD for the Conduct of Operations*. The AJODWG will address recent policy developments on environmental protection, the Comprehensive Approach (NATO's response to crisis management involving political, civil, and military instruments of power), and strategic communication, and include lessons learned from operations in Libya. Finally, AJP-5, "AJD for Operational Level Planning," was drafted and is awaiting member nations' ratification and should be approved as formal doctrine by this fall.

The U.S. Role in AJD

The Joint Staff J7 leads the effort in providing the U.S. military's position on warfighting guidance to all the Alliance nations. The Chief of J7's Joint Education and Doctrine Division (JEDD) serves as the U.S. Head of Delegation (HOD) to the AJODWG. The HOD represents the Chairman and J7 within the multinational AJOD forum, responsible for expressing the official position of the United States and ensuring that U.S. roles, extant capabilities, and warfighting philosophy are accurately represented throughout the AJDA. In this capacity, the HOD approves U.S. ratification responses for AJPs and reviews emerging multinational doctrine publications for consistency with U.S. law, regulations, and approved and emerging joint publications. Additionally, the United States serves as custodian, or author, of 10 AJPs and 1 AP, *Joint Symbology*. By taking ownership of 11 of the 49 publications in the AJDA, the United States continues its enduring commitment to further develop of NATO's AJD portfolio. Most noteworthy among AJD development is AJP-3.4.5, *Allied Joint Doctrine for Military Support to Stability and Reconstruction (S&R)*, which is expected to be approved this fall. It defines planning considerations in the event that NATO provides S&R support until the relevant nonmilitary authorities are able to assume the duty. It also emphasizes cooperation with civilians in accordance with NATO's Comprehensive Approach—engagement of the requisite civil and military elements of international power to end hostilities, restore order, commence reconstruction, and begin to address a conflict's root causes.

For the upcoming AJODWG (September 24–28, 2012), significant U.S. input to the working group will include doctrine updates for several publications. Additionally, the U.S delegation will provide a timely doctrinal update to inform NATO's early development efforts in the interrelationship among cyberspace operations, information operations, electronic warfare, military information support operations (formerly psychological operations), and strategic communications and communications strategy.

Conclusion

In a globalized world, nations will be less likely to conduct operations unilaterally; they are more likely to participate as part of an alliance or coalition formed to achieve internationally agreed objectives. Cooperation between nations is necessary to working effectively in a coalition environment, allowing political and military objectives to be achieved when unilateral action would be impractical or undesirable. Developing, accepting, and following sound doctrinal principles are the important first step when operations are to be conducted by multinational forces.

The fundamental challenge in executing multinational operations is the effective integration and synchronization of available assets toward the achievement of common objectives. Successful planning, execution, and support of multinational military operations require clearly understood and thoroughly implemented allied joint doctrine. **JFQ**

Joint Publications (JPs) Under Revision

- **JP 2-0**, *Joint Intelligence*
- **JP 2-03**, *Geospatial Intelligence Support to Joint Operations*
- **JP 3-00.1**, *Strategic Communication and Communications Strategy*
- **JP 3-04**, *Joint Shipboard Helicopter Operations*
- **JP 3-07.4**, *Counterdrug Operations*
- **JP 3-11**, *Operations in Chemical, Biological, Radiological, and Nuclear Environments*
- **JP 3-12**, *Cyberspace Operations*
- **JP 3-13**, *Information Operations*
- **JP 3-16**, *Multinational Operations*
- **JP 3-18**, *Joint Forcible Entry Operations*
- **JP 3-27**, *Homeland Defense*
- **JP 3-28**, *Defense Support of Civil Authorities*
- **JP 3-32**, *Command and Control for Joint Maritime Operations*
- **JP 3-35**, *Deployment and Redeployment Operations*
- **JP 3-57**, *Civil-Military Operations*
- **JP 3-59**, *Meteorological and Oceanographic Operations*
- **JP 3-60**, *Joint Targeting*
- **JP 4-0**, *Joint Logistics*
- **JP 4-01**, *The Defense Transportation System*
- **JP 4-01.6**, *Joint Logistics Over-the-Shore*
- **JP 4-08**, *Logistics in Support of Multinational Operations*

JPs Approved (last 6 months)

- **JP 3-07.3**, *Peace Operations*
- **JP 3-33**, *Joint Task Force Headquarters*
- **JP 3-41**, *Chemical, Biological, Radiological, and Nuclear Consequence Management*
- **JP 4-01.2**, *Sealift Support to Joint Operations*
- **JP 4-01.5**, *Joint Terminal Operations*
- **JP 4-02**, *Health Service Support*