JFQ | Joint Force Quarterly

Issue 73, 2nd Quarter 2014

Evolving Theory for Cyberspace

Educating Future Strategic Leaders

Next Steps in Targeting

Joint Force Quarterly

Founded in 1993 ▪ Vol. 73, 2nd Quarter 2014
http://ndupress.ndu.edu

GEN Martin E. Dempsey, USA, Publisher
MG Gregg F. Martin, USA, President, NDU

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

Executive Editor
Jeffrey D. Smotherman, Ph.D.

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

Internet Publications Editor
Joanna E. Seich

Photography Editor
Martin J. Peters, Jr.

Senior Copy Editor
Calvin B. Kelley

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

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

Cover 2 images (top to bottom): Airman from 336th Fighter Squadron performs Missing Man Pull-up in flyover during internment ceremony of Brigadier General Robinson Risner at Arlington National Cemetery (U.S. Air Force); Marines reload M777 howitzer with 155 mm artillery shell during multiple-rounds fire mission as part of 2-day dual-fire training exercise at Schofield Barracks, Hawaii (U.S. Marine Corps/Matthew Bragg); UH-60M Black Hawk helicopter pilot and commander of C Company "War Lords," 2nd Battalion (Assault), 10th Combat Aviation Brigade, Task Force Knighthawk, prepares cockpit prior to launching on personnel movement mission at Kabul International Airport (U.S. Army/Peter Smedberg).

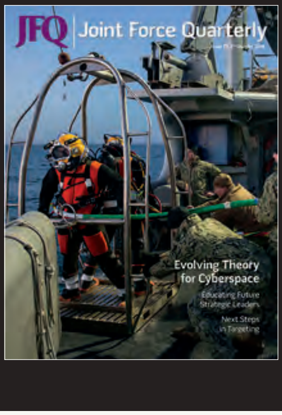
In this Issue

Dialogue

Forum

JPME Today

Commentary


JFQ Joint Force Quarterly
Evolving Theory for Cyberspace
Educating Future Strategic Leaders
Next Steps in Targeting

About the Cover

U.S. Navy divers assigned to Mobile Diving and Salvage Unit 2, Company 2-2, lowered into water January 9, 2014, from Military Sealift Command rescue and salvage ship USNS *Grasp* to search for missing Sailor of MH-53E Sea Dragon helicopter that went down off coast of Virginia (U.S. Navy/Wyatt Huggett).

Features

Recall

Book Reviews

Joint Doctrine

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

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

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

Submissions and Communications
JFQ welcomes submission of scholarly, independent research from members of the Armed Forces, security policymakers and shapers, defense analysts, academic specialists, and civilians from the United States and abroad. Submit articles for consideration by email to JFQ1@ndu.edu, with "Attention A&R Editor" in the subject line. Or write to:

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

Telephone: (202) 685-4220/DSN 325
Email: JFQ1@ndu.edu
JFQ online: www.dtic.mil/doctrine/jfq/jfq.htm

2nd Quarter, April 2014
ISSN 1070-0692

Police barrier at pro–European Union rally in Kiev attended by over 100,000, November 24, 2013 (Flickr/Ivan Bandura)

Letter

To the Editor: I write in response to Derek S. Reveron and James L. Cook's article "From National to Theater: Developing Strategy" that appeared in *Joint Force Quarterly* 70 (3rd Quarter 2013). I agree wholeheartedly with the authors on their position that only "vital" national interests are worth dying for. However, I caution against accepting their idea that national interests that are (merely) "important" are necessarily worth killing for.

To begin, air strikes by manned aircraft carry risks. Reveron and Cook posit the 2011 North Atlantic Treaty Organization air campaign to prevent genocide in Libya as worth killing for, but not worth dying for. But we have to keep in mind that Major Kenneth Harney and Captain Tyler Stark had to eject from their F-15E over Libya on March 21, 2011. If we had not safely extracted them, and, instead, the U.S. public had watched video of their bodies dragged through the streets or hung from a bridge, the Obama administration would have quickly learned whether the American public was ready to see U.S. Servicemembers dying for this cause.

Looking back to March 27, 1999, in Serbia, when Lieutenant Colonel Dale Zelko, flying an F-117A stealth fighter, was shot down by an SA-3 missile, we should recognize that anytime American air crews fly into a combat zone, they risk being unable to fly home from that mission. I suggest manned air strikes should be flown only when U.S. vital national interests are at stake since the crews risk death and cannot kill with absolute impunity.

It might be tempting to argue that unmanned aircraft, cruise missiles, or ballistic missiles do not carry that same risk and might satisfy this new criterion of important interests that are worth killing for but not worth dying for. That would be a grave error for at least two reasons. First, the authors should consider Winston Churchill's statement mentioned in their own article: "The statesman who yields to war fever must realize that once the signal is given, he is no longer the master of policy but the slave of unforeseeable and uncontrollable events." With a near-peer adversary, it would not be surprising if missile strikes triggered counterstrikes against U.S. forces or territory. But even with a lesser foe, asymmetric warfare might be employed to retaliate against America in a way that caused casualties.

Second, if the country we strike has not attacked the United States or an ally—or we do not have a United Nations (UN) Security Council Resolution authorizing the use of force against them—the United States would be committing an illicit act of aggression that would technically constitute initiating an act of war. While UN Ambassador and Pulitzer Prize–winner Samantha Power is an advocate of "R2P" (a responsibility to protect against genocide, war crimes, crimes against humanity, and ethnic cleansing), the third pillar of the R2P global norm unanimously adopted by heads of state and government at the 2005 UN World Summit states, "If a State is manifestly failing to protect its populations, the international community must be prepared to take appropriate collective action, in a timely and decisive manner and in accordance with the UN Charter." In other words, R2P is expected to use the other instruments of national power, rather than military force, except when a UN Security Council Resolution authorizes that use of force.

I believe there is still no better test of whether to employ U.S. military force than the six-point test first articulated by Secretary of Defense Caspar Weinberger in 1984 (and referred to by the authors as the Weinberger Doctrine):

- The United States should not commit forces to combat overseas unless the particular engagement or occasion is deemed vital to our national interest or that of our allies.
- If we decide it is necessary to put combat troops into a given situation, we should do so wholeheartedly, and with the clear intention of winning.
- If we do decide to commit forces to combat overseas, we should have clearly defined political and military objectives.
- The relationship between our objectives and the forces we have committed—their size, composition, and disposition—must be continually reassessed and adjusted if necessary.
- Before we commit combat forces abroad, there must be some reasonable assurance we will have the support of the American people and their elected representatives in Congress.
- The commitment of forces to combat should be a last resort.

In 2003, some advocates of "shock and awe" considered the Weinberger Doctrine outdated by claiming that the United States no longer needed to honor the second point because we could succeed with a smaller force that outmaneuvered the foe. Later, we came to regret not having enough U.S. forces on the ground to provide stability in Iraq immediately after the hot war ended. I recommend the Weinberger Doctrine also be considered for unmanned aircraft or missile strikes when under the control of the U.S. military. We should not be willing to kill for a national interest that we are not ready to risk dying for.

View of Zaatari Camp for Syrian refugees as seen on July 18, 2013, from helicopter carrying Secretary of State John Kerry and Jordanian Foreign Minister Nasser Judeh (State Department)

American security policy experts have recognized that articulating and prioritizing national interests are fundamental to knowing what resources to commit ever since Hans J. Morgenthau's *In Defense of the National Interest: A Critical Examination of American Foreign Policy* was published in 1951. Each administration can have a slightly different take as to which are vital national interests.

So which national interests are worth killing for? In 2000, the Commission on America's National Interests defined *vital national interests* as "conditions that are strictly necessary to safeguard and enhance Americans' survival and well-being in a free and secure nation."[1] Those vital national interests agreed upon by the commission can be summarized as:

- prevent, deter, and reduce the threat of nuclear, biological, and chemical weapons attacks on the United States or its military forces abroad
- ensure U.S. allies' survival and their active cooperation with the United States in shaping an international system in which we can thrive
- prevent the emergence of hostile major powers or failed states on U.S. borders
- ensure the viability and stability of major global systems (trade, financial markets, supplies of energy, and the environment)
- establish productive relations, consistent with American national interests, with nations that could become strategic adversaries.

When national interests at stake are less than these, we should not be willing to have American Servicemembers die or kill for them.

—Commander Thomas J. Reid, USN (Ret.)
Defense contractor in support of Space and Naval Warfare Systems Command

Note

[1] Robert Ellsworth, Andrew Goodpaster, and Rita Hauser, co-chairs, *America's National Interests: A Report from The Commission on America's National Interests* (Washington, DC: The Commission on America's National Interests, July 2000), available at <http://belfercenter.ksg.harvard.edu/files/amernatinter.pdf>. See also Graham Allison, U.S. National Interests, PowerPoint briefing, February 18, 2010, available at <https://dnnpro.outer.jhuapl.edu/media/RethinkingSeminars/021810/Allison_ppt.pdf>.

Ike Skelton, 1931–2013

Champion of Military Education

By Harold R. Winton

Harold R. Winton is Professor of Military History and Theory in the School of Advanced Air and Space Studies.

Education is persistently undervalued in most military institutions. This lack of attention is based on two realities of military life: education engenders the habit of questioning, while sound discipline, particularly in combat, requires unhesitating obedience; furthermore, education requires reflection, but war demands action. Thus, the military Services tend to draw broad lines of demarcation between their thinkers and their fighters.

One man other than the 19th-century soldier Sir William Butler who understood the evils of this tendency was a small-town lawyer from Missouri named Isaac Newton "Ike" Skelton IV. Mr. Skelton entered Congress in 1977 and rose to become Chairman of the House Armed Services Committee (HASC) in 2007. But before he reached this position, Congressman Skelton was a key player in congressional efforts to reduce the dysfunctional inter-Service friction so glaringly displayed during Operation *Desert One*, the abortive 1980 attempt to rescue American hostages in Tehran. This effort culminated in passage of the Goldwater-Nichols Defense Reorganization Act of 1986, which is widely regarded as a landmark of constructive military reform.

But Congressman Skelton sensed that the passage of Goldwater-Nichols was not enough; something else had to be done to assure that America's warriors could *think* strategically in order for its military Services to *act* strategically. That something was to enhance the Services' educational systems. Congressman Skelton enlisted the aid of retired Air Force Colonel Archie Barrett, who graduated from West Point in 1957, earned a Ph.D. from Harvard in 1971, and joined the HASC staff after his retirement. With Barrett's active assistance, Skelton undertook a systematic program to draw attention to the dearth of strategic thinking in America's Armed Forces, lay out the rationale for education as the primary antidote, survey the state of military education, and propose concrete reforms to enhance it.

The first two phases of this endeavor took place over the course of roughly

6 weeks from October to November 1987, during which Skelton delivered five speeches on the House floor that over a quarter-century later are still worth reading. His theme was contained in a series of rhetorical questions in the first speech: "Where are our strategic thinkers of today? Does our military structure no longer nurture such individuals? Is our professional military education system such that it would be impossible for [an Alfred Thayer] Mahan, [George C.] Marshall, or [Maxwell] Taylor to make a contribution? Does our military spend so much time studying weapons systems and tactics that there is no room for strategic thinking?"[1] In subsequent speeches, he raised important questions about existing trends in military education, argued that it was the "weak link" in America's defense armor, contrasted American strategic thinking in World War II with that of the more recent past, and described how the soon-to-be-established HASC Panel on Military Education, which he would chair, would go about its work.

Over the next 14 months, Congressman Skelton's panel conducted 28 hearings in which testimony was received from 48 witnesses, including Admiral Stansfield Turner, the former president of the Naval War College who had fundamentally restructured that college's curriculum in the wake of the Vietnam War; the commandants of all the Services' intermediate and advanced educational institutions; the four Service chiefs; and a wide variety of senior commanders and civilian educators. I was privileged to attend one of those hearings. Congressman Skelton was exceptionally knowledgeable about both the past and the present of military education and was capable of exercising the power of his office with persistence and authority.

Congressman Skelton's panel published its report in April 1989.[2] It found that the existing military education system lacked the rigor and focus required to equip the Services intellectually to provide for the common defense. It called upon the Department of Defense to focus educational institutions on specified learning objectives, enhance the quality of both civilian and military faculty, establish a two-phased system for the education of joint officers, form an Institute for National Strategic Studies at National Defense University, institute a CAPSTONE course for the education of newly selected general officers, and require all intermediate and senior educational institutions to adopt essay-based examinations. These recommendations were unevenly implemented at the time, and some have endured longer than others. But their net effect was positive: Congressman Skelton put the Services on notice that Congress considered military education important, even if they did not.

Congressman Skelton's effectiveness as an educational reformer stemmed in part from his lifelong interest in history, particularly military history. When he was a boy, his father would occasionally allow him to wear the Sailor hat from his service aboard USS *Missouri*. When Ike put it on, "it was as if whispers of warriors floated inside that hat—whispers of important lessons learned through experience in battles past."[3] Congressman Skelton was serious about learning from the past to benefit the present and future, and he always stressed the importance of "lessons learned" through the study of military history. Congressman Skelton strongly valued his lifetime of first-hand military education through parcipitation in staff rides—as both host and guest—to some of the most historic battlefields. In what one might call his valedictory speech, given when he received the 2012 Sylvanus Thayer Award, he approvingly cited President Harry Truman's admonition, "If you want to be a good American, then you must know your history."[4]

As America faces a dangerous and uncertain future, as well as significant fiscal constraints, Congressman Ike Skelton's determined efforts to hold high the light of military education leave a legacy we would do well to emulate. **JFQ**

Notes

[1] Cong. Rec. H26703 (1987) (statement of Rep. Skelton).

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

[3] Ike Skelton, "Whispers of Warriors: The Importance of History to the Military Professional," *Naval War College Review* 53 (Summer 2000), 7.

[4] "Ike Skelton's Acceptance Speech of the 2012 Sylvanus Thayer Award," West Point, NY, October 18, 2012, available at <www.westpointaog.org/page.aspx?pid=5186>.

Chairman talks to Servicemembers at Bagram Airfield about the future of U.S. military operations in Afghanistan and force reductions (U.S. Air Force/Gary J. Rihn)

From the Chairman

Representing Servicemembers who make up today's Joint Force is my greatest honor as Chairman. As the principal military advisor to the President of the United States, Secretary of Defense, and the National Security Council, I work to develop a shared understanding of our capabilities and the Nation's needs in order to provide sound advice and to represent the views of the Joint Chiefs of Staff. To be effective, I must build relationships of trust with those elected to make decisions about the use of military force. But I did not begin to establish relationships with civilian leaders only when I became Chairman.

Long before I came into this position, I believed that the responsibility for managing the relationship between the military and those we serve falls to every one of us who are privileged to wear our nation's uniform. Whether it is a lieutenant interacting with a local mayor on behalf of her Soldiers or my own interaction with national-level civilian leadership, one of our most important responsibilities is to inform decisionmakers about who we are and what we do.

Teamwork in a Complex World

Our nation's security depends on more than just military prowess. Our informational advantages, economic strength, and diplomatic power all play essential roles in keeping America secure. Our nation requires all of these instruments, and we are strongest when they work in concert. But this is not a simple task.

In my nearly 40 years of service, I have witnessed the increasingly precise application of force. In close coordination with other instruments of power, our nation has used the military to shape environments, empower diplomacy, and help achieve national objectives in complex and uncertain situations. As our weapons become ever more precise, it is tempting to choose force as the preferred instrument of power. Precision, however, does not always translate into control over a situation. Carl von Clausewitz reminds us that "war is the province of chance," and because our profession is about the management of violence, it is our responsibility to explain the capabilities—and limitations—of what force alone can achieve.

Gaining a shared understanding of how the instruments of national power must integrate to achieve objectives requires frequent and substantive dialogue. This dialogue must be based on a solid foundation of mutual trust, and that trust is not built overnight. It can be lost in a minute, so it must be constantly reinforced.

The Ultimate Source of Power

Building relationships of trust with our counterparts in government service is essential, but we must also sustain the trust between those of us in uniform and the country we have sworn to defend. All of our power, whether diplomatic, military, or economic, is ultimately derived from the American people.

Our men and women in uniform must always trust that as long as they remain in harm's way, the Nation will ensure they have what they need to complete the mission. In fact, my moral obligation to those serving is to ensure that when we send them to defend the Nation, they will be trained and ready to accomplish the mission. The American people have demonstrated their appreciation for us in very powerful ways. And they trust us as an institution more than any other institution in America. But at the same time, I think there is a deficit of understanding between those of us who serve in uniform and our fellow citizens.

This is not the somewhat overstated concern about losing contact with the American people. The deficit of understanding concerns the very role of the military. The Armed Forces have been on a war footing for more than 12 years, and we have an entire generation of military leaders who have known nothing else. As we return to our garrisons, we must reengage with our fellow citizens. While interest in the military peaks during times of war, building trust and a true understanding of the capabilities and limitations of military power takes time and constant engagement. We must encourage a shared understanding of what our profession means not only during times of war, but also in everyday life and in the everyday business of promoting our national interests. In a world of rapidly evolving threats and challenges, it is important that we strengthen that dialogue with the American people.

Chairman talks with Jim Miklaszewski (chief Pentagon correspondent with NBC News) and other members of media aboard USAF C-40 aircraft en route to Afghanistan (DOD/D. Myles Cullen)

Moving Forward Together

The military theorist Ardant du Picq once stated that four brave men who do not know each other would not dare to attack a lion, but that four less brave men who know each other well would attack resolutely. Today's Joint Force enjoys the best of both worlds. It is comprised of women and men who have repeatedly demonstrated physical and moral courage, and among the Services there is an unparalleled trust and understanding developed over the last 13 years of war. We have realized the vision that General Colin Powell laid out for the Joint Force just over 20 years ago: "We train as a team, fight as a team, and win as a team."

The development of our joint capabilities is a great achievement, but it will not be enough. In an uncertain world, it is vital that we expand the concept of teamwork to include our brothers and sisters in uniform and our civilian counterparts. Understanding among those of us in the military and our fellow servants in the diplomatic corps, our civilian policymakers, and, most importantly, the American people is essential to our ability to effectively provide for the common defense.

And that is why in the time remaining to me, I plan to increase my commitment to have a conversation with our national leaders and the American people about the capabilities of their military, not only in times of war, but also in times of peace. I encourage you to do the same. It falls on each of us to sustain the trust and confidence of those we serve and with whom we serve. JFQ

Martin E. Dempsey
General, U.S. Army
Chairman of the Joint Chiefs of Staff

Combat Logistics Battalion 4 Marines stand by for sun to set before beginning night marksmanship shoot (U.S. Marine Corps/Mark Stroud)

Are We Really Ever Off Duty?

As we in the U.S. military continue to renew our commitment to the Profession of Arms, the title of this article asks a compelling question for everyone who wears the cloth of the Nation. While I believe the question has an easy answer, let us not downplay the significance of asking it at *every* level of professional development. Most serving in the Armed Forces understand the deeper meaning of the question, as well as the commitment to the profession and the American people that goes along with it. Therefore, most military professionals would provide the short answer: "No, we are never really off duty."

Indeed, we are a more effective and a more disciplined force when we live by the high standard of *always on duty* or *never off duty*. You choose and use the term that best resonates with you. I prefer the latter as it conveys a more subtle and steady narrative that is less prone to technical interpretations. To others, the short answer of *no* may not process as quickly. My hope for that particular audience is that by the end of this article, the meaning of the question and resulting answer shall provide a better understanding of why it is individually and organizationally advantageous for us all to live by such a standard of ethical, moral, and professional behavior. Maintaining a "never off duty" posture is not a new idea or the result of a recent study—it has been and should always remain an integral part of our total composition as members of the profession.

A disciplined, dedicated, and structured military career embodies certain individual traits and attributes, such as professional behavior, integrity, respect, and bearing, which collectively provide an internal beacon to guide us. However, living by such a high military standard does not mean that we have to sacrifice every aspect of an otherwise normal life, such as neglecting obligations to family, exercising appropriate periods of rest, and so forth. But it *does* mean that regardless of time or circumstance, we are always fulfilling our obligations as professionals, whether during or after working hours.

To be human is to be imperfect and it is safe to say that none of us has been or will be consistently flawless in meeting a preeminent standard as *never off duty*. We all face temptation and periods in our careers (and personal lives) where we may be drawn to convenience, greediness, even luxury, resulting in shortfalls. It is an *individual* decision to take the right or wrong road. When wrongful temptation overrides Servicemembers' decisions (the wrong road), our integrity should be immediately challenged by our better selves, our teammates, our profession, and even our nation's citizens. Depending on the severity of the decision made, significant setbacks can result for the profession, including degradation in faith and confidence with the public, injury, even loss of life. This is where those who act less than honorably tarnish and scar the reputation of our Profession of Arms. Maintaining a conviction of *never off duty* instills a disciplined standard of living and will help guide decisions that may in fact prevent or avoid a poor plan or a poor choice.

By virtue of qualifying to join the Armed Forces, I strongly consider those achieving the title of *Soldier*, *Marine*, *Sailor*, *Airman*, or *Coastguardsman* to have reached *a high watermark in their lives*, and the profession benefits greatly from the diversity, skills, and determination toward excellence our Servicemembers bring. We *all* want not only to be good in our service but also great in our duty.

The majority in our formations do it right. They challenge themselves to live by the moral and professional standard of *never off duty*, and most believe if this standard is not carried to its fullest, individuals and teams can break down in discipline, morals, and ethics, thereby drawing discredit, failure, or embarrassment to one's unit, Service, country, family, and self. A true serving professional understands the severity of that breakdown and will exhaust every effort to avoid it. Furthermore, I find that Servicemembers who truly understand *never off duty* become exceptional role models and mentors to all others.

At various points along our military career and glide path, maybe even as early as basic training, some key legacy phrases may help as reminders of why one is *never off duty*: "You get paid 24 hours a day," "You can be recalled at any time"—and the one I think resonates best—"Don't think the rules stop or the standards drop at 1700 just because it's the end of the work day; there is no time card to punch." Each phrase conveys that when we volunteer to serve the Nation, it is a 24/7 obligation and our obligations and responsibilities as members of the Profession of Arms never expire.

All five Service branches have unique cultures and identities, and as such, they define, understand, and implement *never off duty* in different ways that ensure members achieve and maintain standards. But regardless of Service branch, duty assignment, geographical location, or individual occupational specialty, there are commonalities and consistencies for maintaining professional behavior, ethics, and proper representation of the Nation. Operating in a mindset of *never off duty* in our everyday lives should prove professionally lucrative. I would even go so far to say that allowing this operating principle into our professional lives will raise our ability to sidestep temptation and wrongful personal actions or choice.

Regardless of one's military status—whether taking annual leave or liberty, attending school, appearing at a social function, serving an internship, moonlighting an after-hours job, shopping for groceries, or conducting combat actions against an enemy force—*never off duty* provides that disciplined methodology to our military lives. It is a behavior rooted in moral soundness, high values, with cause and effect. It maintains a standard and positively impacts professional focus and conduct. It is reachable and sustainable for everyone, every day, every time. We are a much better organization with it than without it. We are *never* off duty. JFQ

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

Secretary Hagel conducts news conference regarding Afghanistan and evolving crisis in Ukraine at NATO defense ministerial meeting (DOD/Glenn Fawcett)

Executive Summary

A seemingly incomprehensible set of events is occurring as I write this column: the People's Republic of China is asserting its desire to extend an air defense zone in the Pacific, the Syrian crisis continues unabated, violence in nations transitioning from one form of government to another is the norm from Iraq to Egypt to Libya, Iran seems to be yielding to international pressure to control its nuclear ambitions, Venezuela seems poised for an economic collapse, bombings and other violence in Pakistan continue, and the Russian Federation has annexed Crimea triggering a possible response from the North Atlantic Treaty Organization (NATO). This particular situation seems to have been taken from a script of an early post–Cold War NATO exercise.

What if anything can we expect a joint force—weary from more than a decade of warfighting in Iraq and Afghanistan—to do? As the costs of the joint force continue to rise, voices from all parts of the political spectrum are asking this very question. Of course, the global security environment is rarely without challenges, but without doubt current situations are hardly going to give us a sense of growing global security. Often those who seek trends in events are looking to see if such a series is expected or is a discontinuity that signals a break with the past.

Against this backdrop, Secretary of Defense Chuck Hagel rolled out the Department of Defense (DOD) budget with significant and ongoing reductions to the department and the Nation's joint force even as the Obama administration works to comply with congressional budgetary limits. Risks will continue to be calculated. Diplomatic efforts will be used in concert with military planning to avert confrontations. As interested parties in the outcome of this environment, we should be asking the right questions about the future of U.S. military strength. One of the more important questions I ask my students at the beginning of the courses I teach is fundamental: What do the American people want their military to do as it meets its constitutional commitments? Implicit in that question lies a more practical one, which the current administration (and every other administration) is working or will work to answer: What will be the shape, size, and capabilities of the U.S. military in coming years as it works to assist in dealing with the world? Hopefully this edition and all future editions of *Joint Force Quarterly* will both give voice to those who have ideas that will be useful and inform the debate as it evolves. The *JFQ* mission continues and we look forward to your contribution to our mutual mission success.

This edition's Forum focuses on a range of ideas related to cyber concepts that continue to be the hottest area among our submissions. Returning to these pages to expand on his widely read article on 10 propositions on cyberspace, Brett Williams presents a compact guide for the joint force commander, as well as anyone who might serve on these joint staffs, on how to deal with cyberspace operations. Addressing one of the more vexing problems in the cyberspace arena, John Shanahan suggests military commanders need to develop consistent standards for dealing with those who damage systems from the inside. A trio of authors from the U.S. Air Force Academy—Ervin Rokke, Thomas Drohan, and Terry Pierce—has developed a new way to take full advantage of combined arms warfare in light of 21st-century cyber developments. Highlighting another growing sector of cyber-related activities of interest to the joint force, Veronica Chinn, Lee Furches, and Barian Woodward look to the private sector to bring about a national answer to security needs in cyberspace.

As promised, this edition has a new section, JPME Today, which is dedicated to highlighting authors and issues that hopefully will engage readers with the Chairman's emphasis on joint education as a key ingredient to the future joint force. As I mentioned in *JFQ* 72, our intent is to place the journal in direct support of authors and ideas from the joint professional military education community as well as voices from outside the classrooms to help the best thinking flow into and out of the minds of our faculties and students. Like our other sections, we hope this encourages voices in support of ongoing efforts and those with ideas to enhance the continuing education efforts both here at the National Defense University (NDU) and across the Services.

In our first article in JPME Today, addressing specific challenges from the Chairman and the future defense environment, NDU President Gregg Martin and Provost John Yaeger discuss how the Chairman's University is undergoing a significant set of changes in joint professional military education delivery to better meet the needs of 21st-century strategic leaders. From one of the top competitors in the Chairman of the Joint Chiefs of Staff Strategic Essay Competition, Strategic Research Paper category, and 2013 Air War College graduate John Gay provides a significant contribution to the debate on whether biofuels could enhance our national energy security. Army War College faculty members William Braun and Charles Allen recommend a serious look at military shaping capabilities to prepare the joint force for any contingency across the spectrum of future conflict. In a team effort from the Joint Forces Staff College, John Bilas, Scott Hoffman, John Kolasheski, Kevin Toner, and Douglas Winton recommend important changes to joint targeting within a campaign to be more inclusive of nonlethal activities and interagency, intergovernmental, and multinational capabilities.

Our Commentary section presents important points of view on three diverse topics. Revisiting one of the most notable if not controversial theorists of the late 20th century, Michael Pietrucha offers a new look at John Warden's "Five Ring" theory in light of changes in airpower and the effects of globalization since Operation *Desert Storm* when the theory was first used in warfighting. Adding an important international voice to the ongoing discussion of developments in the Asia-Pacific region, retired Vice Admiral Fumio Ota, formerly of the Japanese Maritime Self-Defense Force and a graduate of the Industrial College of the Armed Forces, provides rare insights from his personal and frequent contacts with senior Chinese military leaders in recent years. As the U.S. defense budget gets more fiscally constrained, so too will joint force operations. Highlighting the importance of one function that joint operations support, William Fraser, the commander of U.S. Transportation Command, and Marshall Ramsey describe the impact of geography on mobility support for the successful conduct of global logistics.

We next bring you a range of insights from across the joint force in our Features section—on Libya, the U.S. Army's contribution to joint missile defense, better use of civilian capabilities in Africa, improving interagency operations, and the requirement for a junior officer's joint logistics course. Three years after the war in Libya, Todd Phinney assesses the results achieved in Operation *Unified Protector*, the NATO-led portion of that conflict. Michael Tucker and Robert Lyons describe a key element in any joint operation at the high end of the conflict spectrum: the capabilities and value Army air and missile defense units add to the joint force. Suggesting that U.S. Government responses to past disasters indicate a need for nongovernmental responses to humanitarian crises, Charles McDermott outlines methods where civilian capabilities would be a better fit for these contingencies, especially in Africa. Identifying a gap in current joint training, Wilson VornDick describes a well-considered program for filling this requirement for junior logistics officers.

Another international voice brings us a thoughtful World War II article in our Recall section. As some Americans are not familiar with combined and joint operations prior to our entry in the war after Pearl Harbor, Harald Høiback solidly fills in this gap with a revisit to those fearful days for the Allies at Dieppe in 1942. Three outstanding book reviews along with an important joint doctrine essay on cross-domain synergy by William Odom and Christopher Hayes round out the issue.

Let us know what you think about these ideas, and I encourage you to join in the discussion about the world ahead for the joint force. Our mutual success depends on the great thinking and writing of our contributors as you continue to be read and appreciated worldwide by a growing audience of more than 60,000 readers in print and online. Your leadership is depending on you to help them guide the joint force no matter what the environment. JFQ

William T. Eliason
Editor in Chief

Office of Naval Research Project BlueShark creates high-tech, futuristic environment to demonstrate what operational work environments might look like and what emerging innovative technologies might provide in next decade (U.S. Navy/John F. Williams)

The Joint Force Commander's Guide to Cyberspace Operations

By Brett T. Williams

Joint force commanders (JFC) earn the right to command because, regardless of their "native" domain, they are able to direct joint operations in the land, maritime, air, and space domains to achieve campaign objectives. Commanders must develop the same capability to direct operations in the cyber domain since mission success increasingly depends on freedom of maneuver in cyberspace. The preeminent JFC requirement for freedom of maneuver in cyberspace is command and control (C2). It is impossible to fully employ today's joint force without leveraging cyberspace. Other examples include the fact that cyberspace is heavily used to support shaping and influence operations, particularly in the realm of deterrence. The ability to collect, analyze, and use intelligence information depends on cyberspace. Moving data from sensor to shooter and getting access to information all the way to the tactical edge are fundamental requirements for cyberspace. Finally, there are evolving opportunities to project power in and through cyberspace to support attaining campaign objectives. Since cyberspace operations

Major General Brett T. Williams, USAF, is the Director of Operations, J3, for U.S. Cyber Command.

are fundamental to success, commanders cannot continue to run the risk of inappropriately delegating key operational decisions because they and their staffs lack an understanding of the domain. This article argues that despite the technical complexity of cyberspace, the JFC can and should direct cyberspace operations at the operational level of war using current operational doctrine and existing planning and execution processes.

Some people are reluctant to read about cyberspace because they perceive the subject to be "too technical." This piece is intentionally written in the lexicon of joint operations to make it easily understandable, but more importantly to make the point that at the operational level, we must plan and execute cyberspace operations just as we do land, maritime, air, and space operations. What prevents us from taking this approach today is a lack of shared cyberspace knowledge and an agreed upon operational approach that links cyberspace missions and actions and places them in the larger context of joint operations.

The approach outlined here contributes to a shared understanding of cyberspace that is necessary for senior decisionmakers both inside and outside the Department of Defense (DOD). When senior leaders meet to shape national security policy, consider operational plans, or allocate resources, common shared experience means that decisions related to the land, maritime, air, or space domain rarely require accompanying background information regarding the roles and functions of units or weapons systems. The same is not true for cyberspace operations, yet we attempt to structure the meeting in the same way: "Skip the background and get to the decision slide." The risk in this approach is de facto decisionmaking by the people who prepared the brief. There is too much at stake for our senior leaders not to understand cyberspace operations in the same way they understand operations in the other domains. The approach to cyberspace articulated here is useful because it is understandable without a degree in computer science, significant expertise in signals intelligence, or the ability to configure a firewall. At the same time, it is unrealistic to think that we are going to conduct operations in cyberspace without learning some new concepts and associated terminology, at least to the level of this article.

This operational approach will be effective only if we take the time to evolve current conflict theory to account for cyberspace. There is an analogy with airpower here. Airpower did not change the nature of war, but it did change its character. We had to alter our mental framework for conflict to account for the unique capabilities of airpower. In the same way we had to develop airpower theory and make adjustments to broader conflict theory, we need a theory for cyberspace operations that will allow us to understand the implications of employing cyberspace capabilities at the tactical, operational, and strategic levels. The theory must capture the ubiquitous nature of cyberspace and its relevance and interaction with government, commercial, and civilian sectors. Additionally, the theory must cover the complete spectrum from national security policy to detailed technical operations and account for the fact that the domain changes constantly. The process of operational design could be useful in this endeavor.

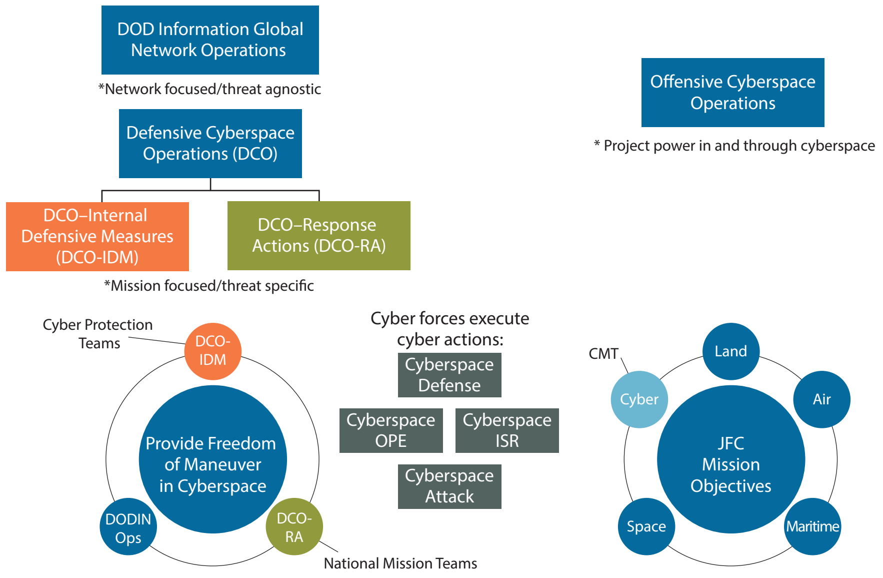
This approach to cyberspace operations reflects the work of the author and his colleagues that began at U.S. Pacific Command and substantially evolved at U.S. Cyber Command (USCYBERCOM). As much as possible, we use the terminology and processes found in the following joint publications (JPs): JP 1, *Doctrine for the Armed Forces of the United States*, JP 3.0, *Joint Operations*, JP 5.0, *Joint Operation Planning*, JP 3.12, *Cyberspace Operations*, and JP 3.60, *Joint Targeting*. The first section presents four axioms developed by the author that underpin the main thesis that we can and should approach cyberspace operations just as we approach operations in the other domains. The next two sections describe an operational approach that allows a JFC to provide friendly freedom of maneuver in cyberspace and to project power in and through cyberspace in support of campaign objectives. The final section describes individual cyberspace actions that create the effects to execute the operational approach. Although this article focuses on DOD operations, the concepts are applicable to any organization that finds itself at risk from malicious cyberspace activity.

Four Axioms

Axiom #1. Use of the term *cyberwar* is not productive. War, conflict, and competition are all characterized by enduring principles that were established long before cyberspace. The creation of cyberspace has simply offered another environment or domain within which to exercise the elements of national power. Focusing inordinately on the unique nature of cyberspace operations at the tactical level tends to draw senior policymakers and their military commanders into a narrowly defined view of conflict and away from a whole-of-government approach to both policy and operations. The result is a tendency to overstate the relevance of cyberspace operations within the context of all other activities that influence the actions of people with opposing goals. Relying on tactical actions from any single domain to be "dominant" is a pitfall that we have mostly learned to avoid, and we should not have to relearn the lesson as we integrate cyberspace operations into joint planning. It is the integration of land, maritime, air, space, and cyberspace *operations* that achieves *campaign* objectives.

Axiom #2. Established joint doctrine accommodates operations in cyberspace quite well, so we do not need to invent anything new. USCYBERCOM staff has found that there are few adjustments required to integrate cyberspace operations into existing planning and execution processes. The joint operation planning process (JOPP) that uses mission analysis to produce a plan or order adapts well to cyberspace operations. In a similar way, the joint targeting cycle, which begins with an endstate and commander's objectives and continues with target development, weaponeering, execution,

Figure 1. Cyberspace Operations


DOD Information Global Network Operations
*Network focused/threat agnostic
Defensive Cyberspace Operations (DCO)
DCO–Internal Defensive Measures (DCO-IDM)
DCO–Response Actions (DCO-RA)
*Mission focused/threat specific
Offensive Cyberspace Operations
* Project power in and through cyberspace
Cyber Protection Teams
DCO-IDM
Provide Freedom of Maneuver in Cyberspace
DODIN Ops
DCO-RA
National Mission Teams
Cyber forces execute cyber actions:
Cyberspace Defense
Cyberspace OPE
Cyberspace ISR
Cyberspace Attack
CMT
Land
Cyber
Air
JFC Mission Objectives
Space
Maritime

Supported by all-source intelligence, information technology, and routine communications activities

and assessment, readily accommodates cyberspace targeting.

Axiom #3. We have a pressing need to develop cyberspace operators who are credible and effective in the J3 (operations) and J5 (strategic plans and policy) within both the Joint Staff and combatant commands. For emphasis, that is the J3 and J5, not just the J2 (intelligence) and J6 (command, control, communications, and computers systems), and at all of the combatant commands, not only USCYBERCOM. Despite the technically complex nature of cyberspace and the potential for increasing levels of machine-to-machine interaction, success will always rely on the leadership and technical skills of Soldiers, Marines, Sailors, and Airmen. Joint staffs consist of what we typically think of as operators, members of the combat arms who are educated, trained, and experienced in operations. Cyberspace expertise usually comes from people with intelligence, communications, or cryptology backgrounds—career fields typically categorized as support forces. If we are going to treat operations in cyberspace like operations in the other domains, the Services must commit to unique career fields for cyberspace. There has been a focus on providing highly trained, technically skilled personnel who come mostly from the enlisted or warrant officer ranks. DOD must rapidly bring the same emphasis to cyberspace officer career development. Cyberspace, like the other domains, requires officers who are developed across their careers in a way that positions them to lead at senior levels in both command and staff. Cyberspace officers should spend their first 10 years becoming tactically proficient in all aspects of cyberspace operations, complete Service and joint military education, serve on joint staffs, command in their areas of operational specialties, and do all the other things necessary to produce general and flag officers whose native domain is cyberspace.

Axiom #4. Words matter. Routine misuse of the word *cyber* is one reason we do not have a common framework for discussing cyberspace operations. *Cyber* is neither a verb nor a noun that can stand on its own. Saying "cyber" should not automatically connote offensive operations. Additionally, questions such as "Is cyber intel?" or "Is cyber comm?" are counterproductive as they encourage legacy stovepiped views of cyberspace operations. *Cyber* is most useful as part of the compound word *cyberspace*, and cyberspace is simply the manmade domain and information environment we create when we connect together all computers, wires, switches, routers, wireless devices, satellites, and other components that allow us to move large amounts of data at very fast speeds. It follows that cyberspace operations are those conducted in cyberspace with the objective of providing friendly freedom of maneuver in cyberspace and projecting power in and through the domain in support of JFC campaign objectives. Intelligence and communications are support functions to cyberspace operations just like intelligence and communications support operations in all the other domains. Both intelligence and communications functions must be more closely integrated with cyberspace operations than operations in the physical domains; however, it is important to maintain the distinction between supporting activities and the operations themselves.

Missions and Objectives

Building on these four axioms, we can now describe cyberspace operations in terms of intent, mission categories, and actions. In anticipation of at least a few fighter pilots and infantry officers reading this, it has been necessary to include a picture that will serve as a reference for the discussion. The test at the end is being able to define the terms and articulate the interrelationships depicted in figure 1 to indicate the minimal level of understanding necessary for commanders and their staffs to plan and execute cyberspace operations.

The two cyberspace objectives relevant to the JFC are providing freedom of maneuver in cyberspace and projecting power in and through cyberspace to achieve campaign objectives. There are three categories of cyberspace missions for attaining these two objectives:

- DOD information network operations (DODIN Ops)
- defensive cyberspace operations (DCO)
- offensive cyberspace operations (OCO).

Cyberspace forces execute four actions to create the necessary effects in the domain:

- cyberspace defense

- cyberspace operational preparation of the environment (OPE)
- cyberspace intelligence, surveillance, and reconnaissance (ISR)
- cyberspace attack.

DODIN Ops Mission

Providing freedom of maneuver in cyberspace must be the JFC's top cyberspace priority because of the reliance on cyberspace for command and control across the joint force. Effective C2 allows the commander to get information, move information, and use information to make better decisions faster than the enemy, which is an advantage we cannot give up and cannot achieve without assured access to cyberspace. It must be acknowledged that cyberspace will always be a contested domain, and it is unlikely we will ever have continuous or uncontested cyberspace superiority; however, in the same way we approach operations in the other domains, we must have sufficient control of cyberspace at the time and place we need it. We provide the requisite level of freedom of maneuver in cyberspace through the mission categories of DODIN Ops and DCO.

DODIN Ops include designing, building, configuring, securing, operating, maintaining, and sustaining the information environment that we rely on for operations. DODIN Ops should be done in a proactive manner and include actions focused on information technology (IT) consisting of hardware and software, data, individual users, and system administrators. Examples include correcting known IT vulnerabilities, encrypting data, and ensuring user and administrator training and compliance. It is useful to think of DODIN Ops as being "network" focused and threat agnostic. They are *network focused* in that they approach security from the perspective of IT in the operational configuration. Traditionally, DODIN Ops have not emphasized the security of data at rest or in motion within or across the information environment, even though it is the integrity and security of the data that matter most to the commander. They are *threat agnostic* in that their security measures are not focused on a specific threat. Instead, our security baseline seeks to mitigate known vulnerabilities from a broad range of threats. For the same reason people lock their car doors regardless of where they park or the fact that we check identification at the gate, it is prudent to establish a level of security to defend our information environment against a general category of malicious cyberspace activity to include insider threats. A useful byproduct of establishing strong baseline security is that it makes the cyberspace terrain a hard target and encourages adversaries to go after softer ones.

A key tenet of DODIN Ops is to provide a consistent level of security across all components of the DODIN. This is important for three reasons. First, the nature of cyberspace, as currently architected, means that a risk shared by one is a risk shared by all. Just as a single negligent sentry puts an entire base at risk, a single careless user or system administrator introduces risk to an otherwise secure network. Second, the majority of malicious activity in the DODIN can be mitigated with currently available techniques since the vast majority of adversary exploitation utilizes known vulnerabilities. The vulnerabilities are not corrected for a variety of reasons to include lack of resources (time, people, money), inadequate leadership emphasis, hubris ("We are really good, no one can get into our network"), or simple ignorance of the security requirements. Third, strong security compliance allows us to focus our efforts on the most sophisticated threats. All too often our most capable people spend the majority of their time dealing with serious compromises that could have been prevented with basic security compliance.

Even perfectly executed, the security provided through DODIN Ops is not sufficient alone to defend our information environment. Until we substantially evolve the architecture, a variety of technical and policy challenges will continue to inhibit our ability to evaluate, report, and correct compliance deficiencies. Efforts are under way to address these technical challenges specifically with DOD's Joint Information Environment (JIE). Making JIE a reality soon is critical to providing defensible cyberspace, but no matter how much we improve technically, leadership awareness and command accountability will remain essential to cyberspace security. Commanders need to treat the DODIN like the weapon system it is and hold both users and network operations personnel accountable for their actions. The constantly changing nature of the domain, the low price of entry for malicious actors, and the large potential payoff for cybercriminals, hacktivists, or nation-states means that we must do more than make passwords 15 characters long. Commanders must prioritize resources to achieve the highest possible compliance with IT security directives. Doing so sets the first line of defense in a layered cyberspace defense strategy. Unfortunately, even perfect DODIN Ops execution is not sufficient to provide freedom of maneuver in cyberspace. Defensive cyberspace operations are required to engage and defeat the full range of cyberspace threats.

DCO Mission

Defensive cyberspace operations are passive and active cyberspace defense activities that allow us to outmaneuver an adversary. The ultimate goal of DCO is to change the current paradigm where the attacker enjoys significant advantage. DCO provide the ability to discover, detect, analyze, and mitigate threats, to include insider threats. As opposed to DODIN Ops, we should think of DCO as mission focused and threat specific. They are *mission focused* because they are prioritized against key cyber terrain to ensure data move securely across the information environment. They are *threat specific* because they are executed against specific threats with malicious capability and intent to affect our key cyber terrain. The first step in directing the DCO mission is having the commander identify the key cyber terrain. For example, if missile defense is a priority then perhaps the Ballistic Missile Defense System (BMDS) is key cyber terrain. Step two in this example is technically enumerating the key cyber terrain from sensor to shooter. Essential elements of the key cyber terrain for BMDS include the various sensors that collect launch data and the networks and systems that move that data to a variety of command centers for attack assessment. From there, the data must move quickly and securely to direct an appropriate response. One rapidly determines there are many systems involved, all with their own vulnerabilities along with additional vulnerabilities at the points where one system connects to another. There are more vulnerabilities than we can address, and therefore we must prioritize our efforts against adversaries with specific capability and intent to interfere with our key cyber terrain.

By linking vulnerabilities with adversary capability and intent, we have identified the primary risk areas on which to focus our defensive efforts. Defending BMDS or any other key cyber terrain involves both subcategories of DCO: internal defensive measures (IDM) and response action (RA). IDM are those actions we take internally to friendly cyberspace, and RA is taken outside our information environment to stop or block the attack.

The essential tasks for DCO-IDM are hunting on friendly cyber terrain for threats that evade our security and directing appropriate internal responses. There are several key requirements for effective DCO-IDM. First, there must be sufficient personnel specifically trained to operate on the individual systems and components that make up the key cyber terrain. Second, we must have timely intelligence and information-sharing as well as shared situational awareness to direct the actions of the hunt mission; simply wandering the network looking for things that do not "look right" is not going to work. Third, we have to evolve how we think about authorities to operate on friendly cyberspace. In any example of key cyber terrain, there will be multiple network authorities and program managers. Ultimately, the appropriate commander must have the authority to direct DCO forces to operate across the entirety of the key cyber terrain. Finally, we must create capacity and diversity in DCO-IDM forces. Most of the current capability exists at the global level, and there are a variety of technical and policy limitations that degrade effectiveness. Effective DCO-IDM requires forces that can operate at all levels in the DODIN in a coordinated fashion. USCYBERCOM has defined the need for Cyber Protection Teams (CPT) to conduct the DCO-IDM mission. CPTs are training to a high technical standard, and their capabilities include analyzing key cyber terrain, hunting on friendly cyber terrain, and emulating threats to test defenses.

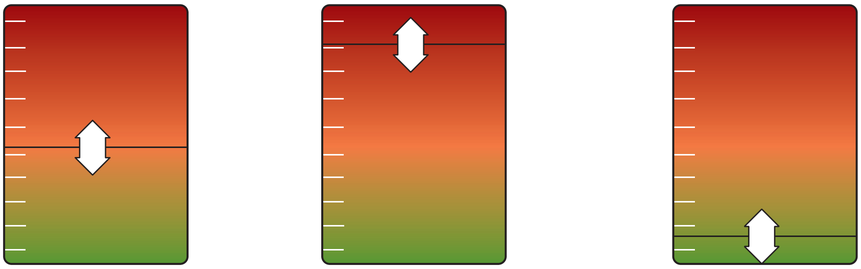
The essential task for DCO-RA is to "kill the archer." We catch arrows with DODIN Ops and DCO-IDM. DCO-RA, however, is about going after the shooter. We do not defend an airfield solely with hardened shelters, surface-to-air missiles, and fighters overhead. By analogy, we should not expect to defend our information environment with DODIN Ops and DCO-IDM alone. In the same way we go into enemy airspace to shoot down airplanes, crater a runway, or destroy a C2 facility, the commander needs options to conduct DCO-RA outside friendly network space to stop the attack before it reaches our key cyber terrain. The forces tasked with the DCO-RA mission under the USCYBERCOM model are the National Mission Teams (NMTs), which are trained to the highest technical standards. They operate in accordance with all the legal and policy guidance impacting operations outside friendly cyberspace. NMT success relies on timely intelligence, information-sharing, shared situational awareness, and close synchronization with the CPTs executing the DCO-IDM mission.

The JFC Integrated Approach

As with any military operation, actions along a single line of effort rarely accomplish the commander's scheme of maneuver, and the same holds true in cyberspace. To provide freedom of maneuver in cyberspace, we must optimize the employment of forces across DODIN Ops, DCO-IDM, and DCO-RA. One way to think about this employment construct is to envision a lever that controls each of the three mission areas. There are constraints, restraints, costs, benefits, and risks associated with moving the levers up or down, and there are impacts across all three mission areas when any single lever is moved. Commanders must achieve a balance that satisfies their mission objectives at an acceptable level of risk. Figure 2 is a visual depiction of this concept.

The lever on the left represents DODIN Ops and is set at the baseline

Figure 2. Providing Freedom of Maneuver in Cyberspace



DOD Information Global Networks Operations

Limits
- Command and control agility
- Operational flexibility

Defensive Cyberspace Operations–Internal Defensive Measures

Limits
- Identify key cyber terrain
- Link vulnerabilities to threat
- Capability and capacity
- Authorities

Defensive Cyberspace Operations–Response Actions

Limits
- Policy
- Rules of engagement
- Authority

- Intelligence
- Access
- Capability

security level. Moving the lever up "hardens" the environment through actions such as restricting access to and from the DODIN, isolating high-risk applications or services, and rerouting traffic to enable more effective sensor coverage. We should carefully consider moving this lever up since network hardening tends to reduce C2 agility and operational flexibility.

The center lever represents DCO-IDM and is the linchpin to providing freedom of maneuver in cyberspace. Hunt operations and key cyber terrain analysis enable both the DODIN Ops and DCO-RA missions as long as there is effective information-sharing and maneuver synchronization. We would like to push the DCO-IDM lever all the way up, but there are significant limits. For instance, it could be challenging just to get the commander's staff to identify key C2 requirements by operational phase. As described above, the process of technically enumerating the key cyber terrain and its associated vulnerabilities is a large technical challenge. Correlating enemy capability and intent with known vulnerabilities is another level of complexity. Manning, training, and equipping sufficient teams is a major hurdle. Finally, there are myriad authorities' issues involved when working across multiple networks, systems, applications, and services.

The third lever is DCO-RA, which we would also like to push all the way to the top, but we have to account for two categories of limitations that are exactly analogous to operating in the physical domains outside of friendly space. The first limits are the constraints of policy, rules of engagement (ROEs), and authority for execution. We are challenged by the fact that these constraints are constantly evolving as both the domain and our understanding of the domain change. Adding to this challenge, many of our senior leaders have a limited understanding of cyberspace operations, and that lack of understanding can lead to risk aversion or unhelpful focus on tactical issues. The second set of limits describes the same restraints associated with any target. The planner has to have the intelligence support to understand how the target system operates, access to the target, and the capability to impact the target to generate the desired effect. Cyberspace targeting is complicated by the rapidly changing nature of the target systems, the extensive target development required to achieve a weaponized solution, and our nascent ability to describe both desirable and undesirable effects for cyberspace operations. Integrating cyberspace targeting within the existing construct of joint targeting and the creation of a Joint Munitions Effectiveness Manual for cyberspace capabilities are major steps in the right direction.

Here is a simple example of how this operational approach provides a response to a malicious cyber event. Assume we have intelligence indicators that an adversary is going to launch a cyber attack against a key C2 system, and we have identified 100 compromised servers around the world that will host malware for the attack. Working from left to right across our levers, we would determine if moving the DODIN Ops lever would allow hardening actions that would reduce our attack surface with acceptable operational impact. We would then task our DCO-IDM forces to focus on the highest risks on the key cyber terrain. It is unlikely that we would have sufficient forces to cover all the key cyber terrain, so we would request additional support through the normal Request for Forces process. Next we would examine DCO-RA options to determine if there are any preauthorized, preplanned actions that could be taken to block the attack. We would have to first verify that planned actions had not been rendered ineffective due to changes in the targeted networks. Then we would need to confirm that existing ROEs and authorities were sufficient for the commander to order execution. If not, the commander could request the necessary additional authority to engage the enemy. If the ROEs were not expanded, we would potentially have to harden the network and/or redirect DCO-IDM capability and accept risk in other portions of the key cyber terrain. It is important to note that even without authorization to stop or block the attack, the DCO-RA mission is critical for intelligence purposes. The DCO-RA forces operating in adversary space provide critical information regarding attribution; adversary tactics, techniques, and procedures; and exposing capabilities not yet deployed. Such intelligence information is critical for executing DODIN Ops and DCO-IDM. Our BMDS defense example shows that providing freedom of maneuver in cyberspace requires a coordinated, synchronized, integrated planning and execution process across all three missions. Key to success is that all forces are trained to the same high standard and that they have access to the same intelligence. We cannot treat DODIN Ops and DCO-IDM as maintenance activities with no need for highly skilled personnel or sensitive intelligence information.

Cyberspace Integration

Turning now to the right side of figure 1, we can discuss integration of cyberspace operations with operations in the physical domains to achieve JFC campaign objectives. The best way to integrate cyberspace operations is to use the commander's existing JOPP. Experience at USCYBERCOM suggests that standard doctrinal planning and execution processes work for cyberspace operations. Existing boards, bureaus, cells, and working groups that do mission analysis, course of action development, center of gravity determination, collection management, targeting (both deliberate and dynamic), and assessment all require little if any adaptation to account for cyberspace operations. Of course, personnel with appropriate cyberspace operations experience must be integrated into the commander's joint staff in the same way the staff has the requisite mix of officers with land, maritime, air, and space experience. Additionally, trained and ready cyberspace forces must be made available, and there must be an effective C2 structure with associated processes supported by the right information environment and effective knowledge management tools.

A complete C2 discussion is beyond the scope of this article, but a key element

Sailors conduct duties at U.S. Fleet Cyber Command Maritime Operations Center, Fort Meade, Maryland (DOD)

for success is the designation of a joint force cyberspace component commander (JFCCC) who operates at the same operational planning and execution level as the functional component commanders for the land, maritime, and air domains. The JFCCC will direct DODIN Ops and DCO to provide freedom of maneuver in cyberspace and will direct offensive cyberspace operations (OCO) to project power in and through cyberspace. The JFCCC will work with the other component commanders to establish supported and supporting roles throughout all phases of the operation. Those familiar with OCO in the context of recent conflicts may infer that the greatest utility lies in Phase 0 and I to support shaping operations, information operations, military deception, and preparation of the environment. OCO will continue to play a key role in these early phases; however, in future engagements these operations will increasingly provide opportunity for significant impact throughout the campaign. Worth noting is that the JFCCC and associated cyberspace forces operate during both steady state and crisis similar to a theater special operations command and that the USCYBERCOM commander has combatant command responsibility for those forces (similar to U.S. Special Operations Command) in order to globally synchronize and integrate activities in cyberspace.

This description is not meant to oversimplify the process of integrating cyberspace operations into JFC planning and execution, and admittedly there are three major challenges that make this difficult. First and foremost, the JFC does not have access to cyberspace operators—officers who are trained from commissioning at the tactical level in all three mission areas—DODIN Ops, DCO, and OCO—and then professionally developed as joint warfighters. Until we develop such officers, we will continue to rely on members of the traditional combat arms to learn enough about cyberspace to integrate cyberspace operations into the planning and execution process they already understand. The second challenge is the level of security we have attached to many cyberspace operations. High levels of security compartmentalization can inhibit integrated planning and execution, and this dynamic is not unique to cyberspace. The third challenge is authorities. One could argue that it is more likely to receive an execute order authorizing kinetic action that could result in death and destruction than it is to expect a JFC to be delegated authority to conduct DCO-RA or OCO. Hesitancy to delegate authority for cyberspace operations is a reflection of our limited shared understanding of cyberspace and in some cases erroneous preconceived notions about the domain. For actions in the physical domains, we are comfortable with issues of sovereignty, probability of kill, anticipated collateral damage, and fratricide. Because we cannot articulate these same considerations for cyberspace in nontechnical, easily understood terms, the authority for execution is typically held at a level above the JFC. One way to address this challenge is to use the standard target validation and vetting process for cyberspace targets. This would force us to address all of the normal targeting issues to include intelligence gain/loss, operations gain/loss, and, unique to cyberspace operations, technical gain/loss where we have to evaluate the risk of exposing a particular capability because that exposure may put an unrelated operation in jeopardy. Once we develop the same disciplined planning approach and precision attack capabilities for conducting DCO-RA and OCO that we have developed for prosecuting targets in the physical domains, the JFC will get execution authority.

To sum up the bottom right side of figure 1, cyberspace operations at the operational level of war can and should be treated like operations in the other domains. We do not need to invent new planning and execution processes; we just need to conduct cyberspace operations with the same disciplined approach as all other joint operations and provide commanders with the relevant considerations in familiar, understandable terms.

Cyberspace Actions

To frame the employment of forces in the cyber domain, we finish with a description of the four actions listed in the center of figure 1: cyberspace defense, cyberspace ISR, cyberspace OPE, and cyberspace attack. These actions are conducted by the JFC to execute DODIN Ops, DCO, and OCO missions. It is important not to conflate the missions with the actions. In other words, the action of cyberspace defense is not associated only with providing freedom of maneuver in cyberspace, and cyberspace attack is not conducted only for offensive purposes.

Cyberspace defense actions are conducted by the commander with authority over the information environment to protect, detect, characterize, counter, and mitigate threats and vulnerabilities. Cyberspace ISR is normally authorized under military authorities and conducted to provide critical operational information to support follow-on actions. Cyberspace OPE consists of nonintelligence actions that set the stage for follow-on operations. Finally, cyberspace attack counters the adversary's ability to achieve objectives through degradation, disruption, or destruction of infrastructure and/or capabilities. Cyberspace attack can also manipulate data in a way that impacts the adversary's information systems. It is important to recognize that cyberspace attack, like all forms of attack, is designed to generate effects in the physical domains. The desired effect may be as simple as creating uncertainty in the opponent's decision calculus, or we may seek a destructive effect that in the past could only have been possible with kinetic action. Understanding these actions and their relationships to the missions of DODIN Ops, DCO, and OCO is foundational to understanding cyberspace operations. In the same way that JFCs understands how offensive counterair contributes to air superiority and antisubmarine warfare contributes to maritime superiority, they must understand how cyberspace defense, ISR, OPE, and attack contribute to providing friendly freedom of maneuver in cyberspace.

Final Thoughts

The intent of this article is not to oversimplify or dismiss the complexity of operating in cyberspace. Instead it is to advocate for making cyberspace operations part of the powerful synergy we currently create with joint force operations. Cyberspace is difficult to visualize. We cannot create a two-dimensional Big Ass Map that we can all sit around to discuss operations. At the same time, there is a huge, largely unacknowledged benefit in that we can use existing concepts and language as a starting point to explain and teach cyberspace operations. This article is focused on cyberspace operations in support of the commander, but there is a broader implication as well. We have a requirement to determine how cyberspace impacts national security policy, grand strategy, and conflict theory; force development including personnel recruiting, development, and retention; all aspects of resourcing from joint capabilities development to programming, budgeting, execution, and defense acquisition; military support to entities outside of DOD; and force structure across the Active and Reserve components. In these and other endeavors, we should fight the temptation to invent new and unique ways of doing business. Instead we should start with the existing processes and make appropriate adjustments to account for the unique nature of cyberspace. Rarely should cyberspace operations require senior leaders to adopt a completely new frame of reference regardless of the decision at hand.

The military departments play a key role in defending our national security interests, and when the military is called into action, we rely on commanders to lead our forces. Today's commanders must be prepared to defend the Nation in all domains including cyberspace. They cannot do so without trained and ready forces, situational awareness of cyberspace, effective command and control, defensible architecture, appropriate delegation of authority for execution, and an operational approach to tie it all together. The operational approach described here provides a starting point for commanders to integrate cyberspace operations within the joint doctrinal framework employed every day to accomplish their assigned missions. **JFQ**

Airmen conduct cyber operations at Joint Base San Antonio–Lackland in support of command and control and network operations (U.S. Air Force/William Belcher)

Achieving Accountability in Cyberspace
Revolution or Evolution?

By John N.T. Shanahan

Consider three scenarios, all based on actual incidents, and consider how violations in cyberspace have effects far beyond the actual incidents.

Cross-domain Violation. During a crisis in the Arabian Gulf, a young Sailor working in an operations-intelligence cell on an aircraft carrier that is part of a U.S. Central Command (USCENTCOM) carrier strike group (CSG) is tasked to provide satellite imagery of a new base of operations used by the Iranian navy. The best imagery available is on an unclassified Web site. Due to the urgency of the situation, the Sailor disregards standard operating procedures for transferring data between networks and downloads the image to an unclassified thumb drive and inserts the thumb drive into a Secret Internet Protocol Router Network (SIPRNet) USB port to transfer the imagery in preparation for a briefing to the commander. Unfortunately, the thumb

Major General John N.T. Shanahan, USAF, is Commander of the Air Force Intelligence, Surveillance, and Reconnaissance Agency at Joint Base San Antonio–Lackland, Texas. His previous assignment was to the Pentagon as the J39 Deputy Director for Global Operations, Operations Directorate, Joint Staff.

drive is infected with treacherous malware, which is subsequently transferred to the ship's classified and unclassified networks through this cross-domain violation. Within hours, the malware propagates throughout both networks and begins to beacon to a site known for its state-sponsored cyberspace espionage activities. There is no choice but to shut down both the unclassified and the secret networks on the carrier, isolating it from the rest of the CSG and from higher headquarters ashore and leading to disastrous consequences for ongoing operations.

Network Protection Shortfalls. At a major Air Force installation in the United States, communications personnel in a tenant unit, whose primary unclassified operating network is neither owned nor operated by the installation host commander, fail to load a patch directed in a tasking order that is designed to close a significant vulnerability in the unit's network. A rogue cyberspace actor discovers and takes advantage of the well-known vulnerability using a socially engineered spear phishing email to inject malware throughout the network. Consequently, the entire network must be shut down for 2 weeks to clean up the infection, with major consequences for deployed personnel who rely extensively on the combat weather data provided by the tenant organization.

Cleared Defense Contractor (CDC) Shortcomings. A small CDC in San Diego that designs and builds critical components of a major weapons system fails to adequately protect its unclassified proprietary network. A known nation-state actor gains access to the company's network and begins to exfiltrate megabytes of data. The National Security Agency (NSA) teams up with the Federal Bureau of Investigation (FBI) and Department of Homeland Security (DHS) to detect and identify the perpetrators, but the company does not take the necessary steps to clean and safeguard its network even after notifying the CDC of the ongoing attack. Within a month the company loses almost all the information on its network relating to the sensitive weapons system components, not only providing the nation-state a major economic advantage in future business negotiations, but also giving the offending state a decade's head start in designing an indigenous system and allowing it to build countermeasures against the U.S. system.

Cascading Effects

In all three vignettes, actions in cyberspace led to cascading effects and debilitating consequences in multiple domains beyond cyberspace and affected operational readiness. A root cause analysis aimed at identifying the origin of the consequences quickly leads to hard questions about the fundamental issue of accountability. In the first case, should the CSG commander be held responsible? What about the Sailor's supervisors at every layer throughout his chain of command? And what happens to the individual who brought an unclassified thumb drive into secure spaces on the ship? In the second case, what should happen to the tenant unit commander? Should the host installation commander be held accountable for the tenant unit's mistake? What about the host installation's communications squadron commander? In the third scenario, should the CDC be barred from future business with the Department of Defense (DOD) or the U.S. Government? Should it be forced to clean and protect its network before it is allowed to continue operations?

These represent only a sample of the questions that must be answered to establish responsibility and mete out punishment. To help provide the framework required to identify the right questions and responses, it is useful to examine three disciplines that are already associated with longstanding robust cultures of accountability: nuclear operations, aviation mishap investigations, and, as simple as it may sound, driving a car.

Our adversaries and potential adversaries—nation-states, nonstate actors, criminals, hacktivists, and insider threats—are moving ever faster along the cyberspace continuum from exploitation to disruption to destruction. To counter the dangers we face in cyberspace today requires a more comprehensive approach than simply enhancing information assurance, improving automated defense tools, and creating more policies and procedures to deter substandard practices. There is a compelling need to establish meaningful accountability for actions or inaction affecting cyberspace operations. Establishing accountability for activities in and through cyberspace is now at least as important as attribution when striving to prevent or punish bad behavior whether that behavior is a result of friendly or adversary actions.

When dealing with our own personnel and organizations, providing explicit accountability guidelines is necessary to assure the confidentiality, integrity, and availability of "blue" cyberspace. We have not fully developed or implemented key tenets of cyberspace accountability throughout U.S. military operations even though we are beginning to grasp the magnitude of what happens when we ignore it or treat it lightly. If we accept the proposition that our military's approach to cyberspace accountability is inadequate, yet reject the canard that achieving accountability in cyberspace is a fool's errand, the next logical question is what it will take to fix the problem.

Because of the ubiquity of cyberspace, exceptionally low barriers to entry, ease of use, dizzying rate of change, and inherent complexity in both the interconnection of multiple systems and the internal functioning of individual systems, no single revolutionary action, policy, procedure, or pronouncement will fix our problem of accountability in cyberspace. However, we know from our experiences in other disciplines that certain fundamental conditions are necessary to enable a true and enduring *culture of accountability.* We do not need to create these elements from scratch in cyberspace. Instead we need a rapid, evolutionary transformation of current activities that focuses on fostering and maturing the culture of accountability that is based on education and training (and begins the moment one enters the military); establishment of clear chains of custody for all networks and systems; establishment of defined processes and procedures, as well as explicit guidance on acceptable behavior;

advanced methods for controlling access; and a standardized joint process for "cyberspace mishap investigations" that parallels the process used so successfully in military aviation safety over the past 30 years. The final and in many ways most important ingredient in the accountability soup is enforcement as a commander's program, as there is a direct and crucial link between accountability in cyberspace and operational readiness.

There are useful analogies between military nuclear weapons operations and cyberspace operations, and safety, more than any other attribute, exemplifies the concept of accountability in nuclear operations. The remarkable safety record accumulated over the past 60 years in Navy and Air Force nuclear activities has been directly attributable to an uncompromising approach to safety as well as unflinching scrutiny of mistakes, adoption of lessons learned, and enforcement actions. Honest mistakes are evaluated and corrected, and recommendations for improvement are applied quickly and consistently throughout the Services to prevent similar future mishaps. Intentional negligence or inattention to detail, on the other hand, is punished swiftly and unmercifully. To paraphrase one old-school Air Force general, when it came to punishing mistakes in nuclear operations, firing the responsible commander would be accompanied by the admonition, "I don't know if you are just unlucky or a bad leader, but I can't afford to waste any more time finding out."

Yet the differences between nuclear and cyberspace operations are stark enough to suggest that the solution to cyberspace accountability lies in a hybrid approach that not only includes some aspects of the nuclear enterprise but also recognizes that the unique nature of the environment demands other less narrow solutions. Nuclear operations are *special*, with access restrictions throughout every aspect of operations. We would not want it any other way and we cannot afford to have it any other way. In this country, every decision involving employment of a nuclear weapon emanates from one person: the President. In relative terms, only a very small percentage of U.S. military personnel are allowed access to nuclear command and control or to the weapons themselves. To receive such access requires undergoing a psychological and medical vetting process known as the Personnel Reliability Program (PRP), which remains in place as long as an individual maintains access to the nuclear enterprise. PRP involves multiple levels and layers of compartmentalization to ensure that only a tiny number of people are granted access to the entire nuclear decisionmaking ecosystem. There are many technical safeguards throughout the nuclear command and control communications process and with the nuclear weapons themselves to prevent accidental or unauthorized actions. The strategic consequences of one mistake can be enormous, so accountability must always remain at the heart of all nuclear operations. Accountability is the sine qua non of nuclear operations.

On the other hand, cyberspace is ubiquitous. It was designed that way from its inception, and it is exceedingly unlikely that we will ever turn back the clock with respect to access. In fact, the opposite is far more likely: as cyberspace is integrated more and more into everything we do, it is entirely possible that we will even stop thinking of it as a unique "thing." Our dependence on cyberspace is increasing exponentially every year. It is now an unassailable proposition that it will always be available, be as secure as the situation demands, allow nearly instantaneous communication, and be crucial to carrying out the quotidian functions of every household, business, academic institution, military organization, and so much more (though the military must continue to train and exercise to the worst-case scenario—a "day/week/month without cyberspace").

While the specific physical, administrative, and technical controls used in nuclear operations may not be directly transferrable to operations that depend on maximizing access to cyberspace, the combined application of all three types of controls and the rigid enforcement of compliance with those controls offer insights into the critical elements of a cyberspace accountability culture.

The Social Compact of Trust

In addition to activities undertaken to ensure safety in nuclear operations, an approach similar to that used in military aviation safety over the past 50 years, especially since the early 1980s when Class A incident rates began to decrease dramatically after an alarming spike in the 1960s and 1970s, can be particularly useful for cyberspace operations. Serious aircraft mishaps are normally followed by two related but distinct safety investigations, each only 30 days long. The first is a safety investigation board (SIB). It focuses on identifying and correcting the root causes of a mishap and relies on a candid exchange of information. This offers the equivalent of immunity from punishment for admitting to failing to follow procedures or breaking rules in return for providing privileged information (which is never released to the public) deemed crucial to avoiding future similar mishaps. The second, an accident investigation board (AIB), is used inter alia to determine culpability and accountability *throughout every level of the chain of command*, potentially leading up to loss of aviation rating and even nonjudicial punishment. Applying the same level of formality and discipline inherent in aviation safety investigations to serious cyberspace mishaps will be instrumental in enhancing cyberspace accountability.

Likewise, trust and confidence are important to cyberspace accountability. Driving 50 mph down Arlington Boulevard, one can be less than 2 feet away from traffic approaching in the opposite lane at 50 mph. One small mistake would result in a 100 mph collision. Why is it we do not drive in perpetual fear of collision with our hands clutching the wheel in a death grip and our eyes locked firmly on the road? We *trust* that the driver in the other vehicle will not veer into us. We *trust* that his lifelong combination of training and experience has rendered him as interested in and capable of avoiding us as we are of avoiding him. The probability that he will veer into us is never zero, but it is so low that we essentially disregard this danger when we drive.

Students answer questions during Joint Cyber Analysis Course at Center for Information Dominance (U.S. Navy/Jessica Gaukel)

This mutual trust on the road rests on two pillars. The first revolves around minimum standards and the certification process that bestowed driver's licenses on both drivers, plus the benefits accrued by years of experience on the road. The second is constructed around a shared understanding of accountability along with confidence in the consequences of failure to abide by the rules of the road ranging from pecuniary penalties, to insurance rate increases, to loss of one's driver's license, to causing major damage to one's vehicle, and on up to jail time and even death. We need to engender similar trust and confidence in cyberspace to drive the kind of self-interested compliance that allows us to operate without fear. But how?

In recognition of the prominence of safety and trust, while also borrowing critical tenets from the U.S. military nuclear enterprise, we must focus on five critical areas to develop and inculcate the proper degree of accountability for individual or organizational activities in cyberspace.

First and foremost, we must *educate and train*. The ubiquity of cyberspace is not an excuse for failing to emphasize the importance of basic cyberspace protection at every opportunity; to the contrary, cyberspace's ubiquity demands lifelong attention to norms of behavior. Within the Air Force, the Nuclear Weapons Surety Program ensures that personnel are trained and certified on specified functional tasks whenever they hold positions that could affect nuclear operations. It includes initial nuclear surety training as well as recurring training for as long as they perform such duties. In the Navy, the principles inculcated into every nuclear propulsion operator are designed to provide protection through proper operations (the nuclear propulsion principles are integrity, level of knowledge, procedural compliance, forceful backup, questioning attitude, and formality). Applying similar standards to cyberspace means protection training should begin literally in elementary school and receive an appropriate emphasis throughout one's entire career to include all military professional schools (such as Service academies), Service and joint professional developmental education, and technical training. Unfortunately, there are hundreds of real-world case studies to help drive home the costs and risks of bad cyberspace practices in our education and training courses. Despite substantial differences between nuclear and cyberspace operations, when it comes to developing a culture of accountability the nuclear analogy reigns supreme and should be viewed as the gold standard when devising cyberspace protection training at every level.

Next, we should establish an explicit *chain of custody* for every network at every installation and facility throughout the military (and associated CDCs). There cannot be any ambiguity regarding who is ultimately responsible for every system and every network on any given installation. As a wing commander of a major Air Force installation, I did not "own" every network on my base, and more often than not I was not even aware of what was happening with several major networks and associated systems that were owned and operated by tenant units. While I was partly to blame for this lack of awareness (because I never asked all the right questions), the fact that there were so many different systems under different ownership is symptomatic of the chaotic network environment that exists across DOD today (entropy would be an understatement). This is precisely why senior leaders are advocating forcefully for the Joint Information Environment (JIE), which will eventually collapse thousands of DOD enclaves into a more defensible, secure, and standardized architecture that will simplify worldwide cyberspace operations and improve the ability to establish accountability. This is also a crucial step toward changing how we view DOD networks—that is, as mission-critical warfighting platforms rather than utilities we take for granted.

Third, we should provide defined *processes and procedures*, as well as *explicit guidance on behavior*, for cyberspace operations. The concept of "positive control" in nuclear operations is applicable to cyberspace because there must be clearly specified standards of performance and behavior. These standards prevent inappropriate interpretations or assumptions regarding what to do and how to act. While this may initially appear to impose onerous restrictions on the use of "wide open" cyberspace (and as such are anathema to those who are convinced that cyberspace should be no more restricted than the air we breathe), the concept of positive control is reflected in the road signs and traffic controls we live by when driving vehicles anywhere in the world. Absent well-defined guidelines, there will be too much room for misinterpretation or questionable behavior by anyone who touches cyberspace in any capacity.

Fourth, accelerating development of *advanced methods for controlling access* to networks or the information resident on them—such as credential-based access controls, boundary-layer controls, better forensics, and trustworthy computing platforms—is crucial. While one of the principal advantages to cyberspace is the ability to share information nearly instantly and globally, at every level of classification, and with one person or millions, there is no "unalienable right" to unfettered access to all systems and all information. As the U.S. Government learned the hard way in the Private Bradley Manning WikiLeaks incident, in certain cases access to cyberspace must be treated as a privilege, not a right. History teaches that regardless of the domain involved, the "insider threat" remains the greatest danger. That is even truer in cyberspace, demanding innovative ways to minimize the damage caused by the Private Mannings of the world. We must recognize that—analogous to the history of highway safety—the fault does not always lie solely with the operator. We need systems engineered to be used responsibly by people with a reasonable amount of training. Otherwise, we may be asking for unreasonable levels of proficiency on the part of the operator and not enough on the network administrator or software engineer.

Finally, we must *establish a formal DOD-wide "cyberspace mishap" investigation process*. We must treat network/system mishaps the same way we treat military aviation mishaps, for instance, by establishing categories such as Type 1/2/3 cyberspace mishaps analogous to Class A/B/C aircraft mishaps. A *Type 1 cyberspace mishap* would be defined using the criteria of loss of life, significant damage, or major impact to mission resulting in a requirement for formal general officer-led SIB- and AIB-like investigations. Type 2 and 3 mishaps would also require investigations but at lower levels and with varying degrees of reporting requirements.

The Commander's Program

We create the foundation for accountability in cyberspace by training personnel, establishing a chain of custody, providing explicit guidance, improving our methods to control access, and developing a formal investigative process. The other action that must overlay all of those activities is enforcement as a commander's program, to include publication of the implications of failure to obey the rules of the road in cyberspace and a demonstrated commitment to adhere to it. The commander's program for cybersecurity should receive the same emphasis as safety, to include a requirement that commanders at all levels continuously highlight "cyberspace protection" and "cyberspace safety" while also incorporating cyber security into all training, exercise, and inspection programs. Discussing it during periodic safety "down days" is important but hardly sufficient. On one hand, we should not expect a "zero-mistake" cyberspace force. Indeed, it is even more unrealistic to demand a zero-mishap culture in cyberspace than it is in any other domain. On the other hand, there are substantial differences between acts of omission and acts of commission. The former can be ameliorated through a focus on training, but there can be no quarter for the latter because it can easily put entire networks and weapons systems at risk. Still, unless and until the consequences of failure are stated explicitly and adhered to, there will always be room for misinterpretation and lax enforcement of punitive measures.

Along with training and certification and establishing cyberspace chains of custody, explicitly specifying the consequences of failure to follow the rules will build the necessary level of mutual trust and, similar to driving on our nation's roads without the steering-wheel death grip, allow us to operate more safely and securely in cyberspace. We must also strengthen and enforce existing agreements with CDCs. While there will be new financial and administrative costs associated with meeting more stringent DOD cyberspace accountability requirements, CDC chief executive officers, chief information security officers, and chief information officers must understand that the ultimate price for ignoring the rules is debarment from future business with the U.S. Government. While this will be extremely challenging politically, it is essential in halting the egregious exfiltration of sensitive information and intellectual property from CDCs across the United States and globally.

Fortunately, we are not starting from scratch in establishing our culture of cyberspace accountability. Training programs exist for operators and users of DOD cyberspace, to include annual information assurance and protection training. Similarly, the beginning of a chain of custody already exists with the certification and accreditation process, which requires approvals to both operate and connect systems. The standards for the training and certification and accreditation process, in addition to required security controls and a host of other processes and procedures, are documented in a large number of DOD issuances. Moreover, U.S. Cyber Command and the Services regularly perform Command Cyber Readiness Inspections of military organizations and CDCs, though these inspections cover only a small percentage of those eligible to be inspected because of a lack of capacity. JIE and similar initiatives demonstrate a commitment to advancing our security technology. Activities such as the Air Force's Operational Review Board already provide a framework for a cyberspace mishap investigation process.

Despite these ongoing efforts, we still lack the culture of accountability we aspire to, and we see the result in daily intrusions and in network exploitation. Once again, our experience from other disciplines that have figured this out over time offers a simple explanation: our commanders must make cyber security a priority. This will be reflected in the results of inspections, evaluations of unit and personnel performance, and disciplinary action when failures warrant it.

Similar to the accountability we seek to establish for our own cyberspace operations, these principles also apply to development of international norms of behavior in cyberspace. Turning from the tactical and operational to the strategic level, accountability is equally important when considering options to deny objectives or impose costs against cyberspace attacks that threaten our critical infrastructure and key resources. Nation-states, for example, must be held accountable for attacks they allow to originate from or pass through their sovereign territory, even if a nonstate actor or another nation is ultimately responsible for creating and launching the attack. As Microsoft's David Aucsmith puts it, "We must shift our discussion of doctrine away from attribution and towards accountability. People, organizations, and states should have an obligation to assist in cyberspace investigations where their property or jurisdiction is involved. Noncooperation should be viewed as a sign of culpability."[1] Accountability must be linked to the concept of cyberspace deterrence; that is, our political leaders should form an explicit link between establishing culpability for a cyberspace attack and the substantial costs that will be imposed for disregarding formal warnings. And, of course, this requires following up with actions to match the rhetoric. To do otherwise would completely undermine one of the core tenets of accountability.

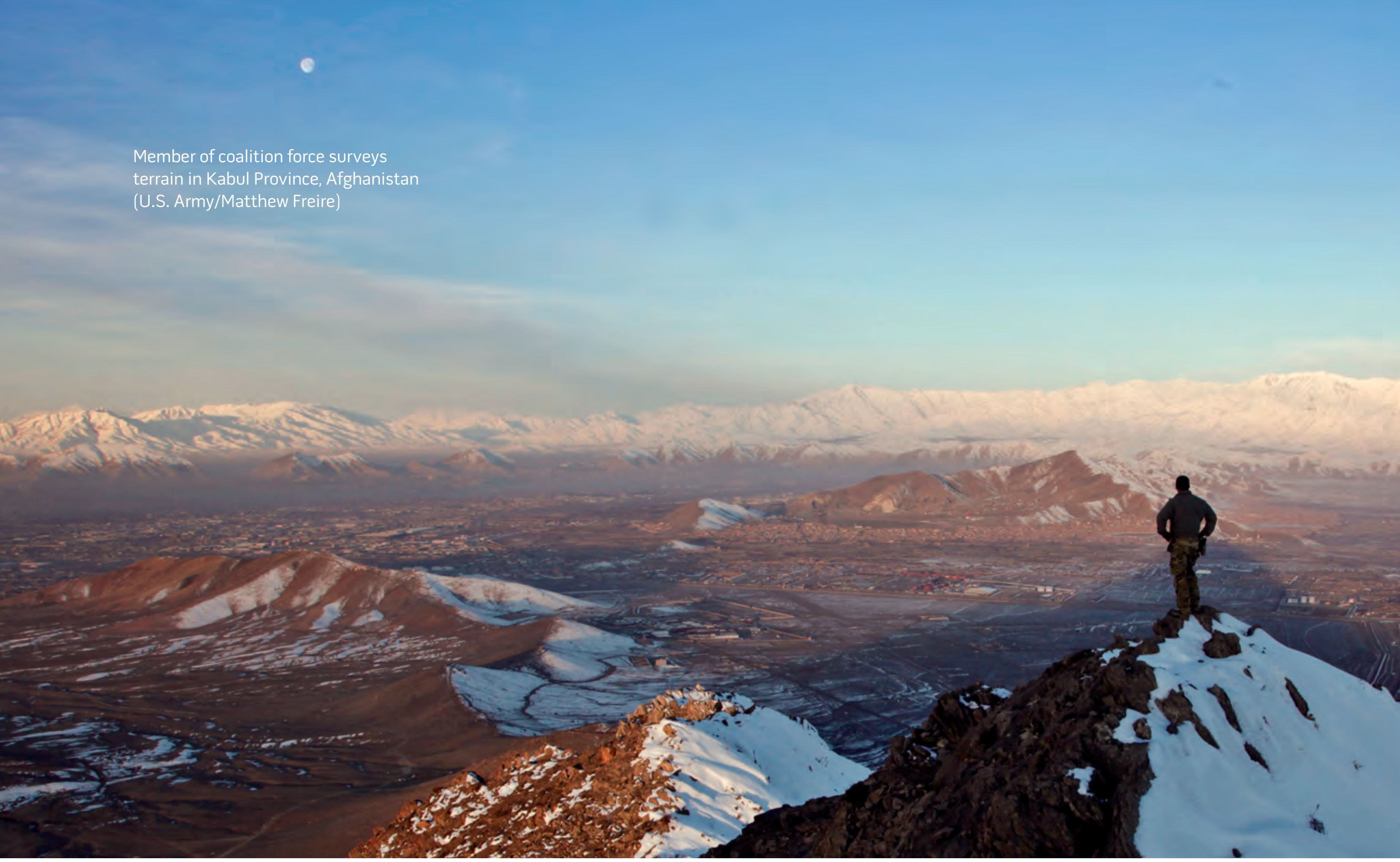
Implementation of the processes and procedures throughout the five focus areas outlined above suggests alternate endings for the three vignettes that open this article. The first incident never occurred because of the cyberspace protection training the Sailor received throughout his life and early in his Navy career, because the ship's network defenses prevented insertion of a thumb drive into a SIPRNet computer, and because he knew via the commander's intent that his commander would not tolerate the violation of rules prohibiting the use of the thumb drive. In the second scenario, the tasking order was implemented automatically, and even if it was not, there were only a small handful of different networks on the installation, allowing a recently established regional JIE Enterprise Operations Center to quickly identify and patch the vulnerability remotely. Finally, thanks to new Federal Acquisition Regulations and comprehensive cybersecurity legislation, the CDC in the third scenario was contractually and legally forced to shut down its network within the first hour after NSA/FBI/DHS identification of the nation-state exploitation operation. When the CDC subsequently refused to expend the funds necessary to fix its network defenses, it was barred from future business with the U.S. Government.

Conclusion

The cyberspace genie cannot be put back in the bottle. To the contrary, cyberspace genies are proliferating by the millions, so an evolutionary rather than revolutionary approach to accountability is called for. The perfect cyberspace defense will never exist. While the offense-defense pendulum will continue to swing in both directions, the advantage will reside perennially with the cyberspace attacker and the inside threat. Moreover, the wars of the future will be network-enabled, and we ignore this simple fact at our peril. In this game of highly complex four-dimensional chess, the side that can maintain and control its own networks while continuously adapting to a chaotic, fluid information environment will gain a distinct advantage. To develop and mature the necessary degree of accountability in cyberspace—a domain in which, more than any other save the nuclear enterprise, one tactical misstep may have grave strategic consequences—we must rely on the combination of the five focus areas described here with the view that their implementation is a commander's responsibility. Unless and until commanders place and foster the necessary and equal level of emphasis in all five core areas within their personnel—analogous to adhering to the principles of nuclear propulsion—the requisite culture of accountability in cyberspace will never take root. JFQ

Note

[1] David Aucsmith, "The Technology and Policy of Attribution," in *#Cyber Doc: No Borders—No Boundaries*, ed. Timothy R. Sample and Michael S. Swetnam, 14 (Arlington, VA: Potomac Institute Press, 2012).



Member of coalition force surveys terrain in Kabul Province, Afghanistan (U.S. Army/Matthew Freire)

Combined Effects Power

By Ervin J. Rokke, Thomas A. Drohan, and Terry C. Pierce

The information revolution continues to recast how power is generated and how it can be used to achieve desired outcomes. Advanced technologies and novel communication tools are enabling individual and group actions to achieve truly disruptive effects. As recent events confirm, a single individual operating in the cyber domain can spark the stock market to lose billions of dollars, attack military infrastructures, and seize the initiative on key international and domestic political issues. Web-based social networking can mobilize and align the power of group action with ease and speed. And individuals can be manipulated through the Internet to perform harmful acts.[1]

The private sector, not the military, is driving this revolution. The Services are understandably looking for revolutionary ways to employ these information age technologies in warfare. The problem is that traditional combined arms warfare (CAW) doctrine used to generate maximum combat power in the natural domains of land, sea, air, and space is not accommodating the broad range of novel power emerging in particular from the cyber domain. This article argues that a modified construct for how we think about the security challenge can enable our military to better observe, blend, protect, and project all types of power in the natural and cyber domains. In essence we recommend supplementing our current emphasis on traditional kinetic instruments of power with more explicit attention to desired effects.

Background

Combined arms warfare is the traditional concept that modern militaries use for maximizing combat power. It provides a lens through which to view the security arena and opens the door to a cognitive path for determining how

Lieutenant General Ervin J. Rokke, USAF (Ret.), is Senior Scholar in Residence in the Center for Character and Leadership at the U.S. Air Force Academy. Colonel Thomas A. Drohan, USAF, is Permanent Professor and Head of the Department of Military and Strategic Studies at the U.S. Air Force Academy. Captain Terry C. Pierce, USN (Ret.), is Director of the Center for Innovation at the U.S. Air Force Academy.

best to protect national security including economic interests.[2] CAW, in sum, is the prescribed doctrinal route that the joint force follows in developing strategies and force structures. It involves the "full integration of arms in such a way that to counter one form of armament the enemy must become more vulnerable to another."[3] Its historical legacy is impressive, dating back in the Western tradition as far as the Macedonian armies in the fourth century BC. Alexander the Great artfully combined phalanxes, cavalry, and dismounted runners in a novel way to conquer the Persian Empire.[4] In Chinese history, CAW was employed during the Spring and Autumn Period from the eighth through the fourth century BC. Over a millennium later, Carl von Clausewitz's *On War* offered a theoretical model of conflict that included the basic tenets[5] of the CAW concept.[6] Over time this combined arms construct has acquired nearly an immutable status as an unchangeable law of warfighting akin, perhaps, to Newtonian classical physics.

Quite clearly, CAW continues to enjoy substantial support among senior military leaders, particularly those in joint force. In 2008, for example, General James Mattis, USMC, then-commander of U.S. Joint Forces Command, issued guidance reaffirming the importance of using "time honored principles" in joint doctrine that have been "tested in combat" and "historically grounded in the fundamental nature of war."[7] He also made clear his strong preference for a combined arms approach as opposed to alternatives such as operational net assessment, effects-based operations, and system-of-systems approaches for developing security strategy and related force structure: "Our goal is to develop a joint force that acts in uncertainty and thrives in chaos through a common understanding of the essence and nature of the problem and the purpose of the operation."[8]

We agree with General Mattis's thoughtful goal statement as well as with his further assertion that we need operational concepts that link *ends* to policy and strategy through clear *ways* and *means*. We need to look no further than America's longest war—Operation *Enduring Freedom* in Afghanistan—to see the impact of failing to connect and fully define desired ends with appropriate ways and means. We also believe, however, that it is time to rethink a theoretical construct when empirical evidence begins to mount and very different phenomena emerge that the construct cannot explain or predict. In this regard, the CAW concept is increasingly unable to adequately accommodate the disruptive striking and resisting power of emerging noncombat arms. Just as Newtonian physics, developed in the late 1600s, was unable to explain the quantum revolution of the early 1900s, the CAW construct is unable to appreciate the dynamics of cyber and social network instruments of power sufficiently, particularly the substantial effects they produce nonkinetically.

Reexamining CAW

Against this background we see a need for more critical thought about how the CAW concept can better relate ways and means to desired ends. Indeed, we believe the paucity of such thought is a serious shortcoming, particularly if we fail to recognize that our enemies are increasingly comfortable operating beyond the traditional CAW concepts to employ the powerful new forces emerging, particularly in the cyber domain. Absent such rethinking, the emerging cyber forces—ours and those of potential adversaries—remain anomalous to our traditional CAW concept: their impacts are neither fully recognized nor anticipated in the context of struggle among adversaries of widely varying characteristics for equally disparate objectives. It is time to reexamine the CAW with a view toward retooling it to more effectively exploit these emerging power anomalies.

Cognitive psychologists tell us that because humans are frequently unable to grasp complex realities in a holistic sense, we craft simplifying "lenses, frameworks, or concepts" to help our understanding. Such is the role traditionally played by the CAW construct. It is a crucial role because it determines the extent to which we are able to view the breadth and depth of truly difficult problem sets; indeed, it is at the very heart of achieving an accurate understanding of our security predicament. We acknowledge that the CAW concept has worked well historically and continues to be helpful for assessing kinetic power in particular. As the late defense innovation chief Vice Admiral Arthur Cebrowski suggested, however, the information age has brought new forms of power from the cyber domain as well as nonkinetic aspects of power from the natural domains, which we believe the traditional CAW concept cannot accommodate effectively. The result is a cognitive tension—an incomplete view of power.

In response to this tension, we are "wired" to introduce new concepts or lenses that can proactively engage and adaptively shape the increasingly complex realities we face in the security arena. In his discussion of the evolution of principles of war, Lieutenant General James Dubik, USA (Ret.), former commander of the Multinational Security Transition

Command–Iraq, draws a parallel between the theories of a scientific revolution and the theories of warfare. He argues that when a substantial scientific theory faced difficulties, "the adherents of that view would treat the difficulties as *anomalies*."[9] At first they would try simply to "tweak" their existing theory to explain the anomalies. As the number of anomalies grew, however, they were forced to craft a new theoretical construct, which altered the perceived reality to accommodate the anomalies. In sum, General Dubik asserts, "the emergence of the information age has shifted the very foundations of the profession of arms. . . . Clearly the framework that guided decisions and actions in the past is just that, past."[10]

Using Dubik's metaphor, it seems we are in the tweaking phase of converting the challenges of operating in cyberspace "into a warfighting mold shaped by the four older domains."[11] A recent literature review of the cyber domain, for example, offers recurring CAW themes: we must *dominate* cyberspace,[12] and we must determine how the cyber domain can be mainstreamed into the CAW model as an operational discipline alongside land, sea, and air warfare.[13] In fact, Navy cyber leaders argue that the information technology "network and its components (information, intelligence, technology, and people) have become a combat system. In this form, they suggest, the network can serve as a platform from which to launch information as a weapon."[14] Some CAW pundits even assert that operating and fighting a network as a warfare platform will enable cyber networks to join existing platforms from the physical domains such as ships, aircraft, and infantry units and form combined arms teams.[15]

Such *tweaking* approaches are focused on translating the cyberspace anomalies into instruments compatible with a CAW concept conceived for dealing with the natural domains. We take strong issue with this approach. Ultimately, we are convinced that it will prove inadequate to force the anomalies of the cyber domain into the CAW concepts of mass, speed, fires, control, maneuver, dominance, superiority, and hierarchy.[16] As a military profession that has traditionally relied on platforms and combat arms for maximizing combat power, the "reality" we perceive when we look through the CAW lens at the many happenings in cyberspace today is random and unfathomably complex. The CAW lens's focus on traditional instruments of warfare from the natural domains of land, sea, air, and space ignores important parts of the "reality picture." Put simply, the CAW model is the wrong construct for conflicts that include action and reaction in the cyber domain (as nearly any conflict in the future will), and it is giving us fits.

CAW Anomalies

In anomaly theory research, the focus is on discovering anomalies and understanding why the current theory does not explain their existence. It is only when we can identify such anomalies that an opportunity exists to improve the relevant theory.[17] Understanding how and why anomalies are emerging is how new constructs are built. Against this background, let us look at several anomalies with a view toward identifying ways to improve the CAW construct's capacity for accommodating and exploiting the emerging forces from the cyber domain in particular.

Cyber Soft Power. Unlike the natural domains, the cyber domain is a manmade entity consisting of networked systems. It is, in a sense, the world's largest ungoverned space with its own medium and constantly changing rule sets.[18] Significantly, it is also shifting the concentration of power—most of which is nonkinetic, or "soft"—from combined arms forces to individuals.[19] It generally does not use physical force in a coercive sense, but rather tends to use networked systems to influence and to persuade behavior by attracting and co-opting. It is distinctive in its capacity to enable single individuals to exert uncommon soft power and private commercial entities to exert far greater influence over the domain than governmental authorities do.

The resulting easy access to this domain by both governments and private individuals creates an abundance of lucrative targets for serious mischief as well as legitimate endeavors, most of which fall outside the CAW focus on traditional instruments of power associated with natural domains. The Stuxnet Cyber Worm, for example, is a powerful instrument, but it remains an anomaly for CAW because it is neither a platform nor a combat arm, and its effects can go far beyond traditional calculations about destruction. Cyber attackers are successfully compromising the network security of banks. In another example, the self-proclaimed Izz ad-Din al-Qassam Cyber Fighters have claimed responsibility for several attacks against American financial institutions that have taken these corporations offline intermittently, costing millions of dollars.[20]

Social Network Power. Cyber technology platforms operating in cyber space, such as Google and Facebook, are providing a powerful destructive tool to conduct Wiki War.[21] The power of such social networks comes from their ability to scale like spreading viruses and create a rapid and direct impact on societal action.[22] For example, the WikiLeaks story of a U.S. Soldier and recent events involving a National Security Agency contractor stealing and releasing hundreds of thousands of government digital secrets have done considerable harm to our nation.[23] In another example, the so-called Syrian Electronic Army hacked into an Associated Press Twitter feed and reported a fake White House attack that briefly wiped out $136.5 billion of the Standard and Poor's 500 Index value.[24] Our CAW focus on ways and means (traditional arms) overlooked the critical factor of ends (effects) and the resulting anomalies were significant.

Virtual Reality Power. As demonstrated by the Boston Marathon bombing, the cyber domain enables terrorists to recruit, radicalize, train, and execute in the virtual world in a far more rapid and precisely targeted manner.[25] Indeed, it enables terrorists to live physically in different regions of the natural domain of land but to operate virtual cells for collaboration and execution in a carefully crafted distributive virtual world. When it suits their purposes, terrorists can shift from the soft power cyber domain to hard power natural domains for destructive attacks. Once again, our CAW concept does not provide a lens sufficient for understanding or predicting such activities.

Crowdsourcing. Finally, the marathon bombing incident demonstrated the capability of social networking tools to build collaborative virtual communities and then harness the resulting "wisdom of crowds" for constructive purposes.[26] The Federal Bureau of Investigation's public release of two poor-quality images of the suspects with a request for assistance resulted in the mobilization of hundreds of private citizens who reviewed their own photography of the event and provided a flood of helpful images to the police. A similar phenomenon explains how the killing of a young woman in Iran resulted in a powerful mobilization of public opinion by private citizens who used their smart phones to photograph the event and quickly distribute the pictures worldwide.

The above examples of power emerging from the cyber domain demonstrate a common capacity for producing desired effects by directly influencing the perceptions and behavior of adversaries whether they are individuals, nongovernmental organizations, or nation-states. In short they provide measurable outcomes in efficient ways for the battle of wits. Regrettably, most of their outcomes are shielded from view by the CAW lens's focus on traditional instruments of warfare associated with the natural domains.

Newtonian Physics and CAW Anomalies

These and multiple other elements of power that are in large part emerging from the cyberspace domain cannot be accommodated adequately by the CAW construct. The cyber domain is challenging previously conceived theories of power by spawning a host of anomalies. This anomaly challenge resembles a similar problem the physics community faced in the early 1900s. Just as the CAW construct has explained hard power in the natural domains for several centuries, Newtonian physics offered a powerful conceptual model for explaining the fundamental forces of nature for several hundred years. Then came Ernest Rutherford's early experiments with the atom, which revealed that nature sometimes did not behave in accordance with Newtonian theory. Put simply, Newton's theory of motion and gravitation had an anomaly; it simply did not accurately predict the physical principles that governed the behavior of electrons orbiting the nucleus of the atom. Niels Bohr, August Heisenberg, and others met the challenge with a new concept for atomic behavior: quantum mechanics.

Kandahar PRT security force leads team member through Shur Andam Industrial Park in Kandahar City (U.S. Air Force /Richard Simonsen)

This article proposes a more modest solution for the CAW anomalies. It is a complement to the CAW concept that accommodates the behavior of participants in the cyber domain as well as soft power participants from the natural domains. We call it the Combined Effects Power (CEP) construct. We are not jettisoning the CAW model. Just as Newtonian classical theory still explains gravity and the mutual attraction of the planets, CAW remains a valid model for understanding hard power in the natural domains. We believe, however, that our proposed CEP concept can serve, like the concept of quantum mechanics for Newtonian anomalies, as a remedy to explain the CAW anomalies.

But unlike the classical and modern physics analogy, we believe CEP is a unifying construct that can amplify and preserve the deepest tenets of CAW's hard power while integrating the critically important soft power behavior we are observing in the natural as well as cyber domains. As a new way of thinking, the CEP construct is capable of accommodating and exploiting these forces in a single, all-encompassing, coherent framework. The integrating tenet for this framework is *effects*. Focusing on effects allows measurement of both hard and soft power. The CEP construct thus effectively overcomes the soft power anomalies generated by our traditional focus on arms and puts the cyber domain on the same playing field as the natural domains.

The CEP construct also has the ability to accommodate not only first- and second-order effects from the CAW construct, but also to align (or harmonize) them with n^th-order effects resulting from soft and hard power regardless of the parent domains. For example, while the CAW construct enables understanding of the first-order effects of "sequestration," the more significant n^th-order effects on subjective aspects of capability, morale, and complex interactions of human networking, for example, are better understood through the broader lens of CEP. This is equally relevant for distributed operations beyond the range of traditional CAW supporting forces as well as for distributed tactical groups self-organizing (or self-coordinating) for reaction to fleeting opportunities in accordance with commander's intent. In other words, the CEP construct would enable us to rack and stack the different orders of first- through n^th-order effects of both hard and soft power more effectively. Indeed, we would see a flattening and simplifying of the command and control hierarchy as well as a wider horizontal span of understanding and control for combat operations.

Combined Effects Power

Once again, we note that atoms existed in 1687 when Newton published his *Principia Mathematica* and that the physical science community believed his laws adequately explained atomic behavior. They did not, however. Only with the quantum revolution in modern times were we able to understand the nuclear atom. And so it is that the CAW model has existed for thousands of years as the intellectual construct for understanding power. But however effective it may have been for understanding the effect of destroying opposing force structures in the natural domains, it is increasingly beset with challenges emerging from the cyber domain as well as nonkinetic forces from the natural domains. Furthermore, we are also concerned that most commanders today are using the CAW mental construct in attempting to understand cyber power. Such an approach is analogous to using reading glasses to observe a distant object.

Then what is CEP? Combined effects power is essentially a way of thinking—a cognitive path that looks at a complicated security problem set through a quite different lens and addresses a new question at the outset: What effects do we want to achieve using both hard and soft power? It expands our frame of reference beyond the traditional CAW lens, which for centuries has focused on natural domain weapons systems and asked the question: How do we most effectively create a coherent, flexible force structure and strategy? With CEP's wider lens and new question, the door is opened for leaders and commanders to better understand the human dimension of conflict—the thinking of our opponents (and allies). Most importantly, perhaps, it recognizes that the information age revolution has dramatically changed the means of application, speed, breadth, and potential impact of soft power.

Put simply, the CEP construct is a way to maximize and harmonize hard and soft power. It allows for the full integration of all effects generated from power arising in both the natural and manmade domains. It rejects the traditional notion that the "supported effort" is always an arm or platform; cyber domain soft power is no longer the default choice for supporting or secondary efforts. The CEP construct's new question and wider lens allow for a level playing field—an accessible battlespace—on which all domains can participate as appropriate. Whereas the aim of CAW was to use all available resources to generate maximum hard power, the aim of CEP would be to use all available resources to generate power relevant to desired effects whether it is hard or soft. The units for measurement of effectiveness would reflect increments of desired effects, not necessarily levels of physical destruction.

Prospects for Change

We are realistic about the difficulties of effecting disruptive changes in so fundamental a construct as CAW. Most certainly we are aware of the rich and intense dialogue during the past decade among Marine Corps leaders such as General Mattis and Lieutenant General Paul Van Riper, who supported the traditional CAW construct, and their Air Force contemporaries such as Lieutenant General David Deptula and Major General Thomas Andersen, who led in developing an effects-based approach as a way of thinking about and executing operations.[27] The passionate commitments of these strategists to quite different ways of thinking about our security challenges were not reconciled, but nevertheless they allowed sufficient flexibility on both sides for joint effectiveness in such practical matters as the Operation *Desert Storm* air campaign. More important for our purposes, the substance of this dispute showed remarkable foresight about the doctrinal imperatives of the emerging and future weapons systems with which we must deal today. As Lieutenant General Deptula explains:

> *Effects-based operations provide a useful construct on how to conduct war that can bridge the gap between the weapons of today and the weapons of the future. It allows useful application of current weapon systems as we acquire a new generation of tools needed to fully exploit the concept. . . . The ability to achieve effects directly against systems without attacking their individual components would allow a preferable application of the concept of parallel war* [or CEP] *than we are capable of today. Indeed, the ultimate application of parallel war* [or CEP] *would involve few destructive weapons at all–effects are its objective, not destruction.*[28]

As the late Admiral Cebrowski suggested, the long-held principles underlying theories of war were "chafing against new realities on the battlefields . . . and when this happens, rules change."[29]

Against that background, an emerging group of strategic thinkers such as Martin Libicki of the RAND Corporation and Major Kris Barcomb, an Air Force cyberspace strategist, is looking at the cyber domain quite differently than simply as new high ground for *natural domain* warfare.[30] For example, Major Barcomb asserts that "hard power will be secondary to soft power in cyberspace for the foreseeable future" and calls for a new paradigm to better understand the proper role of the military in the cyber domain.[31] Using our vernacular, both Libicki and Barcomb seem intent on substantially modifying the traditional CAW model for understanding cyber domain capabilities. We do not know whether Libicki and Barcomb would agree, but we believe this new framework could well focus on what we refer to as the CEP construct.

Once again, implementing such new thinking will not be easy. Despite de facto movement toward more acceptance of effects-based approaches to operations and planning,[32] there remains a tendency throughout all the U.S. Services for continuing their traditional efforts to push the soft power capabilities of cyberspace as well as those emerging from the natural domains through the CAW hard power construct.[33] Cyber experts such as Libicki and Barcomb, intent on crafting a new paradigm for strategic thinking about the critical cyber domain, struggle to overcome such efforts.[34] The major challenges they face include the substantial cultural identity that the CAW model reinforces in our thinking about power as well as its capacity to provide legitimacy for the major weapon systems associated with each of the natural domains.

At the same time, however, the emerging anomalies associated with the cyber domain and other soft power capabilities from the natural domains have an increasing momentum of their own. Their force is significant, particularly for the United States with its great dependence on the cyber domain. If history is a guide, theoretical constructs such as CAW will ultimately give way to adaptations to exploit anomalies emerging from an increasingly complex security environment. The issue is not *whether* CAW will adapt, but rather *when* natural forces will overcome its grip on how we think about our security predicament.

Finally it has not escaped our notice that the CEP construct offers an alternative path for sorting through research and development challenges associated with force structure. We are left with the critical question of whether policymakers and strategists are willing to grapple with a fundamentally new way of thinking about complex and messy issues. Whatever the case, it is clear that our potential opponents are increasingly comfortable in this thicket. **JFQ**

Notes

[1] Gary Strauss et al., "SEC, FBI probe fake tweet that rocked stocks," *USA Today*, April 24, 2013, available at <www.usatoday.com/story/news/nation/2013/04/23/hack-attack-on-associated-press-shows-vulnerable-media/2106985/>; Nicole Perlroth and David Sanger, "Cyberattacks Seem Meant to Destroy, Not Just Disrupt," *The New York Times*, March 29, 2013, B1; Clay Shirky, *Here Comes Everybody: The Power of Organizing Without Organizations* (New York: Penguin, 2008).

[2] Kris Barcomb, "From Sea Power to Cyber Power," *Joint Force Quarterly* 69 (2nd Quarter 2013), 79; also see Paul G. Kaminski, "Dealing with the Cyber Threat to Our National and Economic Security," speech, Pittsburgh, PA, January 10, 2013.

[3] Robert Leonard, *The Principles of War for the Information Age* (New York: Ballantine Books, 2009), 67.

[4] Jonathan M. House, *Combined Arms Warfare in the Twentieth Century* (Lawrence: University of Kansas Press, 2001), 1–2.

[5] Carl Von Clausewitz, *On War*, ed. and trans. Michael Howard and Peter Paret (Princeton: Princeton University Press, 1989), 4, 291.

[6] Clausewitz, 285–291, 295–296.

[7] James N. Mattis, "Memorandum for U.S. Joint Forces Command: Assessment of Effects Based Operations," *Parameters*, August 14, 2008, 22.

[8] Ibid.; attachment with "USJFCOM Commander's Guidance for Effects-Based Operations," August 14, 2008.

[9] James Dubik, "Get on with It," in *Rethinking the Principles of War*, ed. Anthony D. McIvor, 2 (Annapolis: Naval Institute Press, 2005).

[10] Ibid., 8.

[11] Martin C. Libicki, "Cyberspace Is Not a Warfighting Domain," *I/S: A Journal of Law and Policy for the Information Society* 8, no. 2 (2012), 328.

[12] Kendall Card and Michael Rogers, "The Navy's Newest Warfighting Imperative," U.S. Naval Institute *Proceedings* 138, no. 10 (October 2012), 23.

[13] Ibid.

[14] Ibid.

[15] Ibid.

[16] Richard Hundley, *Past Revolutions Future Transformations* (Santa Monica, CA: RAND, 1999), 11–12; Paul Carlile and Clayton Christensen, *The Cycles of Theory Building in Management Research* (Boston: Harvard Business School, January 6, 2005), 4; Barcomb, 80; Libicki, "Cyberspace."

[17] Carlile and Christensen, 4.

[18] Eric Schmidt and Jared Cohen, *The New Digital Age: Reshaping the Future of People, Nations, and Business* (New York: Borzoi Knopf of Random House, 2013), 3, 6; Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica, CA: RAND, 2009), iii.

[19] Ibid., 6.

[20] Perlroth and Sanger.

[21] For a discussion of modern technology platforms as paradigm shifts in soft power, see Schmidt and Cohen, 9.

[22] Ibid., 10.

[23] Ibid., 10, 162.

[24] Alina Selyukh, "Bogus 'Obama injured' tweet upsets US Markets," *Mail & Guardian* (Johannesburg, South Africa), April 24, 2013, available at <http://mg.co.za/article/2013-04-24-false-tweet-from-hacked-ap-account-irks-us-markets>; Dan Goodin, "Hacked AP Twitter feed reporting fake White House attack rocks markets," *ArsTechnica.com*, April 23, 2013, available at <http://arstechnica.com/security/2013/04/hacked-ap-twitter-feed-rocks-market-after-sending-false-news-flash/>.

[25] Schmidt and Cohen, 151.

[26] James Carafano, *Wiki at War: Conflict in a Socially Networked World* (College Station: Texas A&M Press, 2012), 178.

[27] John Correll, "The Assault on EBO," *Air Force Magazine,* January 2013, 51.

[28] David Deptula, *Effects Based Operations: Change in the Nature of Warfare* (Washington, DC: Aerospace Education Foundation, 2001), 21–22.

[29] Anthony McIvor, ed., *Rethinking the Principles of War* (Annapolis: Naval Institute Press, 2005), ix, xii.

[30] Libicki, "Cyberspace," 328.

[31] Barcomb, 83.

[32] See, for example, Air Force Doctrine Document 3-0, *Operations and Planning* (Washington, DC: Headquarters Department of the Air Force, November 9, 2012).

[33] Card and Rogers, 23.

[34] Barcomb, 79.

Airman maintains communications cabling including copper wiring, indoor and outdoor cabling, and telephone switches (U.S. Air Force/George Goslin)

Information-Sharing with the Private Sector

By Veronica A. Chinn, Lee T. Furches, and Barian A. Woodward

Imagine logging onto your bank's secure Web site using your personal computer to pay monthly bills or transfer money between accounts to pay your mortgage. When you enter the Web site address or try to access a favorite link, you receive an error message. You check to see if your router is working and then verify that your Internet service is connected. You check other Web sites, and they load without issue. You call your bank to report the problem and they tell you their service should be available as soon as they fix a technical issue. Meanwhile, time is ticking toward the due date on your bills. This is what can happen when a major bank is under a denial-of-service attack.

At PNC, Wells Fargo, J.P. Morgan Chase, Bank of America, and a host of other big-name banks, this problem occurred in September 2012 and again the following January.[1] Millions of customers could not reach their accounts online because so-called hacktivists were using this method of cyber ransom to prove what they were capable of and to make political points.[2] Most major banks have some protection against such attacks.

Lieutenant Colonel Veronica A. Chinn, USA, is a Future Operations Planner at U.S. Cyber Command. Lieutenant Colonel Lee T. Furches, ANG, currently serves as the Air National Guard Strategic Planner in the Office of the Assistant to the Chairman of the Joint Chiefs of Staff for National Guard and Reserve Matters. Major Barian A. Woodward, USMC, currently serves as a Cyber Defense Capabilities Officer with U.S. Strategic Command.

If they require assistance, the Federal Bureau of Investigation (FBI) has developed the capability to track down many criminal organizations involved in denial-of-service attacks. But what if would-be attackers, sponsored by terrorist groups, nonstate actors, or nation-states, organized themselves to conduct a concerted cyber assault of more than the financial sector? That might be more than even the FBI could handle.

Since nongovernmental entities own and operate a large majority of cyberspace and critical infrastructure, the United States needs not only a whole-of-government approach to cybersecurity but also a whole-of-nation approach. The U.S. Government must articulate the details of such an approach in a strategic framework that identifies a significant role for the private sector. To develop that framework, the Nation needs robust information-sharing between government and industry.

In 2003, the Bush administration issued the beginnings of such a strategy with its *National Strategy to Secure Cyberspace* (NSSC), which called for greater linkages between the public and private sectors. Unfortunately, over the past decade, several shortfalls or ill-conceived initiatives prevented the establishment and maturation of such cooperative paradigms. To engender a whole-of-nation approach to cybersecurity, the U.S. Government must tailor legislative and executive branch efforts to cybersecurity, enable information flow between the Intelligence Community (IC) and the industrial sector, address overclassification of threat reporting information, and maintain assignment for the national lead in cybersecurity to an entity outside the IC.

The NSSC was the first foundational strategic guidance document produced by the United States focused exclusively on cybersecurity. The strategy centers on five mutually supporting priorities:

- National Cyberspace Security Response System
- National Cyberspace Security Threat and Vulnerability Reduction Program
- National Cyberspace Security Awareness and Training Program
- Securing Governments' Cyberspace
- National Security and International Cyberspace Security Cooperation.[3]

A key concept presented in the strategy is "public-private partnership." President George W. Bush stated, "Reducing . . . [cybersecurity] risk requires an unprecedented, active partnership among diverse components of our country and our global partners."[4] This statement suggests that national leadership at the highest level recognized the need to engage outside the government apparatus over a decade ago. The executive branch released the draft version of the strategy to the public for review and convened 10 town hall meetings across the country to elicit feedback. The public was considered an integral part of the resulting strategy.[5]

The NSSC prescribes a whole-of-nation approach and accordingly provides a baseline for analysis of national efforts to secure cyberspace. Its priorities are separate and distinct, each with its unique required actions and initiatives, but a common requirement is information-sharing. In subsequent years, there were numerous reasons for the government's inability to fully develop a culture of information-sharing between the public and private sectors, but four issues stand out.

Information-Sharing Impediments and Shortfalls

First, executive and legislative branch efforts intended to address information-sharing in our post-9/11 reality failed to emphasize all-threat cybersecurity. Rather, most of these narrowly scoped undertakings focused exclusively on counterterrorism. For example, the President issued the *National Strategy for Information Sharing* and Executive Order (EO) 13388, *Further Strengthening the Sharing of Terrorism Information to Protect Americans.* Both apply exclusively to combatting terrorism. Congressional efforts as well, to include the comprehensive Intelligence Reform and Terrorism Prevention Act of 2004, focused solely on counterterrorism. Certainly all these efforts can provide value in countering terrorist-originated cyber attacks. However, defending the Nation against cyber threats transcends such a single-threaded, counterterrorism-steeped scope.

National cybersecurity is an ambitious, broadly focused endeavor seeking to counter a wide spectrum of threats, which certainly encompasses terrorist-launched cyber attacks. However, the cyber threat spectrum includes many nonterrorist dangers as well. The teenaged "script kiddie" in his mother's basement, who may be a cliché but is not yet passé, still presents a risk to national infrastructure. Highly organized cyber criminals hack into and mine financial companies' databases for monetary gain. Internet-based activists—or hacktivists—illegally access computer systems to draw attention to their politically or socially motivated causes. And powerful nation-states back increasingly robust cyber espionage programs. With such a myriad of threat actors and motivations, the United States cannot rely exclusively on counterterrorism-focused intelligence reform as a proxy for broader reforms optimized for the unique pursuit of all-threat cybersecurity.

Second, the IC has few mechanisms for the seamless flow of information to and from potential industry partners. The ideal role for both the public and private sectors involves information-sharing and flow in both directions. For example, industry must share its real-time observations about cyber attacks with the government on its networks so agencies can warn other companies about these threats. Also, the government, particularly the IC, must be willing and enabled to share its threat reporting information with the private sector. The Nation's critical infrastructure owners and operators will then be better able to secure their systems. At present, information-sharing does not occur optimally in either direction. Private industry currently sees two main disincentives to information-sharing with the government. Their primary concern is privacy. These companies are generally concerned that information they share about intrusions into their networks may leak to competitors or potential customers and negatively impact their bottom lines. Also, they fear liability, especially if it becomes known that they lost data or caused the loss of data critical to another company's or individual's financial well-being. These issues significantly impede reporting of cyber attacks to the government.

For its part, the Intelligence Community unfortunately focuses almost exclusively on information-sharing among its 17 member agencies and organizations. To its credit, the IC seems to understand the need for a broader information-sharing focus. While the White House and Congress concentrated rather myopically on terrorism, the IC developed more broadly focused publications. Specifically, their 2008 information-sharing strategy and 2009 Intelligence Community Directive Number 501 implement 2004 intelligence reform act imperatives. These documents are not counterterrorism-specific, which allows potential for their broad application. However, their shortfall in the context of nationwide information-sharing is that they do not facilitate sharing outside the IC. As observed, many other entities—from state and local governments to non-IC military organizations to private industry—have a significant stake and role in the national solution to cybersecurity.

Due to the extreme sensitivity of its work, the Intelligence Community has an institutional but understandable reluctance to share information. However, cybersecurity differs from most IC missions in its inextricable relationship to the industrial base. The need for information-sharing in this arena is similar to that recognized over the past decade in counterterrorism. The government must now extend the lessons learned in counterterrorism information-sharing to cybersecurity. In 2011 congressional testimony, Zoë Baird Budinger and Jeffrey H. Smith of the Markle Foundation observed, "This transformation we are seeing in counterterrorism is built upon principles and practices that can be extended to other key homeland security priorities so that our government can work in a more modern, decentralized, public-private manner to address growing challenges like cybersecurity and economic security."[6]

A key element of extending such an information-sharing paradigm expressly to cybersecurity will include sharing related threat-reporting information. The IC holds much of this information in its databases. Unfortunately, the classification of this information often limits its dissemination to many who could use it to enhance the Nation's cybersecurity. This leads us to a related impediment to information-sharing.

Third, the tendency toward overclassification of relevant data impedes the flow of useful information to industry partners. Setting the stage for the discussion following the 2001 terrorist attacks, *The 9/11 Commission Report* concluded:

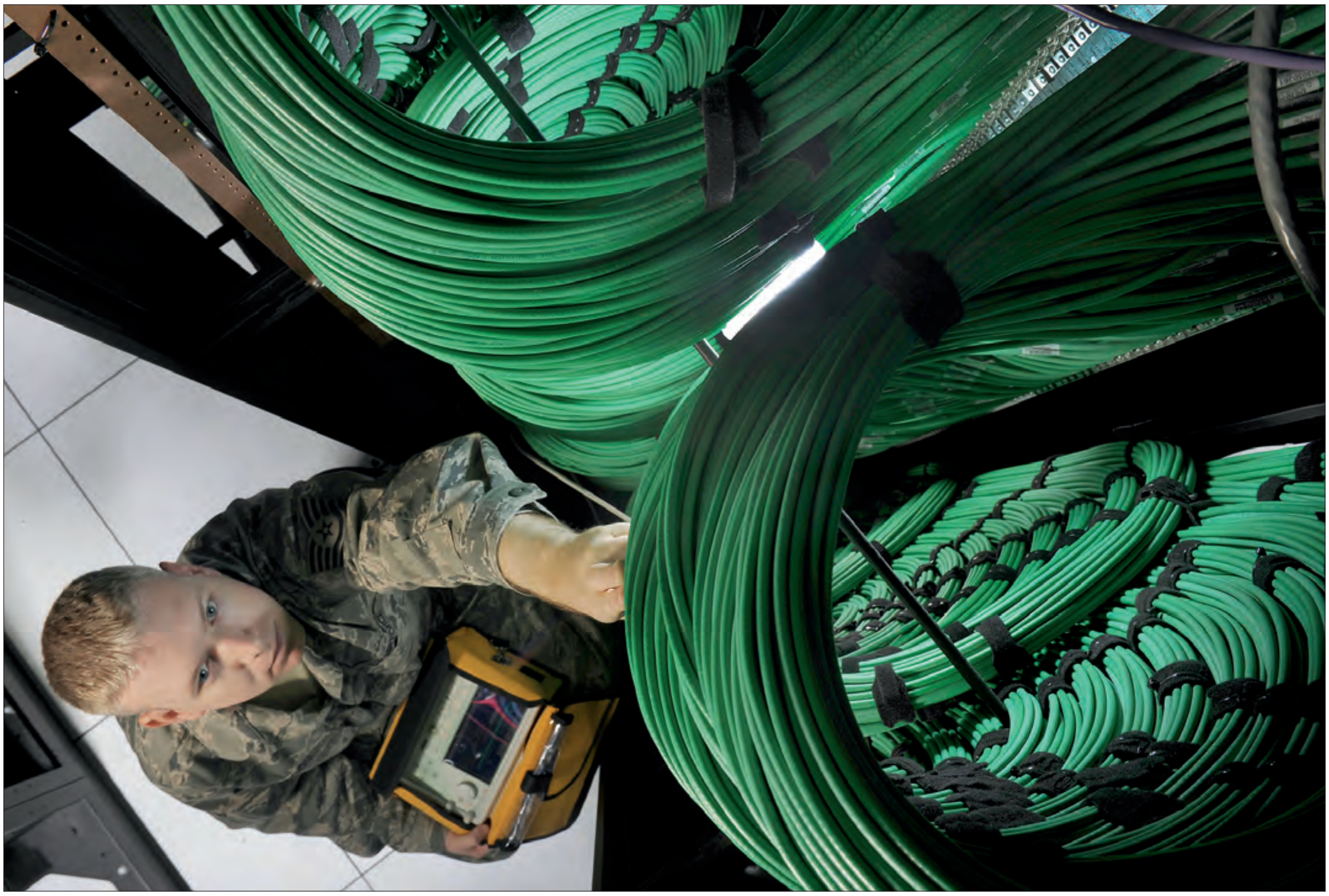
> *Current security requirements nurture over-classification and excessive compartmentalization of information among agencies. Each agency's incentive structure opposes sharing, with risks (criminal, civil, and internal administrative sanctions) but few rewards for sharing information. No one has to pay the long-term costs of over-classifying information, though these costs—even in literal financial terms—are substantial. There are no punishments for not sharing information. Agencies uphold a "need-to-know" culture of information protection rather than promoting a "need-to-share" culture of integration.*[7]

Pursuant to specific 9/11 Commission recommendations and complementary to the Intelligence Reform and Terrorism Prevention Act of 2004, Congress passed the Reducing Over-Classification Act in 2010.[8] Most significantly, the act requires inspectors general from all Federal departments or agencies with original classification authority to conduct a review of classification policies and identify those that may contribute to misclassification of information.[9] Per a 2011 Department of Defense (DOD) Inspector General memorandum, this review is ongoing.[10]

If the DOD review includes the National Security Agency (NSA), arguably the most prolific generator of cybersecurity threat reporting, this act could improve the quantity and usefulness of cybersecurity threat reporting available for sharing among Federal, state, and local governments and private industry. Until this review is complete, however, the Federal Government must remain cautious about overcommitting the work of cybersecurity to the extremely capable but super-secretive agency, bringing us to our final issue: the United States must resist the urge to transfer primary responsibility for national cybersecurity to NSA.

The NSA has remarkable experience in cyberspace operations and information assurance in the DOD realm, but while its preeminent expertise is immensely useful in nonmilitary cybersecurity issues, assigning the lead to NSA would almost certainly prove counterproductive in fostering whole-of-nation collaboration. To illustrate the fears this proposition instills in the cybersecurity community, we can examine the reaction to comments from then Director of National Intelligence Dennis Blair. In congressional testimony in 2009, he kicked off a firestorm within the Department of Homeland Security (DHS) and the private sector by suggesting that NSA's extensive cybersecurity expertise should be "harnessed" to secure Federal and critical infrastructure networks.[11] Many saw this as a play for a lead role in national cybersecurity and expressed concern that NSA would gratuitously enshroud its cybersecurity efforts under high levels of classification. Such a transfer of responsibility would make whole-of-nation collaboration on cybersecurity difficult or even impossible.

The 2008 *Comprehensive National Cybersecurity Initiative* (CNCI) stands as a related example of the effect an overly secretive approach might have on collaboration. Blair testified that the CNCI "develops a framework for creating in partnership with the private sector an environment that no longer favors cyber intruders over defenders."[12] However, the CNCI is classified Secret. Many question how a classified initiative can support



Airman uses spectrum analyzer to check television broadcast network routers (U.S. Air Force/Val Gempis)

such collaboration with the private sector if that community cannot even access the plan. The lead for cybersecurity is best left in the hands of an organization less prone to overclassification of its work. In 2003, NSSC assigned DHS as the lead, and so it should remain, with augmentation from NSA and other agencies.

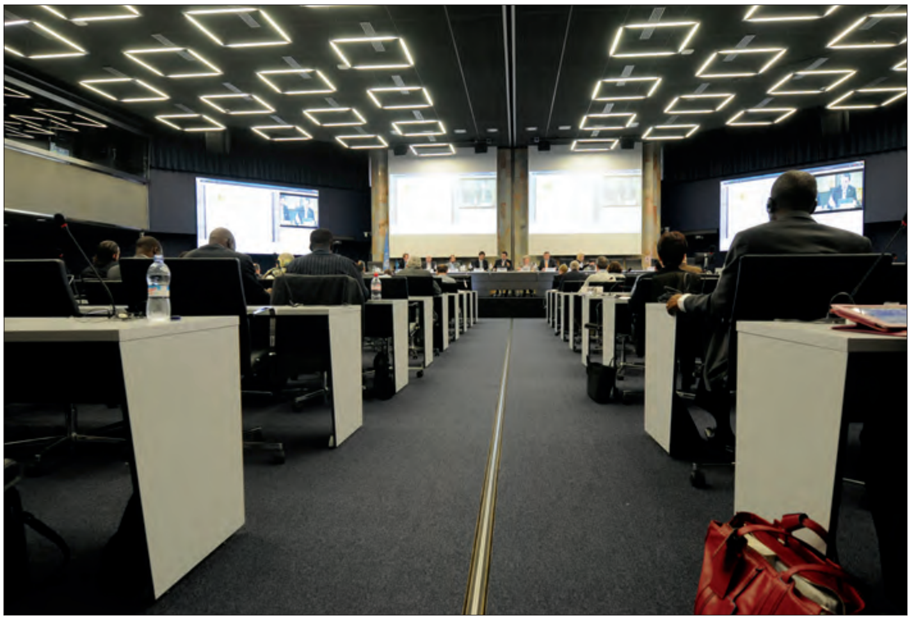
Recent Executive Actions

Many argue that EO 13636, *Improving Critical Infrastructure Cybersecurity*, and Presidential Policy Directive 21 (PPD-21), *Critical Infrastructure Security and Resilience*, take the next step toward creating the whole-of-nation approach envisioned by the NSSC. Both documents focus on critical infrastructure due to the impact on national security, economic stability, and public safety that could result from a deliberate cyber attack. They only differ in their approach. Taken together, they make progress toward a whole-of-nation effort but only constitute a partial solution in the end.

According to Harold Relyea, a specialist in American National Government at the Congressional Research Service and author of the report *Presidential Directives*, there are two primary differences between an executive order and a Presidential policy directive. An executive order has a statutory requirement to be published in the *Federal Register*, but a PPD has no such requirement, which means a PPD can be classified. Additionally, an executive order must be circulated to a general counsel or similar agency attorney as "a matter of circulation and accountability."[13] These differences aside, an opinion written by the Justice Department Office of Legal Counsel in 2000 concludes that "executive orders and directives are equivalent in their force and impact."[14]

EO 13636 directs three primary tasks that must be initiated to set conditions for further improvement of cybersecurity. The first is to identify the critical infrastructure at greatest risk to cyber attack based on the current threat, its vulnerability to cyber attack, and the impact on national interests of its degradation or destruction. The second is to improve information-sharing and ways to more effectively produce, disseminate, and track classified reports that involve critical infrastructure owners and operators. The third is the establishment of a "Cyber Security Framework." The order sets a 2-year timeline to accomplish all these actions with the majority of them within 120 days of the order's publication.[15] Each of these tasks identifies DHS as the lead agency with other agencies in support.

In the words of Frederick the Great, "He who defends everything defends nothing." This is no less true in cyberspace than in other forms of warfare, given the tremendous expansion of Internet infrastructure over the past two



May 2013 workshop to facilitate discussions on work carried out in area of cyber security under Action Line C5 (ITU/Claudio Montesano Casillas)

decades. Therefore, the United States must prioritize the most critical facilities or systems that comprise the backbone of our societal functions. EO 13636 required DHS to provide the initial prioritization of those critical infrastructure facilities at greatest risk to cyber attack by July 2013. The prioritization uses a risk-based approach to examine how a cybersecurity incident could reasonably result in a catastrophic regional or national effect on public health or safety, economic security, or national security. Heads of Sector Specific Agencies (SSAs) must be involved in the process and facilitate information exchange and recommendations from the private sector.

Regarding information-sharing, the executive order takes a two-pronged approach in improving accessibility of cyber threat information to critical infrastructure owners and operators. One approach is deliberately producing unclassified reports to the greatest extent possible. The second calls for granting security clearances and classified access to accommodate instances in which a report cannot be declassified but the information is crucial to the defense of critical infrastructure. While this task addresses access, the matter of identifying what information is to be shared is a subtask of the Cyber Security Framework.

Also, as part of EO 13636, the National Institute for Standards and Technology (NIST) was tasked to implement its final version of a Cyber Security Framework by February 2014. The executive order defines the Cyber Security Framework as "a set of standards, methodologies, procedures, and processes that align policy, business, and technological approaches to address cyber risks."[16] The EO describes what the framework will provide as "a prioritized, flexible, repeatable, performance-based, and cost-effective approach, including information security measures and controls, to help owners and operators of critical infrastructure identify, assess, and manage cyber risk."[17] In military terms, it might be considered a standard operating procedure, a guide against which critical infrastructure companies measure themselves to ensure they instituted the most sensible and secure measures to protect their networked systems from cyber attack.

The Information Technology Laboratory, a branch under NIST, has undertaken the Cyber Security Framework project. The laboratory has "the broad mission to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology through research and development in information technology, mathematics, and statistics."[18] In the Cyber Security Framework, the laboratory now has an immensely challenging task that will entail interfacing with many entities, both public and private.

Similarly, PPD-21 directs a set of tasks that support the NSSC and requires agencies across the government, as well as industry, to provide input towards a potential solution.[19] The directive reinforces the 2003 strategy, which suggests that in order to secure U.S. interests in cyberspace, we must ensure that our networks are both protected and resilient. More specifically, it complements the edicts issued in EO 13636 with additional directives seeking to define both the public and private sector cyber environments to establish better starting points for a national movement toward greater cybersecurity.[20] So while EO 13636 focuses on the critical tasks, PPD-21 focuses on the supporting tasks.

PPD-21 introduces three strategic imperatives that will support and enable the original objectives in the 2003 NSSC: refining and clarifying functional relationships across the Federal Government, enabling information exchange through establishing a baseline for data and system requirements, and information integration and analysis streamlined to inform planning and operational decisions.[21] These imperatives provide the foundation on which the specified tasks in both EO 13636 and PPD-21 can build.

Each task specified in PPD-21 requires DHS to take the lead either solely or in cooperation with SSAs.[22] The first task is to describe the functional relationships across government agencies. This is essentially a comprehensive "who does what" effort at the intersection of critical infrastructure and cyberspace. This may take the form of a basic point-of-contact list, which constitutes a starting point for coordination. The second task is to evaluate existing public-private information-sharing models and recommend what needs to be sustained or changed. The third task is identification of baseline data and system requirements that should serve as the minimum standard for cybersecurity. Fourth, by October 2013, DHS was to provide a demonstration of a near real-time situational awareness capability for critical infrastructure threats and vulnerability assessment. Fifth, DHS must produce a document that will supersede the *National Infrastructure Protection Plan* of 2009. The final requirement is a research and development plan specific to critical infrastructure security and resilience. This plan is due 2 years from the PPD date of publication.[23] DHS has already been working on many of these tasks as part of existing efforts. However, the PPD creates a temporal constraint to emphasize the urgency and necessity of the six tasks.

Remaining Gaps and Potential Legislative Solutions

EO 13636 and PPD-21 in many ways effectively focus on information exchange, along with the critical requirement for resolving the observed impediments and shortfalls and implementing the NSSC information-sharing intent. While these directives provide a workable way ahead in many areas, they are not without significant challenges.

Regarding the first impediment to information-sharing—exclusive focus on counterterrorism with some inattention to cybersecurity—the executive order and PPD represent a refreshing change of direction. These documents demonstrate a concerted effort on the part of the Obama administration to develop much-needed guidance and policy that are specific to all-threat cybersecurity. Of course, these executive branch directives cannot address legislative shortcomings in this regard.

Some bills are circulating through Congress, most notably H.R. 3523, the Cyber Intelligence and Sharing and Protection Act (CISPA). If passed, this act would reiterate many elements already included in EO 13636. Additionally, the bill has potential to address other shortfalls the executive order could not cover due to separation-of-powers issues.

Given current budgetary constraints, one potential element of legislation may be resourcing for EO 13636–related efforts. For example, the executive order directly tasks DHS with expediting security clearance processes, which the department should be able to resource within its current budget authority. However, the order does not provide the resources to extend classified data networks to the critical infrastructure owner and operator's facility or to provide physical security at the new classified material handling location. As Congress holds the "power of the purse," complementary legislation can support the executive order in this and other concerns.

For information-sharing between the IC and industry, the executive order largely addresses the flow in one direction—from the government to private industry. CISPA or other legislation would need to address the flow in the opposite direction. The legislation could potentially include legal standards for government personnel handling sensitive information that pertains to private industry's cyber-based intrusions. Legislators would also need to address liability concerns and further incentives for industry participation in the executive order's voluntary programs. For example, expansion of the Enhanced Cyber Security Services Program bolsters the public-private partnership; however, being a voluntary program means that private industry participation is uncertain at best. The Cyber Security Framework, in varying degrees, builds on NSSC priorities, but its success is also tied to voluntary participation. One of several deterrents to private industry participation may be companies' concern for business confidentiality. Without supporting legislation, EO 13636 lacks the resources to offer incentives to increase participation or—as a last resort—compel participation by law. The program must address the concerns of private industry one way or another to improve participation.

For the flow of information from the government to the private sector, overclassification will likely linger as an impediment to truly useful information exchange. EO 13636 directs the greatest possible development of unclassified reports of cyber threats that identify "a specific targeted entity."[24] This is a positive step toward improving the cybersecurity of U.S. critical infrastructure. Unfortunately, the overclassification of data feeding these reports could compromise the integrity of this goal.

To develop unclassified reports, U.S. agencies must strip out any information that suggests the presence of an intelligence source. Such data are routinely classified at the Top Secret, Secure Compartmented Information (SCI) level. The more SCI data there are in the original report, the less likely it is that a redacted report would be possible or useful. Thus, Congress must take action on the issue of overclassification of cybersecurity threat reporting. Legislators could address gratuitous classification through new acts such as CISPA or through cyber-specific modifications of existing legislation, particularly the Reducing Over-Classification Act.

Many will point out that too much information-sharing can prove catastrophic to national security. A commentary from the Central Intelligence Agency Center for the Study of Intelligence laments the nascent information-sharing paradigm and observes, "the newly enshrined emphasis on 'need to share' has swung the pendulum much too far in the opposite direction."[25] Certainly the 2010 WikiLeaks scandal is an example of vulnerabilities to sensitive information. U.S. Army Private First Class Bradley Manning allegedly provided over 260,000 diplomatic cables, over 90,000 intelligence reports, and one video to the WikiLeaks site, which is dedicated to transparency of government.[26] While most of the information was classified, none of the compromised information exceeded the Secret level, presumably because PFC Manning only had routine access to Secret-level networks. In this case, a downgrade of Top Secret information to Secret or lower could have subjected even more information to compromise on WikiLeaks.

While some may see WikiLeaks as a reason to increase security of sensitive information and reduce sharing, prudent policymaking will consider the dangers of such a potentially overreactive policy. While we must secure our classified information, national security as extended into cyberspace still depends on the flow of information among all parties who can contribute to our collective defense. Thus we must strike a balance between the need for information security and sharing. Accordingly, policymakers should view WikiLeaks as a reason for developing and refining policies, procedures, and constructs for monitoring and tracking information while ensuring its provision to those who may find it useful for their national security work.

Another effort to address classified information flow is to increase the number of private entities that have access to classified cyber threat information. The expansion of the Enhanced Cyber Security Services Program will enable this effort and include critical infrastructure companies and commercial services providers. In its current state, the program provides cyber threat information as well as mitigation standards and procedures to defense industrial base companies. To mitigate issues associated with classified information elsewhere in the private sector, the executive order calls for expediting the security clearance process of "appropriate personnel employed by the critical infrastructure owners and operators."[27] While EO 13636 makes significant strides in bolstering the government–private industry partnership through these efforts, the effectiveness of the order remains uncertain without legislation in support of the policy.

Concerning the fourth and final impediment to public-private information-sharing, the executive branch used its executive order and PPD to clearly reaffirm DHS as the lead for cybersecurity. This is an appropriate measure toward avoiding concerns about "militarization" of cyberspace. That said, NSA has tremendous expertise in cyberspace situational awareness. Additionally, the Defense Department's unique legislative authorities to conduct offensive actions make it *the* key entity in some responses to external attacks on U.S. critical infrastructure. The executive and legislative branches may therefore need to consider additional measures to facilitate the collaboration among all key entities with a stake in U.S. cybersecurity.

Since the release of the 2003 *National Strategy to Secure Cyberspace*, government efforts to attain prescribed intragovernmental and public-private information-sharing have proved fractured and incomplete. Issues have ranged from a lack of concerted focus on cybersecurity in both the executive and legislative branches, to a lack of information-sharing to and from the Intelligence Community, to a systemic tendency to overclassify cyber threat reporting information, to distracting considerations to center the lead for cybersecurity within the military. The Obama administration's Executive Order 13636 and Presidential Policy Directive 21 made positive steps toward rectifying many shortcomings. However, these actions represent only a part of the solution. Congress now must act to provide complementary cybersecurity legislation to fill gaps in the public-private information-sharing construct prescribed in the 2003 strategy. Only then will the United States be fully on the path to a whole-of-nation approach to meet the full scope of cyber threats. **JFQ**

Notes

[1] Michael Mimoso, "Bank DDoS [distributed denial-of-service] Attacks Using Compromised Web Servers as Bots," *Threatpost.com*, January 11, 2013, available at <http://threatpost.com/bank-ddos-attacks-using-compromised-web-servers-bots-011113/77393>; Mimoso, "'Historic' DDOS Attacks Against Major U.S. Banks Continue," *Threatpost.com*, September 27, 2012, available at <http://threatpost.com/historic-ddos-attacks-against-major-us-banks-continue-092712/77055>.

[2] Mimoso, "Bank DDoS Attacks."

[3] Department of Homeland Security (DHS), *National Strategy to Secure Cyberspace* (Washington, DC: DHS, February 2003), x.

[4] Ibid., 11.

[5] Ibid., iv.

[6] Zoë Baird Budinger and Jeffrey H. Smith, Statement Before the Senate Committee on Homeland Security and Governmental Affairs, *Ten Years After 9/11: A Status Report On Information Sharing*, October 12, 2011, available at <www.hsgac.senate.gov>.

[7] National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States* (Washington, DC: U.S. Government Printing Office, July 22, 2004), 417.

[8] Reducing Over-Classification Act, Public Law 111-258, U.S. Statutes at Large 124 (2010), 2648.

[9] Ibid.

[10] Patricia A. Brannin, memorandum to Secretaries of the Military Departments et al., October 26, 2011, available at <www.fas.org/sgp/othergov/dod/ig-overclass-2011.pdf>.

[11] Dennis C. Blair, Director of National Intelligence, Statement Before the House Permanent Select Committee on Intelligence, Annual Threat Assessment, February 25, 2009.

[12] Ibid.

[13] Steven Aftergood, "What's the Difference Between an Executive Order and a Directive?" *Secrecy News*, February 14, 2013, available at <www.fas.org/blog/secrecy/2013/02/eo_pd.html>.

[14] Ibid.

[15] Executive Order 13636, *Improving Critical Infrastructure Cybersecurity*, February 12, 2013, available at <www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity>.

[16] Ibid.

[17] Ibid.

[18] Information Technology Laboratory, "National Institute of Standards and Technology," available at <www.nist.gov/itl/what-itl-does.cfm>.

[19] Presidential Policy Directive 21, *Critical Infrastructure Security and Resilience*, February 12, 2013, available at <www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil>.

[20] Executive Order 13636.

[21] Presidential Policy Directive 21.

[22] Ibid.

[23] Ibid.

[24] Executive Order 13636.

[25] Bowman H. Miller, "The Death of Secrecy: Need to Know . . . with Whom to Share," *Studies in Intelligence* 55, no. 3 (Center for the Study of Intelligence November 9, 2011).

[26] "Bradley Manning," *The New York Times*, January 9, 2013, available at <http://topics.nytimes.com/top/reference/timestopics/people/m/bradley_e_manning/index.html>.

[27] Executive Order 13636.

(Photo by Tara J. Parekh)

"Break Out"

A Plan for Better Equipping the Nation's Future Strategic Leaders

By Gregg F. Martin and John W. Yaeger

Reforming joint professional military education (JPME) has been much discussed and debated in recent years. At the National Defense University (NDU), the time for meaningful change has come. The University is moving out on reform. In this article, we explain the reforms and why they are necessary, and how they will be implemented. We believe they constitute an effective strategy for better educating future leaders for the Nation within a new fiscal reality.

We want supporters and future students to understand and appreciate the strategy, so they can effectively participate in its successful implementation.

Our "breakout" strategy comes in response to guidance from General Martin Dempsey, the Chairman of the Joint Chiefs of Staff (CJCS), and a 1996 graduate of NDU. A firm believer in the critical importance of JPME, the Chairman directed the University to update its curriculum, and among other things, to incorporate desired attributes for future leaders and lessons from the past 13 years of war. In October 2011, he encouraged NDU to begin reform. In February 2012, he personally rewrote the University's mission statement. On July 11, 2012,

Major General Gregg F. Martin, USA, Ph.D., is the President of the National Defense University (NDU). Dr. John W. Yaeger is the Provost of NDU.

he spoke at the University, clarifying his intent that NDU should break out from its current way of doing business to better support our joint warfighters and the Nation. The Chairman's emphasis on change evokes the words of President Abraham Lincoln inscribed on the walls of Lincoln Hall here at NDU: "As our case is new, so we must think anew, and act anew."

In this vein, General Dempsey cited changes at NDU as a first step toward broader reform: "As we continue to advance '[whole of] University' initiatives at National Defense University, we will update the Joint PME curriculum across the force to emphasize key leader attributes. We will also explore how best to adapt our learning institutions to serve a global Joint Force."[1]

Over the past 2 years, NDU has absorbed significant funding and personnel cuts, like our partner institutions across the Department of Defense. During the same period we have prepared broad strategic guidance to our component institutions, executed an "NDU 2020" planning process, participated in the Chairman's Joint Education Review, and moved through a series of scheduled external review and accreditation events. Now, in time for the upcoming 2015 academic year, we are implementing the Chairman's guidance and seizing the opportunity to prepare our future strategic leaders with a program that is more focused on individual learning outcomes and better postured to leverage the full range of talent available to the University. By collaborating more effectively across the University's different colleges and components, we can deliver improved joint education at less cost to the Nation. In more detail, here are why and how we will do it.

Why Change?

Change is hard and some always question whether it is necessary. Skepticism is understandable. Real change that elevates an organization's performance is rare. Many change efforts are ill conceived and mostly cosmetic: shuffling organizational boxes, titles, and authorities without effectively identifying, understanding, and addressing the key impediments to better performance. Any critical problem-solving effort must be based on an accurate diagnosis of the problem to be solved.[2] Even well-conceived efforts often fail due to bureaucratic resistance or for lack of adequate follow-through. Those that do succeed often must pass through a brief period of relative inefficiency before they carry the organization to new heights of performance. Not surprisingly, many people associate organizational change with administrative turbulence that undermines rather than enhances performance. The change we support will be real, substantial, and effectual.

We began with a candid appraisal of our circumstances and key challenges. Stated simply, NDU must better equip future leaders for an increasingly complex and dynamic security environment during a period of severely reduced resources. Our five colleges enjoy strong reputations and offer many opportunities for an excellent education, but a number of scholarly critiques in recent years point out that we can do better.[3] Although views differ, several criticisms are recurring, most notably that our academic standards are not sufficiently rigorous, our curricula can be more current and innovative, our education does not leverage student's prior training and operational experience, and our research centers can be better linked to our students.

Changing National Security Environment. The environment today is not unlike the mid-1970s when the decision was made to consolidate the National War College and the Industrial College of the Armed Forces (now the Dwight D. Eisenhower School for National Security and Resource Strategy) under the National Defense University. The Nation was coming out of a prolonged conflict and facing diminishing resources.

Rigor. Some believe that NDU should accommodate student welfare at the expense of necessary academic rigor. Even though the University maintains its academic regional accreditation, critics note that some of our graduate programs do not typically require a thesis and that our course credits may not transfer to other top academic programs. The need for war-weary and battle-hardened veterans to recuperate and reconnect with their families is genuine and we support it, but we must try to balance quality of life for our returning heroes with an academically rigorous program.

Relevance. Another common critique is that our curriculum is focused on the past at the expense of the emerging future, on military history and the immutable principles of war, and not enough on critical thinking skills relevant to current issues:

> *The current approach to the professional military education and growth of senior officers may not adequately prepare them to meet those coming challenges. . . .* [O]*ther than some adjustments to accommodate counterinsurgency doctrine, the professional military education provided by military institutions in the past decade has largely remained constant in spite of rapid changes in the world.*[4]

In addition, it is often asserted that our JPME institutions, once a major source of innovative educational methods, have "become an intellectual backwater, lagging far behind the corporate and civilian institutions of higher learning."[5]

These concerns are easily overstated, but they have some merit. Certainly we acknowledge the need to focus more on imparting leadership attributes demanded by a security environment that is "characterized by uncertainty, complexity, rapid change, and persistent conflict."[6] In such an environment, leaders require multidisciplinary and adaptive problem-solving skills that prepare them to collaborate and innovate. Most of our students now have experience in joint, interagency, and multinational operations, and some of our best young leaders in recent campaigns demonstrated a willingness to experiment to good effect. We need to make sure that our curriculum captures and transmits their successes in ways that illuminate general principles for effective decisionmaking in similarly complex environments.

Disconnected Research. Another concern raised about the management of the University was its expanding research centers. The good news is that many national security organizations (or "customers") believe that NDU research is a good value. They vote with their dollars, so to speak, and over the past decade spent increasing amounts to fund NDU research. Unfortunately, our students did not receive the full value of NDU's impressive research capacity. The ability of students to tap into this wider body of expertise at the University was limited.

Adapting our educational approach and programs to produce better leaders would be controversial in the best of circumstances. It is even more so in a period of fiscal austerity. The overall resources available to NDU have declined by more than 20 percent in the last several years, from $103 million to a projected $80 million for the 2015 fiscal year. Across the University, programs have been canceled and faculty and support staff positions have been eliminated or gone unfilled. In these circumstances, "business as usual" must give way to a new paradigm. The key is to make sure our strategy for change clearly identifies how to produce better-equipped, critical problem-solving leaders while conserving resources.

What Change?

If we hope to generate better educational output at lower costs per student, it is clear we will have to evolve and adapt. In the coming academic year, we will implement six major innovations to break out from our current educational model.[7] These changes constitute the core of our strategy for better equipping future leaders.

Student Assessments, Tailored Programs, and Learning Contracts. Prior to or soon after arriving at NDU, students will review their careers to date with faculty mentors. Based on previous experiences, interests, and career needs, students and mentors will build a tailored academic program grounded in a core curriculum and enriched by electives and research—not by a predetermined, one-size-fits-all requirement. Faculty mentors will not only explain the core curriculum offered by the University but also work with students to identify topics of particular interest and ways to integrate these into the students' educational experiences. A clear lesson from adult education research is that mid-career professionals must be self-motivated to learn and that they are best motivated when they understand and can participate in structuring their learning experiences. The decisions made by mentors and students will be codified in a learning contract that will be reviewed periodically and at the end of the academic year.

Chairman addresses audience at National Defense University as it welcomes Major General Gregg Martin as its 14th president during assumption of command ceremony, July 11, 2012 (DOD/Tyrone C. Marshall, Jr.)

First Phase: Foundational Expertise. The first phase will consist of a single University-wide core curriculum. These courses will cover foundational material that must be mastered by all serious students of national security. The material will be taught by the most talented subject matter experts we have at the University—whether they currently are assigned teaching, research, or administrative duties—in order to give students the best possible educational experience. The material will meet many of our statutory JPME requirements and introduce the Chairman's Desired Leader Attributes, including gender perspectives, ethics, the Profession of Arms, and lessons from the past decade of war. During this first phase, students will pair with fellow students from other departments, agencies, and other countries to expand their understanding of alternative views and cultures, and they will exploit our Washington, DC, location for first-hand observation of diverse elements of the national security system.

Second Phase: Specialized Expertise. The second phase will deliver the core curricula of our five colleges. Freed from the responsibility to cover basic material, the colleges will focus on their unique and distinguishing competencies. The College of International Security Affairs will focus on international partnering and irregular threats; the Eisenhower School will focus on resource management and organizational performance; the Information Resources Management College (*i*College) will focus on the cyber domain; the Joint Forces Staff College, our southern campus located in Norfolk, Virginia, will focus on joint campaign planning; and the National War College will offer its focus on U.S. national security strategy.

The objective is to benefit students by strengthening the ability of each college to offer deeper expertise in its area of distinctive competence.

Third Phase: Personalized Strategic Leader Development. The third phase is tailored to individual leader development and will focus on electives. All students will complete a Capstone research project or thesis. This final phase of the academic year challenges students to demonstrate what they have learned in the previous two phases by solving a practical problem

National War College faculty members with seminar students (NDU/Katherine Lewis)

in an area of their choosing relevant to their career goals. Depending on the student learning plan constructed at the beginning of the year and knowledge of their next assignment, electives can directly support the research project or assist the student with broader career goals.

Program Evaluations and Ongoing Study Guidance. Throughout the academic year, a concerted effort will be made to improve the way we gather insights from students about their educational experiences. They will provide feedback on all aspects of the educational program. Along with other national security stakeholder feedback, these assessments will be used to adjust the program for better performance. Students will also be encouraged to conduct a self-evaluation of how well they fulfilled their educational contract. An objective of this phase is to provide guidance to graduates for lifelong learning. Their NDU experience should continue after graduation. If there are learning areas or topics that students would like to pursue, relevant faculty will provide additional instructional material and suggested readings before the students depart for their follow-on assignment so they can continue the learning process. We consider this final phase of the academic year an important innovation both for its potential impact on students and for the University.

Our five colleges have benefited from each of their student assessments, but organizations that are asked to evaluate their own performance tend to be biased in a positive direction. Centralizing, collating, and analyzing assessment results in the Office of the Provost will enable the University to identify areas for improvement and work together on whole-of-NDU solutions.

Common Academic Calendar. The final innovation is a backbone initiative that will reinforce the value of the preceding five changes. Too often in the past, students, faculty and staff were not able to take advantage of the many University events relevant to their educational goals because their schedules would not permit participation. Conferences, workshops, distinguished guest speakers, and partnering with research faculty were hampered by rigid schedules that allowed students little free time while on campus. Some common scheduling rules will allow all elements of the University to schedule activities that might interest students in time slots when they will be free to participate. For example, if lunch periods and time slots for guest lectures are common across all the colleges, NDU components could target these periods for workshops and other events open to student and faculty participation. Alternatively, students could use these portions of their schedules to meet with faculty to discuss their theses or other topics of mutual interest.

What Are the Benefits?

A few common themes provide the foundation for these changes. Talent from across the University will be marshalled in support of student learning as the first priority irrespective of whether a person's primary job description is focused on research, outreach, or administration. There are many highly qualified faculty members and experts in our regional centers, campus administration, research centers, and diverse colleges who previously were not available to students—even if the student was intensely interested in their areas of expertise. Under the new program students will be better able to tap the University's full range of expertise—and our commitment to place our students at the center of all we do will be more fully realized.

Greater collaboration across University components is a corollary requirement for our student-centric program. The changes we are implementing are interrelated and mutually dependent, as would be expected in a coherent organizational strategy for change. For maximum effect they must be administered together. They require a whole-of-NDU approach to educating our students. Doing a better job with fewer resources often means organizations must cooperate more across interfaces or stovepipes. This is true for jointness in military operations, for interagency cooperation in the broader national security system, and for educational reform at the National Defense University. Thus, we are modeling for our students the collaborative path they will need to apply later in their careers.

More specifically, we expect the following benefits from these integrated changes:

- The third-phase focus on demonstrated problem-solving under direct faculty mentorship, which builds on critical thinking skills imparted in the first two phases, will help equip future leaders to operate in a complex and dynamic security environment.
- The first and third phases will draw upon the best talent from across NDU to ensure students receive the best that the University has to offer in each subject area, including individual student research.
- Freeing colleges from the burden of teaching common foundational material will allow them to hire and

focus their faculties on their areas of comparative expertise, which will be more efficient and make deeper expertise available to students.

- The student-centric nature of the integrated program, which stresses attention to student needs, interests, and learning objectives, will increase motivation for learning.
- Working within a common academic calendar so that teaching, research, and outreach are mutually supportive will expand student opportunities to learn and get the best from the entire range of activities sponsored by the University.
- The emphasis on clinical, empirical assessments of students, faculty, and programs will enable ongoing improvement not only for programs and faculty but also for the students so they will continue the learning process after departing the University.

What Are the Savings?

One question frequently raised as we have debated these changes internally is whether they really can be enacted within our current resource constraints. Put differently, how will these changes save resources? Most of the cuts to our programs have already been absorbed, albeit at the cost of vacating or not filling a large number of positions. Thus, we do not have to implement this program while making additional large cuts. That said, we believe this program is feasible because it conserves resources in several ways.

First, we are *reordering priorities* to focus on students. For example, the research centers will give priority to supporting teaching and student research rather than making research for its own sake the principal goal. Our research centers have always made responsiveness to the Pentagon a priority, and they will continue to focus on applied research. However, their first priority will be students. Similarly, outreach in support of external requirements (for example, hosting visitors and providing a venue for conferences and other activities) will be a lesser priority except where it manifestly benefits the educational experience of our students. By reordering priorities, we are increasing productivity by tapping the full range of NDU expertise for students, which gives us a bigger educational bang for the buck.

Second, we are *increasing our ability to pool and share* our talented faculty across NDU. We will still graduate the same number of students, but we will no longer teach all foundational material with separate faculty at each of our five colleges. A common academic calendar, for example, creates opportunities to leverage expertise found in one component in other arenas. In recent years, we have already begun moving in this direction. For example, the National War College realized its students needed more exposure to economic issues. It cooperated with the Eisenhower School to obtain the faculty support for economics since Eisenhower has long maintained such expertise.

The Way Ahead

At the National Defense University, we are committed to implementing the Chairman's guidance with an integrated strategy that relies on the whole of NDU and places students at the center of all we do. Our students are experienced professionals; they quickly recognize gaps between theory and practice and the inconsistencies between what they are taught and how NDU operates. If we emphasize the importance of the Chairman's Desired Leader Attributes, which include "the ability to anticipate and recognize change and lead transitions," but decline to lead change at NDU because it is difficult or risky, the students will know. If we teach the essential elements of strategy but our strategy for organizational change does not include those elements, the students will know. If we insist our strategy is student-centric and relies on a whole-of-NDU approach, but we do not offer students the best the University has to give, the students will know. We will not disappoint them. We will deliver the changes we have promised.

Change of this magnitude requires a total team effort for implementation. Many supporting actions remain to be completed if we are to present students with a significantly enhanced educational experience when they arrive on campus to begin academic year 2015. We acknowledge and welcome the participation, inputs, and suggestions from our stellar faculty—and from our friends and supporters as we prepare for a bright future. Indeed, the entire University, and all those who support it, must make these reforms a priority and participate in their implementation if we are to succeed. This includes our incoming students, who we hope will be encouraged to participate more fully in the change process after reading this article. At a minimum, they will now understand why we are moving out on educational reform and that we intend to practice what we teach. **JFQ**

Notes

[1] Martin E. Dempsey, *18th Chairman's 2nd Term Strategic Direction to the Joint Force* (Washington, DC: The Joint Staff, 2014), available at <www.jcs.mil/content/files/2014-01/011714102354_CJCS_2nd_Term_Strategic_Direction.pdf>.

[2] A key requirement for any good strategy is a penetrating diagnosis of the root cause of the problem or challenge that must be overcome. See Richard P. Rumelt, *Good Strategy, Bad Strategy: The Difference and Why It Matters* (New York: Crown Business, 2011).

[3] Some noteworthy critics include Robert H. Scales, "Too Busy to Learn," U.S. Naval Institute *Proceedings* 136, no. 2 (2010); Patrick M. Cronin, "PME: A Strategic Education," *Marine Corps Gazette* 94, no. 6 (2010); George E. Reed, "What's Wrong and What's Right with the War Colleges," *DefensePolicy.org*, July 1, 2011, available at <www.defensepolicy.org/george-reed/what%E2%80%99s-wrong-and-right-with-the-war-colleges>; Kevin P. Kelley and Joan Johnson-Freese, "Getting to the Goal in Professional Military Education," *Orbis* 58, no. 1 (2014), 119–131; and David Barno et al., *Building Better Generals* (Washington, DC: Center for a New American Security, October 2013).

[4] Barno et al., 17.

[5] Scales.

[6] Joint Publication 1, *Doctrine for the Armed Forces of the United States* (Washington, DC: The Joint Staff, March 25, 2013), I-10.

[7] In doing so we intend to emphasize elements from several common adult learning theories. See Sharan B. Merriam and Rosemary S. Caffarella, *Learning in Adulthood: A Comprehensive Guide* (San Francisco: Jossey-Bass Publishers, 1999).

Airman prepares to fuel A-10C Thunderbolt II with 50/50 blend of Hydrotreated Renewable Jet and JP-8; plane then flew first flight of aircraft powered solely by biomass-derived jet fuel blend (U.S. Air Force/Samuel King, Jr.)

Green Peace
Can Biofuels Accelerate Energy Security?

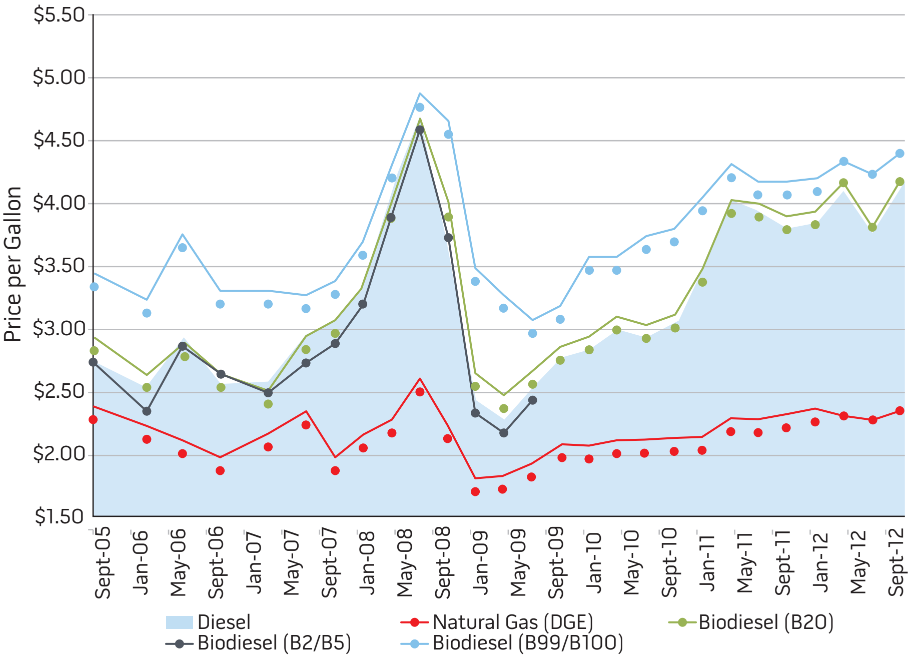
By John E. Gay

The evolution of liquid fuel for transportation has a long history of innovation that began with the steam engine. Initially, wood and coal were the primary fuel sources for propelling various vehicles both on land and at sea, but transferring them was dirty and strenuous and required extensive manpower. The discovery of liquid petroleum and the development of refinery processes quickly shifted transportation energy from coal and wood to liquid fuels. Petroleum offered double the thermal energy of coal and as a result boiler designs became smaller, enabling automobiles, ships, and railway locomotives to travel faster and farther. The transfer of liquid petroleum through pipes greatly reduced refueling labor and provided greater distribution options. As a result, petroleum quickly became the fuel of choice, initiated a global oil boom, and created competing interests among nations.

Today, global economies as well as national security interests depend on domestic and imported oil. As that dependency grows, the fundamental stability of the global oil market is being stressed by inadequate investment in oil production capacity, persistent geopolitical instability, and rapidly growing demand in developing nations.[1] In addition, reliance on a single energy source for transportation fuel—petroleum—has economic, strategic, and environmental drawbacks. In response to these challenges, and controversially using Cold War authorities of the Defense

Commander John E. Gay, USN, is Deputy Public Affairs Officer of United States Fleet Forces Command.

Figure 1. Alternative Fuel Prices vs. Diesel



Source: Department of Energy, "Cities Alternative Fuel Price Report," July 2012, 15.

Production Act, a memorandum of understanding was signed between the Secretaries of Agriculture, Energy, and the Navy to each invest $170 million to jumpstart a biofuels industry and help lead the United States to energy independence.[2]

The 2007 National Defense Authorization Act set an aggressive goal for the military to produce or procure 25 percent of all its energy demands from renewable sources by 2025.[3]

Section 2852 of the 2007 National Defense Authorization Act calls for the Department of Defense (DOD) to establish goals regarding use of renewable energy to meet transportation needs:

> *The Secretary of Defense shall submit to the congressional defense committees the energy performance goals for the Department of Defense regarding transportation systems, support systems, utilities, and infrastructure and facilities . . . (c) Special considerations—For the purpose of developing and implementing the energy performance goals and energy performance plan, the Secretary of Defense shall consider at a minimum the following . . . (4) Opportunities to pursue alternative energy initiatives, including the use of alternative fuels in military vehicles and equipment, (5) Cost effectiveness, cost savings, and net present value of alternatives . . . and (8) the value of the use of renewable energy sources.*[4]

In compliance with the law, the U.S. Army, Navy, Marine Corps, and Air Force have all expressed an interest in being early users of alternative fuels, although Congress did not require the use of alternative fuels in military tactical weapon systems. The Air Force played a lead role in evaluating and testing alternative fuels for military applications and set a goal to be prepared to acquire cost-competitive alternative fuel blends sufficient to meet 50 percent of its domestic aviation fuel requirements by 2016. Moving well beyond compliance with the will of Congress, Secretary of the Navy Ray Mabus established an aggressive energy strategy focused on replacing 50 percent of the Navy's energy consumption with biofuels by 2020.[5] The Army is evaluating the performance of alternative fuels in combat systems but has not yet formally established goals.[6]

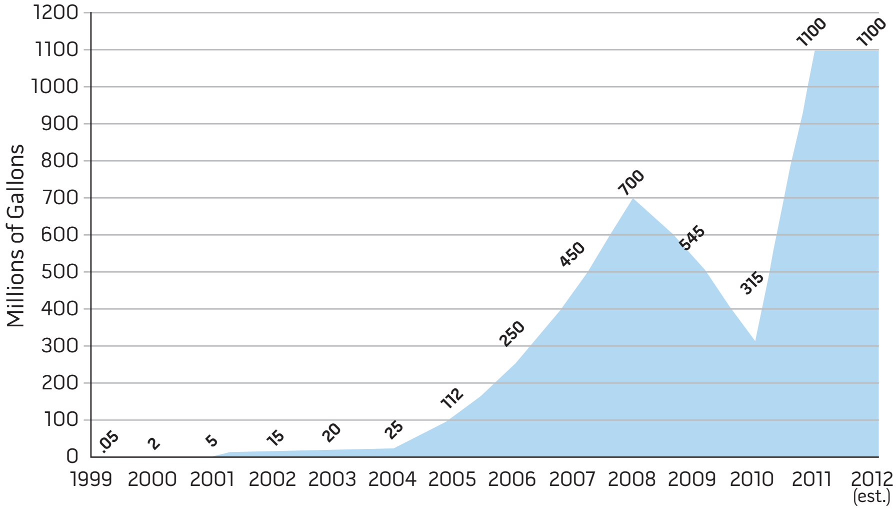
Can military research and investment jumpstart a biofuels industry and provide an alternative to imported foreign oil that is compatible, readily available, and affordable? This article explores the military application and feasibility of biofuels and offers reasons why biofuels will not lead the Nation to improved energy security.

Biofuels Defined

Biofuels are liquid fuels produced from agricultural or other biological materials, and such fuels have been around for more than 125 years. Some of the first automobiles and tractors were capable of running on biofuel, and the first commercial cellulosic ethanol plant opened in the United States in 1910. Biofuels production declined over time because it was expensive, inefficient, and ultimately unsustainable.[7] Corn-based ethanol reappeared in the 1970s after the oil embargo as a way for the United States to reduce its dependency on imported oil from the Middle East, and it attracted interest again in the 1990s as a renewable fuel to help reduce greenhouse gas emissions.[8] Today the most widely used biofuel, ethanol, is produced from the fermentation and distillation of sugar or starch-based crops such as sugar cane and corn. Biofuels also include biodiesel—mono-alkyl esters of long-chain fatty acids derived from vegetable oils and animal fats.[9] Biodiesel is renewable heating oil and a diesel substitute used in Europe, and it is gaining interest in the commercial market in the United States. Common feedstock for biodiesel fuels includes soybeans, rapeseed, canola, palm, other plants, and waste cooking oils and animal fats.[10]

Untreated bio-oil made from thermal processing of tree and plant cellulose is a complex mixture of oxygenated organic compounds with about 25 percent water that is difficult to separate. Bio-oil is not compatible with conventional fuel systems and engines and is unstable in long-term storage. [11] However, it can be stabilized and converted to a conventional hydrocarbon fuel by a complex sequence called hydrotreating.[12] Once hydrotreated, biodiesel is compatible with petroleum-based fuels and miscible in many different concentrations offering "drop-in" advantages without

Figure 2. U.S. Biodiesel Production



Source: National Biodiesel Board Annual Estimates

diesel motor modification. However, hydrotreatment is costly in energy, and some scientists doubt that there is a net energy gain in biofuels because more than 50 percent of the energy stored in feedstock plants comes from fossil fuels in the form of nitrogen fertilizers and pesticides; energy for tilling, harvesting, and transport; and the chemical conversion process.[13] Because a significant amount of fossil fuel is required in the life-cycle production of biofuels, the cost of processing biomass into ethanol or biodiesel is directly linked to the cost of fossil fuels. When the price of oil increases, so do the feedstock and production costs of biofuels. Biofuels and associated renewable energy credits are also part of the global energy trading market, and the biofuels price trends in the same direction as fossil fuels, as observed in figure 1. As a result, it is unlikely that the costs of biofuels will ever become more competitive than fossil fuels.[14]

Biofuels do not offer the same energy density as petroleum-based fuels. Ethanol contains 33 percent less energy per gallon than gasoline and biodiesels contain about 8 percent less energy than petroleum-based diesel fuels.[15] Lower energy density has a direct negative effect on battlefield energy security. That means operational vehicles using biofuels will travel less distance per tank of fuel, thus requiring more fuel to accomplish the same mission. This results in additional logistics requirements in the form of more fuel that will have to be delivered to the troops.

Energy Security

Energy security is having assured access to reliable supplies and the ability to protect and deliver sufficient energy to meet essential requirements.[16] Improving U.S. energy security is principally about reducing excessive costs to consumers resulting from disruptions in the oil supply. It also means having a robust supply portfolio.

In a 2011 speech on America's energy security delivered at Georgetown University, President Barack Obama echoed the conventional wisdom of biofuels:

> *The United States of America cannot afford to bet our long-term prosperity, our long-term security on a resource that will eventually run out, and even before it runs out will get more and more expensive to extract from the ground. We cannot afford it when the costs to our economy, our country, and our planet are so high, not when your generation needs us to get this right. It is time to do what we can to secure our energy future.*[17]

The transportation sector of the U.S. economy almost exclusively relies on petroleum converted by refineries to gasoline, diesel fuel, and jet fuel. That makes America most vulnerable to disruptions in the oil supply. The United States consumed more than 250 billion gallons of refined petroleum in 2011. Some 61 percent of its crude is imported, with 12.7 percent coming from the Persian Gulf.[18] In 2001 DOD consumed 5.2 billion gallons of refined petroleum products domestically and another 4.05 billion gallons overseas, or about 3.6 percent of the U.S. total of refined petroleum consumed.

Global economic growth has generated rapid increases in energy demand worldwide. Crude oil prices jumped from $60 a barrel in mid-2005 to a spike of $140 a barrel in mid-2008. More recently, from July 2011 to July 2012, the price of light crude fluctuated from under $80 a barrel to just over $110.[19] Steady petroleum price increases have supported the government's justification for investing in biofuels development.[20] As a result, the volume of biodiesel produced in the United States has steadily increased over the past 10 years, as observed in figure 2, but this is still only a very small fraction of the 202.7 billion gallons of petroleum consumed in the transportation sector in 2011.[21]

Despite the rising costs of crude, there is little hope that biofuels prices will ever be lower than the cost of petroleum. Even after the billions in government subsidies, the current price of corn ethanol is $.40 a gallon higher than regular gasoline for the same amount of energy in the gas tank.[22] Biodiesel prices range significantly higher. In 2009 the Defense Logistics Agency awarded small contracts for hydrotreated renewable HRJ-5 jet fuel that ranged from $66 to $149 per gallon.[23] Over the past few years, the Air Force and Navy have staged several aircraft and ship demonstrations using compatible drop-in biodiesel and bio–jet fuel as a tactical fuel. In 2011 the Navy spent $12 million for 450,000 gallons of hydrotreated renewable jet fuel and diesel oil made from chicken fat and algae to support an exercise in the Pacific Ocean. The biodiesel used by the Navy cost $26.75 per gallon, nearly 10 times the costs of petroleum-based diesel fuel. That same $12 million biofuels purchase could have paid for more than three million gallons of conventional diesel fuel, or the money could have gone to other critical military programs.[24]

In Afghanistan, fuel reaches the front lines via rail, trucks, and in some cases aircraft from Turkmenistan or Tajikistan. By some estimates 70 percent of the convoys in the theater of war involve "liquid logistics"—the delivery of fuel and water. By the time fuel reaches forward deployed troops, the fully burdened cost—the commodity fuel price plus the total cost of personnel and assets required to move and protect the fuel from the point it is received from the commercial supplier to the point of use—was estimated by the Marine Corps to range $9–$16 per gallon if delivered by land and $29–$31 per gallon if delivered by air. In early 2009 Ashton Carter, Under Secretary of Defense for Acquisition, Technology, and Logistics (AT&L), testified to Congress that protecting fuel convoys imposes a huge burden on combat forces and that by reducing fuel demand the Services could reduce logistics assets and operating costs and mitigate budget effects caused by fuel price volatility.[25] In addition, fuel convoys increase casualty risks for Servicemembers from enemy attacks, improvised explosive devices (IEDs), bad weather, and traffic accidents. According to the Center for Army Lessons Learned, there was one casualty for every 24 fuel convoys in Afghanistan and one for every 38.5 in Iraq.[26] Fuel convoys are extremely vulnerable to IEDs and are responsible for a large percentage of combat-related fatalities. Between July 2003 and May 2009, IEDs alone accounted for some 43 percent of U.S. fatalities in Iraq and 39.7 percent in Afghanistan.[27]

Liquid fuels, whether they are petroleum-based or biofuels, have to be transported on the battlefield at the same cost and risks to our Servicemembers. For this reason, the use of biodiesel does not offer a tactical advantage for enhancing energy security and may increase the risks and number of casualties due to its reduced energy density, which will require more fuel to accomplish the same mission.

In a 2011 report, the Federally funded RAND National Defense Research Institute concluded that there is no direct benefit to the Department of Defense for using alternative fuels rather than petroleum-derived fuels.[28] Biofuels do not offer a tactical military advantage, and unless their price becomes more competitive and the biofuels industry can scale up production, there is little chance the United States will significantly reduce its demand for petroleum-based fuels in the near future. The challenge of biofuels is production, not combustion.

Biofuels and Natural Resources

One of the biggest downsides to increasing production is that all biofuels compete with food agriculture for land, water, agrichemicals, and other farming resources. About 40 percent of the corn grown in America today is used to produce ethanol as a gasoline additive, and food crops such as soybean, rapeseed, and palm are used to produce biodiesels. The large percentage of farmland used to grow corn for ethanol has only replaced 6.5 percent of America's gasoline energy. The ethanol industry expanded based partly on expectations that gasoline consumption would keep rising and that ethanol's share of that growth would continue. Instead, gasoline demand for 2013 is projected to be 6.7 percent below its peak in 2007.[29] Agricultural markets are also volatile in price. When droughts, floods, or freezes affect crop production, food costs and biofuel prices climb together, which is particularly damaging to an economy.[30] For example, the 2012 U.S. Midwest drought forced many ethanol bio-refinery plants to close and demonstrates the insecurity of a biomass fuel supply and the effects on energy security.

Land. Today all biofuels produced in the United States and European Union (EU) are consumed domestically, but current production capacities in both regions are a long way from meeting their own future targets without importing biomass feedstock. The demand for biomass is growing at a time of massive competition for other land use including commercial forestry, food agriculture, industrial agriculture for textiles and chemicals, biomass for electrical power generation, and the expansion of urban areas.[31]

Available land to meet future biofuel demands is unevenly divided across the world. North Africa, South Asia, and Japan have very little arable land left for expansion, and almost half of the world's potentially available arable land is situated in only seven countries: Angola, Argentina, Bolivia, Brazil, Colombia, Democratic Republic of the Congo, and Sudan.[32] Also competing with the United States and European Union for land expansion are China, India, Japan, and South Korea. These nations continue to struggle to find additional agricultural land and are leasing land in other nations as well as trying to reclaim wasteland and saline land internally.[33]

One of the largest competing uses of land for biofuels production will be the food crops needed to feed a growing world population. The grain it takes to fill a sport utility vehicle tank with ethanol could feed one person for a year.[34] This is a major concern considering that according to the United Nations, the world's population is expected to increase from 7 billion in 2011 to 9.3 billion by 2050.[35] One estimate predicts that by 2020 an extra 200 to 500 million hectares of land will be needed for food, animal feed, and pasture to meet the nutritional needs of the global population.[36]

According to Nobel Laureate Michel Hartmut, the growth of plants for biofuels will undoubtedly lead to higher food prices, which will predominantly hit poorer people.[37] The global community has yet to address the key drivers of recent food prices, which have spiked three times in the last 5 years. Estimates suggest that the 2008 food crisis forced 100 million people into poverty and some believe biofuels were responsible for at least 30 percent of the global food price spike that year. ActionAid, an international nongovernmental organization, estimated at the time that 30 million more people went hungry as a direct result of biofuels.[38] Future estimates

Sailor presents samples of traditional F-76 diesel fuel and 50/50 biofuel blend to illustrate use of biofuels in support of Navy Secretary's goal to cut petroleum consumption in half by 2015 (U.S. Navy/Lolita Lewis)

suggest global food prices could rise by as much as 76 percent by 2020, pushing another 600 million into hunger if U.S. and EU biofuels goals are met and no other action is taken to prevent hunger.[39]

To meet the need for land, large-scale land acquisitions, frequently referred to as "land grabs," are taking place around the world. Land formerly used by independent farmers for their own subsistence is often confiscated by governments, with no respect for private land rights, and converted into plantations and crop monocultures. The agriculture products are exported to feed the energy and food demands of the industrialized world with little consideration for the local economies.[40] This practice creates escalating local food prices, food scarcity, and loss of job opportunities, forcing widespread displacement of populations.[41] Oxfam International, a confederation of 17 aid organizations operating in 90 countries, estimates that 567 million acres in the developing world have been sold, leased, licensed, or have been under negotiation to foreign corporations between 2000 and today.[42] According to the Renewable Fuels Agency, an estimated 500 million more hectares, roughly half the area of Europe, will be needed to meet the global biofuels demand by 2020. Land grabs are an example of how mandatory biofuels mandates are counterproductive to global security, to its supporting pillar of energy security, and to U.S. national security strategy.

Water. In addition to requiring more land, biofuels mandates add pressure to natural water resources. Large-scale industrial agriculture operations are often located in major river basins and consume massive amounts of water.[43] According to an Intelligence Community Assessment, numerous countries have already overpumped groundwater to satisfy a growing agricultural demand. This practice is counterproductive because degraded or depleted groundwater produces fewer crops, leading to food security problems and possible social disruption.[44]

A third of all Africans already live in water-scarce environments, and global climate change is likely to increase these numbers significantly. According to Citigroup's chief economist Willem Buiter, in the not-so-distant future water will become "the single most important physical commodity-based asset class, dwarfing oil, copper, agricultural commodities and precious metals."[45] Over the next 10 years, water problems will contribute to instability in regions important to U.S. national interests, and shortages and poor quality, when combined with poverty, social tensions, environmental degradation, and ineffectual government, will contribute to social disruptions that could result in failed states.[46] Biofuels mandates in Europe and the United States pressure agricultural expansion and stress natural resources. These practices are detrimental to energy security and could require U.S. military involvement in countries where there is currently little security threat.

Algae. Some scientists suggest algae may offer biofuels solutions that will not compete with food agriculture or scarce water supplies. Algae are a potential energy source that can be converted into biodiesel and bio–jet fuel, and on paper some scientists believe it could replace petroleum use altogether.[47] Algae have been studied for many years for production of hydrogen, methane, vegetable oils, hydrocarbons, and ethanol.[48] In 2006, after President George W. Bush declared that the United States was "addicted to oil," government algae research was resurrected and venture capital flowed into dozens of algae startups. Scientists and entrepreneurs have been trying to unlock the energy potential of algae for more than three decades. Some companies grow algae in ponds, others grow them in plastic and glass tubes called bio-reactors, and others keep their algae away from sunlight, feeding them sugars instead.[49] The National Research Council concluded that current technology scaled up to produce 39 billion liters of algae-derived biodiesel per year—5 percent of total U.S. transportation fuel needs—would require unsustainable levels of water and fossil fuel–based energy and fertilizer.[50] Today's technologies require between 3.15 and 3,650 liters of water to produce the amount of algae-biofuel equivalent to one liter of gasoline. As a comparison, petroleum requires 1.9 to 6.6 liters of water to produce one liter of gasoline.[51] Some argue that algae can be cultivated in salt water, but even salt water algae require all cooling water and evaporative make-up water to be fresh, or else salinity increases to lethal concentrations.

John Benemann, a biochemist who has spent more than 30 years working on algae, says, "algae biofuels cannot compete with fossil energy based on simple economics." Researchers at the Lawrence Berkeley National Laboratory estimate that biofuels grown from algae in ponds at scale would cost between $240 and $332 a barrel, considerably higher than current petroleum prices.[52] Algae is thus not a viable option to support energy security at this time.

Recommendations

Improving national energy security is principally about reducing the cost of energy to consumers and preventing disruptions in the oil supply. According to the 2010 National Security Strategy, the development of new sources of energy will reduce dependence on foreign oil and provide better energy security.[53] At this time, an investment in biofuels alone will not reduce America's thirst for foreign oil. The Nation must employ other alternatives, such as improving efficiencies, using new technologies to tap into domestic petroleum reserves, and developing better conservation practices.

Efficiency. Global consumption of petroleum will continue to grow about 1 percent per year and will remain the primary transportation fuel in the foreseeable future.[54] The United States is taking steps to produce more fuel-efficient automobiles by employing hybrid technology, developing lighter materials, and improving engine and transmission efficiency. Because of these initiatives, a reversing trend in domestic fuel consumption is expected by 2020. Some of these fuel-efficient technologies are compatible for use in military vehicles and can reduce the fuel needed on the front lines. Investing in fuel-efficient technologies thus enhances our energy security.

Conservation. Liquid fuels make up the majority of military logistics operations and require thousands of personnel at an enormous cost in both money and human life. Until a few years ago, military wargaming did not factor energy into the equation; it was simply assumed fuel would be available on time and where needed. Private industry case studies show behavior-based conservation methods often result in 20 percent or more in energy use reductions.[55] Even small consumption reductions can make a big difference in the logistics burden. Better planning, new doctrine, and conservation training can greatly enhance energy security for military operations.

Domestic Oil and Gas Production. Until quite recently, it appeared the United States was increasing its dependency on foreign oil imports, but today true energy independence has become a real possibility even without the development of alternative fuels. A dozen years ago, shale gas amounted to only 2 percent of domestic production; today it is 37 percent and rising. Natural gas is in such ample supply that its price has plummeted. This unanticipated abundance has ignited a new political argument about liquefied natural gas—not about how much the Nation will import but how much it should export.[56] According to a 2012 report published by Citigroup analysts, North America is "the new Middle East."[57] In 2011 the United States registered the largest increase in domestic oil production of any country outside the Organization of the Petroleum Exporting Countries, and net petroleum imports have fallen from 60 percent of total consumption in 2005 to 42 percent today.[58] Analysts and economists believe that North America can achieve energy independence by 2020. Domestic oil and natural gas production has surged because of new technologies such as hydraulic fracturing and horizontal drilling, which allow companies to tap hydrocarbons trapped in shale and other tight rock formations. Government estimates suggest that domestic production of petroleum will rise another 22 percent to 6.7 million barrels per day by 2020. While domestic production is increasing, better efficiency and conservation practices are on track to reduce the amount of fuel Americans consume by almost 10 percent.[59] Collectively these energy alternatives will greatly contribute to overall national energy security.

Conclusion

For the United States to achieve energy security, it must reduce its dependence on foreign oil. However, should the military—the branch of government responsible for national security—be responsible for investing its limited resources as a venture capitalist to jumpstart a biofuels industry and be forced to purchase fuels at 10 times the cost of readily available petroleum-based fuels? Not only does this not make good economic sense, but it also puts our national security at risk. Biofuels

Airman prepares to refuel F-16 Fighting Falcon, part of field service evaluation for biofuel operations (U.S. Air Force/Jeremy Lock)

mandates divert scarce military resources away from critical programs such as weapons modernization, maintenance, training, and readiness. America's military is the largest consumer of liquid fuels in the world, but it still only accounts for 3.6 percent of annual U.S. consumption. This low percentage is not enough to spark a biofuels industry and affect overall fuel prices.

As this article points out, biofuels are counterproductive to national energy security for four primary reasons. First, the cost of biofuels is directly linked to the cost of petroleum, so as the price of petroleum increases so do biofuel prices. Second, biofuels are not currently available in the quantities needed to meet military demand and it is unlikely the industry will ever be capable of producing a sufficient supply. Third, biofuels energy density is significantly less than fossil fuels, and less energy density means less fuel efficiency. Less fuel efficiency means more fuel convoys will be needed to meet the military's mission, increasing costs and risks to Servicemembers. The fourth and possibly most compelling reason is that the greater demand for biofuels feedstock will foster global threats and as a result may increase the likelihood that our nation may have to deploy forces to new threat areas. Our military depends on the best technology to defend the Nation, and for the aforementioned reasons petroleum will remain the optimal energy source for some time to come. **JFQ**

Notes

[1] Deloitte Development LLC, *Energy Security America's Best Defense: A study of increasing dependence on fossil fuels in wartime, and its contribution to ever higher casualty rates* (New York: Deloitte LLC, 2009), 4.

[2] Moshe Schwartz, Katherine Blakeley, and Ronald O'Rourke, *Department of Defense Energy Initiatives: Background and Issues for Congress* (Washington, DC: Congressional Research Service, December 2012), 18.

[3] National Defense Authorization Act for Fiscal Year 2007, P.L. 364, 109th Congress, *Department of Defense goal regarding use of renewable energy to meet transportation needs* (October 17, 2006).

[4] Ibid.

[5] U.S. Navy, *The Department of the Navy's Energy Goals*, available at <www.navy.mil/features/Navy_EnergySecurity.pdf>.

[6] James T. Bartis and Lawrence Van Bibber, *Alternative Fuels for Military Applications* (Santa Monica, CA: RAND, 2011), ix, available at <www.rand.org/pubs/monographs/MG969>.

[7] Thomas Pyle, "The Navy's Use of Biofuels Is Inefficient and Costly," *U.S. News and World Report*, July 19, 2012, available at <www.usnews.com/opinion/blogs/on-energy/2012/07/19/the-navys-use-of-biofuels-is-inefficient-and-costly>.

[8] Rick Newman, "More Evidence That It's Time to Dump Ethanol," *U.S. News and World Report*, July 31, 2012, available at <www.usnews.com/news/blogs/rick-newman/2012/07/31/more-evidence-that-its-time-to-dump-ethanol>.

[9] Energy Information Agency, "Biofuels in the U.S. Transportation Sector," February

2007, available at <www.eia.gov/oiaf/analysispaper/biofuels_notes.html#133>.

[10] Ibid.

[11] A. Oasmaa and E. Kuoppala, "Fast Pyrolysis of Forestry Residue, 3, Stability of Liquid Fuel," *Energy & Fuels* 17, no. 4 (2003), 1075–1084.

[12] S.B. Jones et al., *Production of Gasoline and Diesel from Biomass via Fast Pyrolysis, Hydrotreating and Hydrocracking: A Design Case* (Richland, WA: Pacific Northwest National Laboratory, February 2009), 4.3.

[13] Michael Hartmut, "The Nonsense of Biofuels," *Angewandte Chemie International* 51, no. 11 (March 2012), 2516–2518, available at <http://onlinelibrary.wiley.com/doi/10.1002/anie.201200218/full>.

[14] "Biofuel markets and policy impacts," in *Biofuels: prospects, risks and opportunities*, The State of Food and Agriculture 2008 (Rome, Italy: Food and Agriculture Organization of the United Nations, November 2008), available at <ftp://ftp.fao.org/docrep/fao/011/i0100e/i0100e04.pdf>.

[15] U.S. Department of Energy, "Biodiesel Benefits and Considerations," February 2011, available at <www.afdc.energy.gov/fuels/biodiesel_benefits.html>.

[16] *Energy Security,* U.S. Code, Title 10, Chap. 173, Sec. 2924, Annual Department of Defense energy management reports, January 3, 2012.

[17] Barack Obama, "America's Energy Security," address at Georgetown University, Washington, DC, March 30, 2011, available at <www.whitehouse.gov/the-press-office/2011/03/30/remarks-president-americas-energy-security>.

[18] "U.S. Crude Oil Imports by Country of Origin," available at <www.eia.gov/dnav/pet/pet_move_impcus_a2_nus_epc0_im0_mbblpd_a.htm>.

[19] Energy Information Administration, "Spot Prices for Crude Oil and Petroleum Products," available at <www.eia.gov/dnav/pet/pet_pri_spt_s1_d.htm>.

[20] Rosamond Naylor and William Wrigley, "Biofuels, Rural Development, and the Changing Nature of Agricultural Demand," Center on Food Security and the Environment, Stanford Symposium Series on Global Food Policy and Food Security in the 21st Century, April 11, 2012, 6.

[21] U.S. Energy Information Administration, "Refinery Sales Volumes of Other Petroleum Products," available at <www.eia.gov/dnav/pet/pet_cons_refoth_d_nus_VTR_mgalpd_a.htm>.

[22] "AAA Daily Fuel Gauge Report, Oil Price Information Service," *National Average Fuel Prices*, available at <http://fuelgaugereport.opisnet.com/index.asp>.

[23] Anthony Andrews et al., *The Navy Biofuel Initiative Under the Defense Production Act*, R42568 (Washington, DC: Congressional Research Service, June 22, 2012), 3.

[24] Pyle.

[25] Deloitte, 15.

[26] David S. Eady et al., *Sustain the Mission Project: Casualty Factors for Fuel and Water Resupply Convoys* (Arlington, VA: Army Environmental Policy Institute, September 2009), 6.

[27] Operation *Iraqi Freedom*, Operation *Enduring Freedom* Coalition Fatalities, available at <http://icasualties.org/OEF/Index.asp>.

[28] Bartis and Van Bibber, 83.

[29] Mark Peters, "Ethanol's Long Boom Stalls, Fuel-Additive Plants Close as Gasoline Demand Falls, Federal Mandates Are Met," *Wall Street Journal*, June 11, 2012, available at <http://online.wsj.com/article/SB10001424052702303395604577434782358634706.html>.

[30] Newman.

[31] Alan Broughton, "Sierra Leone—Land grabbing: A new colonialism," *Globalfaultlines*, available at <http://axisoflogic.com/artman/publish/Article_65146.shtml>.

[32] Renewable Fuels Agency, "Review of Indirect Effects of Biofuel, Evaluation of the drivers of land use change Review of future demand and supply of biofuels to 2020 and their impact on GHG-emissions," June 26, 2008, 28, available at <www.globalbioenergy.org/uploads/media/0806_AEA_-_Review_of_indirect_effects_of_biofuels.pdf>.

[33] Ibid.

[34] David Roberts, "Why the military is trying to reduce its fossil fuel use," July 30, 2012, available at <http://grist.org/climate-energy/why-the-military-is-trying-to-reduce-its-fossil-fuel-use/>.

[35] United Nations, United Nations Department of Economic and Social Affairs/Population Division, *World Urbanization Prospects: The 2011 Revision* (New York: United Nations, 2012), 1.

[36] E. Gallagher, *The Gallagher Review of the Indirect Effects of Biofuels Production,* Renewable Fuels Agency, UK, July 2008, 29, available at <www.unido.org/fileadmin/user_media/UNIDO_Header_Site/Subsites/Green_Industry_Asia_Conference__Maanila_/GC13/Gallagher_Report.pdf>.

[37] Hartmut.

[38] Tim Rice, "Meals per gallon, the impact of industrial biofuels on people and global hunger," ActionAid, available at <www.actionaidusa.org/eu/publications/meals-gallon-impact-industrial-biofuels-people-and-global-hunger>.

[39] Ibid.

[40] Broughton.

[41] Rice.

[42] Ibid.

[43] GRAIN, *Squeezing Africa Dry: Behind every land grab is a water grab*, available at <www.grain.org/article/entries/4516-squeezing-africa-dry-behind-every-land-grab-is-a-water-grab>.

[44] Maria Otero, Global Water Security, Intelligence Community Assessment, May 9, 2012, available at <www.state.gov/j/189598.htm>.

[45] Ibid.

[46] Schuyler Null, "Global Water Security Calls for U.S. Leadership, Says Intelligence Assessment," *NewSecurityBeat*, available at <www.newsecuritybeat.org/2012/03/global-water-security-calls-for-u-s-leadership-says-intelligence-assessment/>.

[47] Ibid.

[48] John R. Benemann, "Opportunities and Challenges in Algae Biofuels Production," 5, available at <www.fao.org/uploads/media/algae_positionpaper.pdf>.

[49] Marc Gunther, "Green Crude: The Quest to Unlock Algae's Energy Potential," *Yale Environment 360*, available at <http://e360.yale.edu/feature/green_crude_the_quest_to__unlock_algaes_energy_potential/2582>.

[50] Robert F. Service, "Large Scale Algae Biofuels Currently Unsustainable, New Report Concludes," *ScienceInsider*, October 24, 2012.

[51] Ibid.

[52] Gunther.

[53] The White House, *National Security Strategy* (Washington, DC: The White House, May 2012), 2.

[54] Pike Research, "Algae-Based Biofuels—Demand Drivers, Policy Issues, Emerging Technologies, Key Industry Players, and Global Market Forecasts," available at <www.pikeresearch.com/research/algae-based-biofuels>.

[55] John Laitner, Karen Ehrhardt-Martinez, and Vanessa McKinney, "Examining the Scale of the Behaviour Energy Efficiency Continuum," The Foundation of Future Energy Studies, 218–219, available at <www.mitenergyclub.org/assets/2009/10/25/LaitnerEA2009_EfficiencyBehaviorContinuum.pdf>.

[56] Daniel Yergin, "America's New Energy Reality," *Dallas Morning News*, June 9, 2012.

[57] Tim Mullaney, "U.S. Energy Independence Is No Longer Just a Pipe Dream," *USA Today,* May 2012.

[58] Yergin.

[59] Mullaney.

Soldier pulls watch during traffic checkpoint coordinated with members of Afghan National Army outside of Combat Outpost Yosef Khel, Paktika Province (U.S. Army/Ken Scar)

Shaping a 21st-Century Defense Strategy

Reconciling Military Roles

By William G. Braun III and Charles D. Allen

Once again the U.S. military is transitioning from a period of sustained conflict to a resource-constrained and uncertain future. Accordingly, the Nation is again debating its global role and how to develop an appropriate national security strategy. Even before that strategy is fully formulated, the military submitted a budget that comports with fiscal austerity while sustaining current readiness and investing in capabilities to meet future requirements for a complex international security environment.

This article expands the national security debate by advocating adapting the joint force to the emerging strategy and security environment through enhancing its shaping capabilities. The principal stimulus driving the need for change is the 2012 Defense Strategic Guidance, which sustains the security strategy shift from deterrence and containment to

William G. Braun III is Professor of Strategy, Policy, and Landpower in the Strategic Studies Institute at the U.S. Army War College. Charles D. Allen is Professor of Leadership and Cultural Studies in the Department of Command, Leadership, and Management at the U.S. Army War College.

cooperation through engagement. The emerging consensus suggests the future national security strategy will direct a regionally tailored force for limited engagement.[1] As with any fundamental shift in national policy objectives, strategy, or operational concepts, the initial guidance is seldom the last word.[2] The military must be sized and resourced to adapt to the realities of strategy and policy adjustments as they occur. It is critical that military capabilities are resourced for the national strategy and that they posture the joint force to create and seize opportunities. The objective is a military that protects and advances U.S. interests in times of peace while providing robust and flexible options to confront aggression worldwide.

A Shift from Containment to Engagement

To establish context for the emerging military narratives, it is necessary to trace the trajectory of the national security debate since the end of World War II. The Cold War grand strategy, often attributed to "the father of containment" George Kennan, carried the Nation through the last half of the 20th century.[3] In his famous "X article" published in 1947, Kennan advocated replacing cooperation with the Soviet Union with a strategy of long-term containment of their expansionist philosophies. While the strategy matured during the Cold War, the military's role remained stable.[4] With a few notable exceptions, the Armed Forces provided credible and robust conventional combat capability to defend national interests, exercised legitimate coercive power to maintain international order through containment, and demonstrated a mutually assured destruction capability that discouraged nuclear confrontation.

With the demise of the Soviet Union and the end of the Cold War, a search for a new grand strategy narrative began. President George H.W. Bush presented a vision of a "new world order" to Congress in 1990 that emphasized "cooperation," where "nations of the world can prosper and live in harmony."[5] President Bill Clinton described how the vision could be achieved through a strategy of "engagement and enlargement," thus giving it structure. This particular strategy relied primarily on economic and diplomatic efforts, backed by military force, and was designed to expand the global reach of democracy and economic prosperity.[6] President George W. Bush's National Security Strategy reiterated many of the tenets of the earlier post–Cold War security strategies. Faced with the new reality of terrorist attacks and the emergent demands of two simultaneous wars, Bush emphasized the role of military power and highlighted the U.S. prerogative for preemptive action to counter rogue states or terrorist organizations that might strike without warning.[7] While President Barack Obama's 2010 National Security Strategy acknowledged the role of the military, it reverted to much of the language related to cooperation and burden-sharing reflective of the 1990s.[8]

The national security strategy is in transition again. The strategic environment presents a weak global economy, a struggling U.S. economy, and shrinking defense resources. While the current national security strategy is not fully developed or articulated, it appears to conform to a general trajectory evident since the Cold War, from containment and deterrence to cooperation and engagement, with more limited ambitions than those initially expressed in the 1990s. This emerging narrative is designed to address a security environment that includes a nonhostile but rising rival in Asia (China), international nuclear proliferation (Iran, Pakistan, and North Korea), revolutions against existing world order (the Arab Spring in the African Maghreb and Egypt), continued unrest in the Middle East (the Levant), and growing concern over instability and violence (Mexico and other Central/South American nations) in the Western Hemisphere.

The national security strategy narrative is expected to focus on engagement and cooperative relationships to advance U.S. interests and establish a stable international order. It should appropriately emphasize the use of economic and diplomatic means backed by the limited use of the military as a coercive instrument of national power. In this era of fiscal austerity, emerging consensus emphasizes a regionally tailored military strategy of limited engagement.

The current Defense Strategic Guidance (January 2012) directs the military to adapt to the future strategic environment even as it remains a "global presence emphasizing the Asia-Pacific and the Middle East" and at the same time is "prepared to confront and defeat aggression anywhere in the world," all with a much smaller size and reduced resources.[9] In underwriting this strategy, the Secretary of Defense is expected to develop a joint force that is "smaller and leaner" but "will remain agile, flexible, ready, innovative, and technologically advanced."[10] This is a tall order that requires prioritization and trade-off of risk. The security establishment requires a model for dynamic force adaptation and a framework to develop the narrative that guides prioritization.

The organizational concept of dynamic equilibrium may provide such a model. It draws on an ecological system metaphor to examine an organizational response to a changing environment. The "open system" ecological metaphor is rooted in chaos, complexity, and systems theories. Several elements of the metaphor can be applied to the military's adaptation to the evolving threat, security, and operational environments.

The dynamic equilibrium metaphor captures the interactive and multidimensional nature of systems and the continuous adaptive change imposed by each member of an ecosystem on the other. This interactive adaptation is a dynamic where the norm is constant change in response to multiple simultaneous stimuli from other members and elements of the system. There are two broad mechanisms of change within the theory—iterative evolution and rapid adaptation.[11] The first is more common in nature. The second can produce rapid (transformational or revolutionary) change, but just as often results in the death of many members of the system

Solider and Afghan police officer search terrain in Kunar Province prior to firefight (U.S. Army/Gary A. Witte)

and the emergence of a new ecosystem. Death occurs when an organism stops adapting and no longer actively influences or is influenced by the system.[12] The remaining sections address several dimensions of the military's environment that must be considered as our leaders adapt the joint force for the future.

Equilibrium in the Military Narrative

Threat versus Opportunity. National security literature tends toward threat-based analysis. Security studies and military planning are likely to focus on approaches that prevent unfavorable order and unacceptable levels of disorder,[13] while identifying and planning for black swan contingencies.[14] Conversely, contemporary organizational and business literatures promote strategies that focus on opportunity identification and exploitation.

Applying this opportunity perspective to security strategy and military implementation concepts can facilitate the identification of alternative approaches to achieving national objectives. Instead of physically "pivoting" to the Asia-Pacific and Middle East, one could envision a strategy that employs military power in various regions to rebalance our global efforts to indirectly influence the regions prioritized by U.S. national leadership.[15] In addition one may develop innovative ways to exploit military relationships and partnerships while employing other instruments of national power.

Time Horizons Equilibrium. The military narrative should include linkages to current policy, strategy, and resources while engaging proactively in actions that adapt the organization to future threats, opportunities, and political perspectives. This results in two time horizons for strategic decisions that affect force development. The near-term horizon is driven by prioritized distribution of available resources, which has to be justified in the context of current national strategy and policy objectives. The long-term horizon is based on estimates of future threats, operational environment opportunities, and the range of potential strategy and policy decisions that may be pursued by future administrations. The long-term horizon requires senior leaders to establish aspirational goals and a vision of the range of military capabilities to achieve them. The Services' primary concern is with the near-term horizon, which requires the distribution of resources to maintain readiness while initiating the evolutionary change and development initiatives that move the force in the direction of the long-term vision.

Military Strategy Equilibrium. Absolute war and peace are archetypal states that are never fully realized. Competition spans a continuum from the civil order of peace through major combat manifested by war. Unattended turmoil and misunderstandings among nonhostile rivals can lead to escalation of hostility and increased incidence of extreme violence. Similarly, managing disorder within the context of combat operations is necessary to nurture the civil order associated with peace.

The U.S. security establishment has acknowledged the vital role of the military in shaping the security environment. In 1997, Chairman of the Joint Chiefs of Staff General John Shalikashvili stated, "The military has an important role in engagement—helping to shape the international environment in appropriate ways to bring about a more peaceful and stable world." In the next sentence he provided a caveat: "The purpose of our Armed Forces, however, is to deter and defeat threats of organized violence to our country and its interests."[16] When faced with austere budgets, reduced force structure, and uncertain futures, senior civilian and military leaders typically revert to a rhetoric dominated by the force sizing and prioritization mantra to "fight and win the Nation's wars," with all other uses of the military being "lesser-included" capabilities.

The military's force-sizing construct since the Cold War has been a two-theaters strategy. While arguably underresourced, the construct was based on an aspiration to fight and win two nearly simultaneous major regional contingencies.[17] In his February 2014 press conference, Secretary Hagel conveyed that the construct was now passé and stated as well that "we are no longer sizing the military to conduct long and large stability operation." [18] He went on to say that the Army will be sized to decisively defeat aggression in one major combat theater while defending the homeland and supporting a joint force engagement in another theater.

When not engaged in war, the military structure and its inherent capabilities are available to America's political leaders for other missions. In practice the military does a great deal more than simply preparing for and executing regional contingencies and major combat operations. Especially with regard to landpower, a force capable of fighting two major regional contingencies can accomplish a number of "lesser-included" tasks during periods of relative peace. The deterrent quality of a ready force is intended to provide the Nation with sufficient coercive power to discourage the escalation of national rivalries into major combat operations. Should that deterrence fail, the military's mission has historically been to decisively defeat the enemy.

Realist/Balancer versus Idealist/Engagement Foreign Policy. Air-Sea Battle has occupied a great portion of the public debate regarding the military's strategic narrative since the release of the Defense Strategic Guidance. Air-Sea Battle's key characteristics include military involvement starting at the commencement of hostilities, withstanding an initial attack, executing a blinding and suppression campaign against enemy long-range intelligence, reconnaissance, and surveillance (ISR) and strike systems, and seizing the initiative in the sea, air, space, and cyberspace domains. From this posture, the execution of the concept would create time for "options to resolve a prolonged conventional conflict on favorable terms" through blockades, sustained logistics, and the expansion of military and industrial production.[19]

Considerations of the role landpower plays in this operational concept appeared late in the concept's development.[20] But even as a latecomer, landpower's role was soon recognized in clearing coastal areas of surface-to-ship missiles, providing for land-based air defense, and performing myriad sustainment functions associated with establishing theater operations and sustaining the joint force. As this joint operational concept is further developed, it is likely that the vital role for landpower will be better understood.

If the United States adopts a realist foreign policy, the approach of balancing rising powers with regional partners and preserving the ability to counter rivals once hostilities commence is a sound strategy. The Air-Sea Battle operational concept facilitates countering a hostile enemy with strategic stand-off and anti-access/area-denial capabilities.

However, senior national security leaders should reconsider the utility of resourcing an operational concept that limits the range of military options to direct confrontation, especially when countering nonhostile rivals. Such an approach seems unwise, especially in cases where the rival's economic markets may be closely linked to the U.S. economy. This limited approach would leave our leaders with few military options to counter a rival that confronts the Nation directly with economic and diplomatic power, and employs military power through distant or amorphous proxies. One can easily envision the coercive power levers a rival could bring to bear short of hostilities, making military employment options and posturing to deter hostilities moot.

The prioritization of resources to prepare the military for the future must accommodate both the future security environment and the political reality that U.S. policy and international action do not align perfectly with either realist or idealist perspectives of political science theory. Actual policy and international political choice reflect a hybrid approach. The range of military capabilities must accommodate options for dealing with the future environment that are based in both realist and idealist perspectives.

American Landpower: Prevent—Shape—Win

The Army Chief of Staff (CSA) has Title 10 responsibilities to field the Army and sustain America's joint force. General Ray Odierno, in the 2012 Army Posture Statement, presented the Army's primary roles as prevent, shape, and win, with readiness, force structure, and modernization as the principal rheostats to adjust resource prioritization to adapt the Army to the strategic and fiscal environment. Current military force sizing is based on a "fight and win" philosophy. The fight and win imperative encompasses decisive joint combat capabilities for the rapid defeat of enemies and a decisive end to hostilities.

The "win to prevent" paradigm offers two paths to achieving a political objective prior to the onset of combat. A force-in-being's "win" capabilities discourage opportunistic rivals from engaging in hostilities and prevent hostility expansion to other regions after the start of conflict. America must maintain a legitimate military deterrent power by fielding a force-in-being capable of decisively defeating any enemy while demonstrating the political will to use it.

The Air-Sea Battle concept combined with operational concepts for landpower (combined arms maneuver, wide area security, counterinsurgency, and counterterrorism doctrines) provide the basis for decisive combat operations to accomplish the military's "win" mission. Air-Sea Battle facilitates coercive access to contested areas, thereby enabling landpower forces to deploy, stabilize, and exploit successes in the accomplishment of strategic objectives. However, short of resorting to coercive methods and direct hostilities, an emphasis on "win" capabilities offers few military options using cooperation and engagement to address rivals who choose to challenge U.S. interests.

The military's ability to shape the security environment addresses such nonhostile or indirect competition. In addition, shaping provides for the establishment of conditions that support a return to civil order once employment of "win" capabilities manages extant hostilities. The shaping function is directed toward influencing the focal nation's people and leadership. Influencing segments of a society and their leadership short of conflict is achieved largely through trust relationships and cooperative engagements. For the military these operations are normally landpower-centric. Thus, in addition to traditional fight and win capabilities, the Army needs to develop an ethos that embraces shaping as part of its warrior culture.

"Shape to win" and "shape to prevent" paradigms have their own mechanisms to achieve desired objectives. The "shape to win" model is analogous to flexible deterrent options and has been associated with campaign planning for decades. The "shape to prevent" model manifests itself in several ways, with the common theme of enriching cooperation and partnerships that contribute to favorable order. Shaping contributes to achieving national security objectives in environments that span conditions from civil order to war and back to civil order.

The shaping role contributes to winning and preventing war in a number of ways:

- Forward presence shaping operations provide early warning by means of regional cultural engagement, and opportunities to gather human intelligence and geographic access through established relationships.
- The shaping role develops a cooperation-based capacity and desire for regional partners to confront military challenges in a manner that could not be achieved independently.
- Conducting shaping operations with supportive partners can block rival power ambitions short of hostilities; it is a realist/balancing argument.
- Shaping operations conducted with potentially opportunistic partners offer positive cooperative engagement incentives short of confrontation to modify their behavior.
- Shaping facilitates U.S. force redeployment following hostilities with some assurance of leaving the foundations of sustainable civil order behind.
- Shaping operations permit the military to contribute to the engagement and enlargement objectives associated with promoting liberty under the rule of law, human rights, and the subordination of the military to legitimate civil authority throughout the peace-war continuum.

Unlike combat operations, shaping does not require the threat of hostilities to execute. The military can conduct Building Partner Capacity, Security Cooperation, Stability, and Security Force Assistance missions in the absence of a threat; or it can combine these shaping operations with counterinsurgency and counterterror combat missions to synergistic effect in nonpermissive security environments short of major combat operations.

In 2005, Department of Defense (DOD) Directive 3000.05 established security operations as a core military mission. It directed that stability (shaping) operations "shall be given priority comparable to combat operations."[21] On a national scale, this effort was reinforced when President George W. Bush signed National Security Presidential Directive 44 directing the Department of State to be lead agent, using the Office of the Coordinator of Reconstruction and Stabilization to coordinate and harmonize all strategies and plans associated with reconstruction and stabilization activities for states transitioning from conflict and civil strife.[22]

More recently the 2012 Defense Budget Guidance, which followed the Defense Strategic Guidance, called for "a fresh approach to the traditional 'two war' force-sizing construct that had shaped defense planning since the end of the cold war."[23] Yet, of the military's 10 primary missions outlined in the guidance, only 4 are designated as criteria for force sizing. Three of the four involve building the capacity to win wars. The shaping missions that provide stabilizing presence and support counterinsurgency operations are accompanied by specified caveats limiting their resourcing.[24]

Both 2012 defense guidance documents convey that the U.S. security establishment is more focused on defeating threats than developing military capabilities to manage the security environment. Americans understandably prefer short-duration, decisive conflicts, and they frequently consider wars to be acts of political choice. However, in *The Utility of Force*, Rupert Smith presents a convincing argument that protracted conflicts "among the people" represent the reality of modern warfare.[25] Managing the security environment through shaping offers an attractive alternative to either proposition—decisive large-scale conflict or protracted war "among the people." First, shaping operations provide a feasible and prudent alternative in which U.S. military capabilities advance cooperative behaviors to maintain a stable security environment short of coercive hostility. Second, involvement in wars and deteriorating security environments is not always subject to U.S. preference or choice. History is replete with examples of Washington being compelled to military action to restore order or confront aggression. Forward presence shaping operations can provide early warning and offer noncoercive access, thereby opening a range of military options to prevent war or restore civil order short of major combat operations. Unfortunately, shaping operations associated with forward presence, partnering to build relationships,[26] security cooperation, and stability operations[27] continue to be misunderstood, undervalued, and underresourced in austere economic environments.

The development of shaping operations requires the deliberate resourcing of specific force design, readiness, and modernization initiatives. Embracing shaping does not imply undervaluing the imperative to "fight and win the Nation's wars." Shaping and winning operations are appropriately designed to provide complementary capabilities. One generally accepted lesson has emerged from the last several decades of conflict: the resultant civil order—not the defeat of a specific threat—defines victory in modern warfare. By necessity, if there are insufficient resources to prepare for both missions simultaneously, a portion of the force may temporarily focus on the "win"

Soldiers rally in urban operations complex at Nevada Test and Training Range (U.S. Air Force/ Michael R. Holzworth)

or "shape" role during a particular operation or deployment. But that does not absolve operational units of the requirement to conduct either decisive combat or shaping operations with a limited amount of predeployment or rotational training.

America's security establishment should acknowledge the vital role of landpower as the force capable of shaping a population-centric security environment, whether through the coercive power of combat operations or the influence generated by shaping operations. "Shape to prevent" and "shape to win" models define the respective conditions necessary to achieve political and military victory in modern warfare.

The arguments against resourcing shaping capabilities and capacities align generally with the following themes. First, it is not the function of DOD or the Army to execute these operations. The activities associated with shaping operations, primarily Building Partner Capacity, Security Cooperation, and Stability (especially when they involve development or law enforcement) fall outside DOD's roles, missions, and authorities. For this reason, national leaders are reluctant to commit resources to build DOD capabilities to engage in these operations, and security-minded interagency partners are not willing to allow the department to assume responsibility for their execution.

Shaping operations are necessary to prevent conflict, mitigate its impact, and provide the opportunity to transition to some form of a sustainable civil order. In the last decade of war, no Federal agency has marshaled the resources or changed its capability sufficiently to execute these missions as well as the Army. Some adjustments in roles, missions, and authorities are therefore necessary to enable other agencies to set objectives and provide oversight when developing plans, while requiring the Army to develop and design tailored capabilities to execute these missions. Once U.S. political leadership recognizes the value of military shaping operations as a legitimate foreign policy execution tool during peacetime, the Army will have to embrace the shaping mission within its professional jurisdiction.

A military argument for resisting the prioritization of resources for shaping capabilities is a belief that any reduction in the "fight and win" capability will endanger the military's contract with the American people—to win the Nation's wars. Adherents to this view proffer the opinion that should the military fail at shaping, there are other Federal departments and agencies capable of providing assistance. There is not, however, another agency that can fight and win the Nation's wars.

This argument has merit. DOD and the Services cannot abandon their duty

Marines select targets in tactical movement training at Camp Rodriguez, South Korea (DOD/James Norman)

to win wars: The notion of winning in modern warfare (and arguably throughout history) involves a great deal more than simply defeating the enemy's army or planting the U.S. flag in the enemy's capital. It involves encouraging legitimate government and developing indigenous force capabilities that permit U.S. disengagement with some assurance of sustainable security and order.

Conclusion

In summer 2013, DOD's Cost Assessment and Program Evaluation organization released the results of the Strategic Choices and Management Review (SCMR) study directed by Secretary of Defense Chuck Hagel. The SCMR provided resource prioritization guidance to the Quadrennial Defense Review effort within three broad funding bands. It did not alter the regionally prioritized, limited engagement strategy proposed in the 2012 Defense Strategic Guidance.[28]

The continuity of the U.S. post–Cold War security strategy of cooperative engagement, implemented through economic and diplomatic instruments of power reinforced by military power, is appealing. The past two decades suggest that even altruistic aspirations to spread democracy, human rights, and economic prosperity through diplomacy and economic initiatives alone are often foiled by adversaries with different agendas. U.S. military leadership must embrace civilian leaders' expressed desire to reduce the size and economic burden of the force, while at the same time preparing it for the full range of potential confrontations.

The argument that the military must retain the ability to "fight and win the Nation's wars" when shaping operations are resourced as lesser included capabilities is incongruous with current national security strategy aspirations. And it is not realistic to expect the whole-of-government engagement capability to increase given the current fiscal environment. The argument to limit resource expenditures, however, is compelling in light of U.S. fiscal circumstances. Faced with a volatile operating environment, austere resources, and an ambiguous group of adversaries, the Nation must strive for dynamic equilibrium as it adapts the joint force to win conflicts, manage security environments, and shape civil order within constrained resources. The new security culture must embrace the military's "shape" and "win" roles. Shaping operations are primarily landpower centric because they are conducted in the human domain among the people. The Army must and will carry the burden of successfully executing shaping operations in support of America's foreign policy security goals.

Current defense guidance charges the military with defeating future threats and protecting national interests worldwide. To do that in an austere resource environment, the force must improve operational effectiveness and efficiency in both combat and shaping capabilities. The Army's recent addition of a seventh warfighting function, Engagement, is an appropriate and needed addition to its doctrine.[29] The next iteration of defense guidance should prioritize the military's role in shaping operations during peacetime as well as recognize the requirement to conduct combat operations. The future operational environment demands a robust military capability to win conflicts among the people, while improving cooperative engagement shaping capabilities to maintain or restore peace. JFQ

Notes

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

[2] For early contrasting views and initial push back on the official strategy and military operational concept, see Douglas A. Ollivant, "Go Army, Beat Navy," *Foreign Policy*, September 28, 2012, available at <www.foreignpolicy.com/articles/2012/09/28/go_army_beat_navy>; Colin Clark, "Pentagon takes Second look at Strategy: Where are the holes?" *AoL Defense*, September 10, 2012, available at <http://defense.aol.com/2012/09/10/pentagon-takes-second-look-at-strategy-where-are-the-holes/>.

[3] James Gibney, "Big thinker," *The American Scholar* 81, no. 1 (2012), 114–117, available at <http://search.proquest.com/docview/923850522?accountid=4444>.

[4] John Lewis Gaddis, *Strategies of Containment: A Critical Appraisal of American National Security Policy During the Cold War*, 2nd ed. (New York: Oxford University Press, 2005).

[5] George H.W. Bush, "Toward a New World Order," address to a joint session of Congress and the Nation, 1990, available at <www.sweetliberty.org/issues/war/bushsr>.

[6] *National Security Strategy of Engagement and Enlargement* (Washington, DC: The White House, February 1995), available at <www.au.af.mil/au/awc/awcgate/nss/nss-95.pdf>.

[7] *The National Security Strategy of the United States of America* (Washington, DC: The White House, 2002), 14, available at <www.globalsecurity.org/military/library/policy/national/nss-020920.pdf>.

[8] *National Security Strategy* (Washington, DC: The White House, 2010), cover letter, available at <www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf>. President Obama states, "Our Armed Forces will always be a cornerstone of our security, but they must be complemented." Then he invokes the role of diplomats, development efforts, intelligence, law enforcement, and foreign partner burden sharing.

[9] *Sustaining U.S. Global Leadership*, cover letter.

[10] Ibid.

[11] As examples, see Connie J.G. Gersick, "Revolutionary change theories: A multilevel exploration of the punctuated equilibrium paradigm," *Academy of Management Review* 16, no. 1 (1991), 10–36; and S.L. Brown and K.M. Eisenhardt, "The art of continuous change: Linking complexity theory and time-paced evolution in relentlessly shifting organizations," *Administrative Science Quarterly* 42, no. 1 (1997), 1–34, available at <http://search.proquest.com/docview/203986467?accountid=27965>.

[12] Richard Tanner Pascale, Linda Gioja, and Mark Millemann, *Surfing the Edge of Chaos: The Laws of Nature and the New Laws of Business* (New York: Random House, 2000).

[13] Nate Freier of the Center for Strategic and International Studies coined the phrase *unfavorable order and unacceptable disorder* to describe the security environments most likely to compel U.S. intervention.

[14] It is impossible to plan for *black swan* contingencies in the sense that Nassim Nicholas Taleb used the term in *The Black Swan: The Impact of the Highly Improbable*, 2nd ed. (New York: Random House, 2010), but there are a host of "gray swans" in the environment that could test the robustness of any national security strategy or military operational concept and would satisfy the contingency planning requirement.

[15] Consider the possibilities of influencing China through activities in Africa. To stimulate ideas associated with this potential indirect regional approach, see David E. Brown, *Hidden Dragon, Crouching Lion: How China's advance in Africa is understated and Africa's potential underappreciated* (Carlisle, PA: Strategic Studies Institute, 2012), available at <www.strategicstudiesinstitute.army.mil/pubs/display.cfm?pubID=1120>.

[16] *National Military Strategy of the United States of America: Redefining America's Military Leadership* (Washington, DC: The Joint Staff), cover letter.

[17] Daniel Goure, *The Measure of a Superpower: A Two Major Regional Contingency Military for the 21st Century* (Washington, DC: The Heritage Foundation, January 25, 2013).

[18] Chuck Hagel, Remarks by Secretary Hagel and Gen. Dempsey on the Fiscal Year 2015 Budget Preview in the Pentagon Briefing Room, Alexandria, VA, February 24, 2014, available at <www.defense.gov>.

[19] Jan Van Tol, *AirSea Battle: A Point-of-Departure Operational Concept* (Washington, DC: Center for a New American Security, 2010), xiii.

[20] Philip Ewing, "Services promise to add Army to 'Air-Sea Battle,'" *DoD Buzz*, November 9, 2011, available at <www.dodbuzz.com/2011/11/09/services-promises-to-add-army-to-air-sea-battle/>.

[21] Department of Defense (DOD) Directive 3000.05, *Military Support for Stability, Security, Transition, and Reconstruction (SSTR) Operations* (Washington, DC: Government Printing Office [GPO], 2005); and later reinforced by DOD Instruction 3000.05, *Stability Operations* (Washington, DC: GPO, 2009).

[22] National Security Presidential Directive 44, *Management of Interagency Efforts Concerning Reconstruction and Stabilization* (Washington, DC: The White House, December 2005), available at <www.fas.org/irp/offdocs/nspd/nspd-44.html>.

[23] DOD, *Defense Budget Priorities and Choices* (Washington, DC: GPO, January 2012), 7, available at <www.defense.gov/news/Defense_Budget_Priorities.pdf>.

[24] *Sustaining U.S. Global Leadership*. The four mission sets that joint forces will be sized against are counterterrorism and irregular warfare, deter and defeat, nuclear deterrent capability, and homeland defense/defense support to civil authority. The limiting language associated with providing a stabilizing presence is "with reduced resources, thoughtful choices will need to be made regarding the location and frequency of these operations"; and with stability and counterinsurgency operations the language is "U.S. forces will no longer be sized to conduct large-scale, prolonged stability operations." The language is reasoned and mild in both cases, but it is sufficient to marginalize any argument made in defense of capabilities supporting these missions during the budget wars.

[25] Rupert Smith, *The Utility of Force: The Art of War in the Modern World* (New York: Knopf, 2007).

[26] This is especially so with unsavory partners with whom it is necessary to build trust and legitimacy to influence fundamental change over time.

[27] These may be conducted with "small foot-prints" and to some degree with rotational forces. But to be effective they are inherently long-duration operations.

[28] Detailed results of the Strategic Choices and Management Review are in "Deputy Secretary of Defense Ashton B. Carter and Vice Chairman of the Joint Chiefs of Staff James Winnefield Jr. Prepared Testimony House Armed Services Committee," in *House Armed Services Committee*, Washington DC, 2013.

[29] See U.S. Training and Doctrine Command (TRADOC) Pamphlet 525-8-5, *The U.S. Army Functional Concept For Engagement* (Fort Eustis, VA: TRADOC, February 24, 2014).

Marine Corps linguist for Female Engagement Team 11-2, Task Force Leatherneck, explains how to care for wound at district center in Delaram, Nimroz Province, Afghanistan (U.S. Marine Corps/Catie D. Edwards)

Targeting the JIIM Way
A More Inclusive Approach

By John Bilas, Scott A. Hoffman, John S. Kolasheski, Kevin Toner, and Douglas Winton

Consider two scenarios. The International Security Assistance Force (ISAF) and international community decide to more effectively and efficiently organize their resources and activities to tackle the Afghan opium trade, leading to a significant reduction in opium production. At the same time, a U.S. Army brigade defeats an insurgent cell in Kandahar City without firing a single shot. Yet despite a systematic focus on joint doctrine and a whole-of-government approach to address these scenarios, neither achievement is attributable to following formalized doctrinal guidance on how best to "target" problems preventing the achievement of desired outcomes or effects.

While Joint Publication (JP) 3-60, *Joint Targeting*, dated January 31, 2013, provides a rather comprehensive approach to targeting, it does not adequately address all the joint, interagency, intergovernmental, and multinational (JIIM) considerations required to synchronize activities and achieve desired effects. JP 3-60 requires further

Lieutenant Colonel John Bilas, USMC, is the III Marine Expeditionary Force Intelligence Plans Officer in Okinawa, Japan. Lieutenant Colonel Scott A. Hoffman, USAF, commands the 455th Expeditionary Operations Support Squadron at Bagram Airbase, Afghanistan. Colonel John S. Kolasheski, USA, is a Staff Officer assigned to U.S. Army Forces Command. Lieutenant Colonel Kevin Toner, USA, is the Public Affairs Officer for U.S. Army Japan and I Corps (Forward). Colonel Douglas Winton, USA, is a U.S. Army War College Professor Candidate.

refinement as it fails to guide either commanders or staffs to examine the process for adequately including nonlethal activities and interagency, intergovernmental, and multinational capabilities. This article offers several ways to improve the joint targeting process in a JIIM environment by reviewing how joint doctrine discusses JIIM considerations and showing how JP 3-60 remains too focused on "lethal" activities, recommending a new cognitive model to help commanders achieve their desired endstates, providing examples of successful targeting across JIIM, and recommending a more broadly acceptable name for the process.

Joint Doctrine

Joint doctrine is the body of basic principles that guide the employment of U.S. military force in synchronized, coordinated action toward common goals and objectives.[1] It readily recognizes the need for both coordination and unity of effort between the military and other U.S. Government agencies. In addition, joint doctrine rightfully acknowledges that achieving national strategic, theater strategic, and operational desired conditions requires more than just military instruments of national power. Indeed, as clearly expressed in JP 5-0, *Joint Operation Planning*, during Phase 0 (shape the environment) the diplomatic, informational, and economic instruments of national power have primacy, with military support in activities such as military-to-military engagements and foreign internal defense (FID) training. While military activities typically have precedence during Phases I, II, and III (deter the enemy, seize the initiative, and dominate the enemy), primacy reverts to the other instruments of national power in Phases IV and V (stabilize the environment and enable civil authority). Critically, stakeholders will achieve greater and more enduring effects by coordinating and synchronizing military and nonmilitary efforts throughout all phases.

Assessing operations over the last decade, the imperative of JIIM planning to meet and/or promote national interests and strategic objectives becomes readily apparent. Since 2001 joint doctrine has evolved to incorporate interagency, intergovernmental, and multinational actors into military plans and operations, but it still fails to address how best to involve all JIIM partners in targeting. A quick review of current joint doctrine illustrates this point. Comparing the instances of the use of the word *interagency* in joint publications, the disparity between planning and executing JIIM activities becomes evident (see table 1).

Table 1. Comparison of Joint Publications

Joint Publication (JP)	"Interagency" Instances
JP 5-0, *Joint Operation Planning*	81
JP 3-0, *Joint Operations*	20
JP 3-08, *Interorganizational Coordination during Joint Operations*	544
JP 3-60, *Joint Targeting*	5

JP 5-0 states, "Achieving national strategic objectives requires effective unified action resulting in unity of effort. This is accomplished by collaboration, synchronization, and coordination in the use of the diplomatic, informational, military, and economic instruments of national power"[2] and throughout all phases in a joint campaign. It outlines how the joint force commander should apply joint functions to joint targeting and describes how consensus building among JIIM partners is essential to meeting both national and strategic objectives. The resulting unity of effort creates a commonality of purpose between the military and the other instruments of national power.[3] JP 5-0 further describes how JIIM organizations can be involved throughout joint planning and assessment processes to ensure that command relationships, objectives, and other planning considerations are understood.[4] In turn, this enables JIIM organizations to provide timely and effective feedback and pertinent input into the planning process.

JP 3-0, *Joint Operations*, discusses the importance of synchronizing plans and operations with interagency, intergovernmental, multinational, and partner entities, but it too fails to address fully how these parties should be included in targeting or focused operations to achieve desired effects throughout a joint campaign.[5]

On the other hand, JP 3-08, *Interorganizational Coordination During Joint Operations*, provides both guidance and best practices for conducting either interorganizational or interagency coordination to achieve unity of effort and common understanding and to ensure a whole-of-government approach toward joint operations.[6] JP 3-08 explains the challenges of achieving JIIM unity of effort, but it is focused more on planning than execution.

As a result, the Joint Interagency Coordination Group (JIACG) developed a combatant commander's resource to better assist and coordinate operations. Published in 2007, the *Commander's Handbook for the Joint Interagency Coordination Group* serves as a bridging reference between the JIACG's ad hoc processes and procedures and the development of formal written doctrine.[7] It offers useful ideas to improve JIIM planning but is silent on interagency participation in targeting as a mechanism to overcome the strategic factors that might be preventing the achievement of desired outcomes. As described in this handbook, "the JIACG is a fully integrated participant on the [combatant commander's] staff with a daily focus on joint strategic planning,"[8] lacking the mechanisms inherent in the targeting process to synchronize fully interagency efforts. Current doctrine encourages military targeting to achieve military objectives with a subsequent coordination in the JIACG.

Because "many national strategic objectives require the combined and coordinated use of the diplomatic, informational, military, and economic instruments of national power supported by and coordinated with that of our multinational partners and various [intergovernmental organizations], [nongovernmental organizations], and regional security organizations,"[9] we propose updating joint targeting doctrine to include these participants. The current JP 3-60 defines *targeting* thusly:

> *Targeting systematically analyzes and prioritizes targets and matches appropriate lethal and nonlethal actions to those targets to create specific desired effects that achieve the Joint Force Commander's . . . objectives, accounting for operational requirements, capabilities, and the results of previous assessments.*[10]

While this description appears to suggest targeting as a comprehensive, systematic, and inclusive process, a closer examination of the document reveals that interagency, intergovernmental, and multinational considerations receive little attention. Instead, it mostly describes how these organizations can inform the intelligence and assessment processes the joint force commander uses when developing targeting plans. It does not illustrate how these same organizations inform the planning *and* execution of targeting operations.[11]

A further comparison within JP 3-60 provides a similar narrative regarding the terms *lethal* and *nonlethal*. The word lethal appears 30 times while nonlethal appears 41 times. Based on this simple examination of the document, one could conclude that the two activities earn roughly equal discussions, but a more thorough inspection indicates otherwise. Of the 41 nonlethal entries, 7 are about nonlethal weapons while 12 (30 percent) occur on just two pages (II-15 and II-16). JP 3-60 wisely includes examples to help commanders better understand the targeting process. However, all four examples discuss only lethal activities to attack enemy capabilities (destroying enemy air defenses; disrupting the enemy petroleum, oil, and lubrication infrastructure; defeating the enemy air force; and destroying two bridges).

Joint targeting doctrine has certainly matured over the last decade to capture the real-world experiences of commanders and staffs continuously operating jointly. However, it does not yet recognize the full potential of all the JIIM actors during conflict. The existing model's efficacy is proven and useful during Phases II and III but becomes less instructive as operations transition to Phases IV and V. Similar to Phase 0, these latter phases require even greater coordination and synchronization with interagency, intergovernmental, and multinational partners as demands for their unique capabilities grow.

A New Cognitive Model

The references above demonstrate that the joint force values building unity of effort with the military's JIIM partners; however, the doctrine does not extend to execution via the joint targeting process. The following offers an updated model for joint targeting, which all JIIM actors can easily use across the range of military operations.

Considering the numerous joint activities across the range of military operations during all phases, only a small fraction pertains to killing the enemy. Currently, however, JP 3-60 heavily emphasizes lethal employment and is disproportionately enemy-focused. Therefore, the first step to creating a more expansive cognitive model of targeting is to erase the terms lethal and nonlethal from the lexicon since they confuse analysis and encourage stovepipe thinking. Organizing the targeting staff into lethal and nonlethal cells, as is common, decreases effectiveness and efficiency because of the duality of effort and high probability that the efforts themselves could become desynchronized. Indeed, JP 3-60 implies such a staff organization, noting that, "There is typically a parallel lethal/nonlethal effort at the working group level, due to time and SME availability. In some cases, an additional [Joint Targeting Working Group] may be required to process, deconflict, and prioritize all nominated targets."[12]

Since killing is rarely the expressed intent across the range of military operations, what then is "lethal"? Joint forces often characterize security force assistance (SFA) or FID in "lethal targeting." On closer examination, neither of these joint force activities focuses primarily on the delivery of a lethal effect, but rather on how a country can protect itself from internal and external security threats. While it is true the "assistance" will instruct other security forces on how to kill, among other skills, there is little to no lethal activity occurring. In reality, most SFA and FID involves teaching logistics, command and control, and the staff functions necessary to recruit, man, train, equip, and sustain host nation security forces—hardly lethal.

This lethal/nonlethal dichotomy hinders the commander's ability to visualize the full expanse of the operating environment, creates the strong potential to overlook opportunities, and can reduce staff efficiency since, as stated earlier, staffs often organize into separate lethal and nonlethal targeting cells. This inherently decreases efficiency as it stovepipes information, creates unnecessary hindrances to information flow among staff sections, and all but eliminates synergistic effects among targeting cells. Rather, individual targeting cells focus on distinct problems and the application of distinct lethal or nonlethal activities. Instead of synchronizing efforts after the fact, we recommend a single targeting cell and single targeting approach. Such an approach is more efficient, more comprehensive, provides greater synergy, better synchronizes activities resource allocation, and organizationally requires a smaller staff.

In an ideal setting, targeting is a continuous process to assess the operating environment (OE) in order to identify strategic factors and determine the activities necessary for achieving operational objectives, develop courses of action (COA) to overcome the strategic factors, allocate resources, assign tasks, and reassess the OE to evaluate the effect of the activity or identify additional strategic factors that might provide new opportunities and/or challenges precluding the organization from achieving its desired outcomes. Since targeting should be tied to a higher headquarters plan, the commander's operational approach must inform the targeting process to bring activities to bear that transform the OE from current to desired conditions. Subsequently, targeting synchronizes

Air Force major examines patient at temporary medical site at Killick Haitian Coast Guard Base in Port-au-Prince, Haiti, during Continuing Promise 2011 (U.S. Navy/Eric C. Tretter)

the activities across JIIM organizations to achieve the intermediate military objectives or, equally important, the objectives/goals of JIIM partners beyond merely military objectives. This helps inform the development of the Commander's Critical Information Requirements, which seek to answer not only questions on the effective implementation of the operational approach but the targeting process as a whole.

Targeting is the process of addressing the strategic factors that prevent progress from current to desired conditions. The strategic factors will vary across OEs but might include challenges and opportunities such as corruption, security sector capacity, black market economies, resource scarcity, ethnic conflict, and urbanization. The targeting process synchronizes "short-term" activities to achieve the supporting objectives.

JP 5-0's "operational approach" clearly illustrates how lines of effort (LOEs) extend beyond the scope of only the military instrument of power to include, for example, education, infrastructure, and economic development. A line of effort is a conceptual category that allows an organization to unify the efforts of all participants toward a common purpose. Usually LOEs are closely related but need not be sequential in nature.[13] Hence, optimally applied targeting will best achieve synchronization of efforts when it includes all JIIM stakeholders. While ideal, we acknowledge the inherent difficulty and sensitivity in bringing multinational partners and/or host nation individuals into the process.

Organizing the Staff

Just as commanders must routinely adjust task organization to meet environmental and operational changes, they must also consider staff changes to ensure the appropriate integration of JIIM partners throughout all phases of an operation. As noted above, many joint force organizations at strategic through tactical levels have reflexively split their targeting staffs into lethal and nonlethal cells. This dubious bifurcation tends to result in stovepiped analysis and recommendations that pit the "meat-eaters" against the "leaf-eaters." Too often, this results in nonlethal plans

Chief engineer discusses power line construction with Kabul Electricity Directorate engineering liaison and U.S. State Department representative in Seh Du-kahn, Parwan Province (U.S. Navy/Tom Jones)

that are inadequately integrated with the overall plan, inadequately resourced, and inadequately executed leaving commanders and lethal staffs frustrated at the lack of nonlethal progress.

The commander should overcome this divide by organizing the staff around the various lines of effort. Because doctrine cannot anticipate every LOE for which an organization might operate, it cannot prescribe the staff organization that is optimal for every scenario. The commander or his designated representative should consider individual skills and attributes more than Service, branch, or rank. Traditional training and professional military education are often insufficient to produce the skills and attributes that yield excellence in analysis and planning along a nontraditional line of effort. Officers and senior noncommissioned officers with unique experiences or education may generate the best ideas. Indeed, each cell will require officers and senior noncommissioned officers who fully understand their targeting roles and how the process contributes to operational success. In a complex and dynamic JIIM environment, finding the right person for the right position will rely on intuition and judgment that can only be marginally informed by traditional staff structures and grade plates.

Organizing the staff into LOE cells with the right people does not guarantee the staff will overcome the stovepiping tendency. Once the correct cells have been established, they must coordinate their efforts and provide input into other working groups (WGs). Our recommended staff targeting process is designed to develop synergy across the staff to produce fully integrated operations. Additionally, this recommendation provides an institutional access point and incentive for our interagency, intergovernmental, and multinational partners to participate since it improves communication among stakeholders, provides a venue for positions to be heard, and ensures that initiatives are better conceived, integrated, and synchronized.

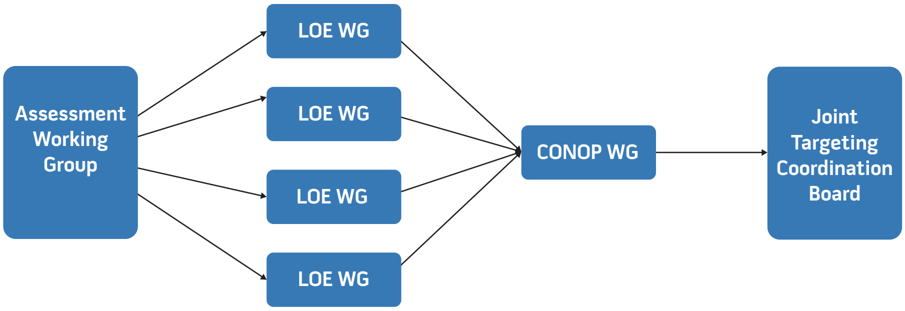
Staff Targeting Process

Physical organization of the staff is just the beginning; inevitably the people who form the staff will separate into various working groups to address the problems at hand. Figure 1 depicts a staff process that might typically lead to getting a commander's decision on recommended courses of action and/or the allocation of resources.

Working groups and boards exist in doctrine and in many headquarters to address the first two steps of the targeting process: assess the OE to identify strategic factors, and develop COAs to overcome the factors. However, little practical or applicable work is accomplished within the groups; rather, in practice, the staff sections often work independently of one another outside the respective working group meetings to identify challenges and concomitant solutions. Hence, working group meetings often become merely informational briefings. Staffs must avoid this tendency. Effective JIIM organizations will establish an environment in which the staff purposefully discusses ideas at the working groups. Effective JIIM targeting requires a battle rhythm event specifically dedicating time for the staff to focus on the OE and the targeting process. An enforced battle rhythm also provides the often less-resourced JIIM actors the necessary predictability to contribute. The resulting working group products should organize the discussion, capture and share information across the staff, and help subordinate units parallel plan and not simply brief the meeting's chairperson.

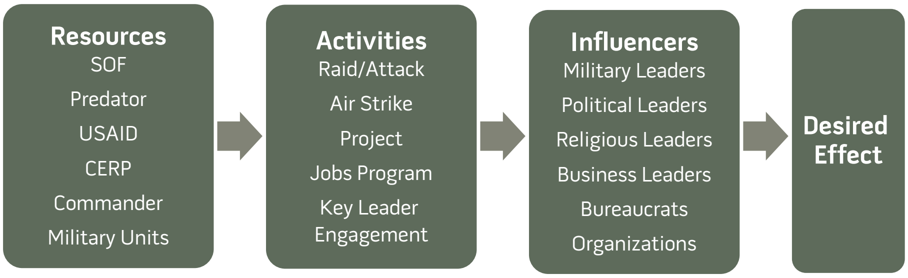
The entire targeting staff gathers to assess the effects of the previous targeting cycle's engagements and the overall OE at the start of each targeting cycle. With an agreed-upon and comprehensive assessment in hand, the LOE WGs meet to assess in more detail and develop COAs to overcome the strategic factors. The Concept of Operations WG is another gathering of the entire targeting staff in which the LOEs present their COAs to the group for consideration and input and ultimately for approval by the meeting's chair. The final Joint Targeting Coordination Board provides the commander or designee the opportunity to approve the COAs and provide guidance for the next targeting cycle. The length of targeting cycles depends on the OE and often the phase. Phase II and III cycles may only be days long while the Phase 0, IV, and V cycles may be months.

Figure 1. The Staffing Process



Key: CONOP = concept of operations; LOE = lines of effort; WG = working group

Figure 2. A New Approach to JIIM Targeting



Finally, figure 2 provides a new targeting model that works throughout the range of military operations, does not separate lethal and nonlethal, and is useful to all JIIM actors. This cognitive model is designed to help stakeholders think through options to address strategic factors throughout the continuous targeting process in order to generate comprehensive and synchronized solutions.

The steps are as follows: 1) determine the desired effect to overcome a strategic factor(s), 2) determine the resources and activities needed to achieve the effect, and 3) identify the positive and negative influencers who have a stake in both the problem and the solution. This cognitive model overcomes the inherent tendency of staffs to see only limited solutions within the lethal and nonlethal realms. Just as one can defeat an enemy cell nonlethally by removing a reason to fight, one can also strengthen governance lethally by killing or capturing those creating instability in a designated operating environment. A stovepiped organization, or an organization whose activities are synchronized after the fact, severely limits the staff's ability to identify the full scope of the problem and/or identify comprehensive solutions.

Examples of Effective JIIM Targeting

Following the joint doctrine methodology of providing examples to illustrate ideas and concepts, we offer an expansion on the two introduced at the beginning of this article. The first example is at the theater-strategic level whereby ISAF, the Afghan government, and international community employed a whole-of-government approach to synchronize Afghan counternarcotics efforts. The second is an example where this new cognitive model was successfully applied at the tactical level during a U.S. Army brigade's deployment to southern Afghanistan in 2011–2012.

In the first example, ISAF and the broader international community developed programs and policies to confront Afghanistan's opium trade. Although the approach did not formally use the targeting process explained here, the thinking involved with identifying strategic factors and courses of action to overcome them was similar.

Table 2. Afghan Poppy Cultivation and Opium Production

Year	Annual Poppy Cultivation (hectacres)	Annual Opium Production (metric tons)
2006	165	6,100
2007	193	8,200
2008	157	7,700
2009	123	6,900
2010	123	3,600
2011	131	5,800
2012	154	3,700

Source: Ian S. Livingston and Michael O'Hanlon, *Afghanistan Index* (Washington, DC: The Brookings Institution, December 13, 2012), 20, available at <www.brookings.edu/~/media/Programs/foreign%20policy/afghanistan%20index/index20121120.pdf>.

Afghanistan is the world's leading exporter of opium, an international trade economy that helps fund the insurgency. To reduce the ill effects of the drug trade, ISAF solicited the support of various JIIM actors inside and outside of Afghanistan: the joint military force, U.S. Government agencies, coalition governments, the United Nations, Afghan Ministry of Interior, and numerous Afghan provincial and district governmental agencies, to name a few.

Though ISAF's support is primarily to provide cordon security, logistic assistance, medical assets, and specialist engineers for improvised explosive device clearance, it is clear the targeting of the narcotics trade in Afghanistan is a complex task requiring both lethal and nonlethal operations in order to provide the greatest effect. As the main focus of the counternarcotics effort is to attack the drug-trafficking organizations vice the individual farmer who may be forced by the insurgents to grow poppy, discernment on exactly what part of the network is to be targeted is complex and requires the expertise of outside agencies and individuals such as the Drug Enforcement Administration, United Nations, and Afghan leaders.

The operational approach and national policies have changed several times over the past decade as stakeholders have better understood the strategic factors involved in Afghanistan's opium trade. Although the results on stemming the cultivation of poppy are mixed, there was a decrease in the number of metric tons of opium produced (see table 2) because of a JIIM approach to targeting both poppy cultivation and more importantly opium production. This approach allowed ISAF and the Afghan government to succeed as they organized for operations and targeted one of the most wicked problems in Afghanistan, characterized by vying personal economic incentives, insurgent pressures, weather, government capacity, and individual and institutional will. Had the stakeholders not used a JIIM approach, the varying intricacies of the narcotics industry would not have been fully understood, opium production would have continued unabated, and insurgent funding would have remained undiminished.

The second example concerns a brigade in Kandahar City, which is the second largest city in Afghanistan and is located along key lines of communication that run throughout the country and into Pakistan. The brigade received intelligence that a city subdistrict was a bed-down location for a high profile attack cell. There were more enemy initiated attacks in one subdistrict than in the other nine. Through the targeting process and running estimates of the situation, the staff discovered various strategic factors in the subdistrict that were contributing to instability: 1) the police were not patrolling often or not at all in the most contentious areas, 2) the subdistrict manager was not effectively connecting to his constituents, 3) Afghan government/ISAF promises for development projects were unfulfilled, and 4) unemployment was high. Further analysis by the staff and the U.S. Department of State District Support Team determined that: 1) the subdistrict police commander was related to the provincial chief of police and might have acquaintances in the attack network, 2) the manager was leery about traveling within the subdistrict as he had little to offer the people, and 3) the village elders were politically disaffected. From this analysis, the commander determined that the risk associated with maintaining the status quo coupled with the prospect that this instability might spread throughout the city was too great, and the brigade needed to reevaluate its approach to operations.

The brigade undertook a comprehensive targeting approach to improve security by resolving strategic factors that allowed the attack network to operate within the subdistrict while actively trying to remove the insurgents from the city. A series of synchronized key leader engagements from brigade to platoons occurred to address the police commander. The stability LOE cell reprioritized the brigade's project list and won Regional Command support to expedite stalled projects. The communicating LOE cell encouraged the manager to invite media representatives to the project "groundbreakings" to help inform the local people of tangible progress. The security LOE cell prioritized intelligence, surveillance, and reconnaissance as well as time-sensitive operations to focus on the enemy cell operating there.

Upon assessing the Commander's Critical Information Requirements, guided by developed measures of performance and effectiveness, the brigade discovered unintended consequences of its activities, but the comprehensive targeting process enabled it to make timely adjustments. First, the police commander accused the subdistrict manager of corruption and embezzlement. To resolve the issue, a series of battalion- and brigade-level key leader engagements influenced the police commander to either provide evidence or retract the accusations. As a result, he retracted the accusations. Second, the village elders were upset because the contractor hired workers from outside the village to build the projects, and they made a thinly veiled threat of violence to the contractor. The contractor correctly explained that the villagers lacked the necessary construction skills. Therefore, the brigade placated the elders by coordinating vocational training for the village. Due to the visible drama surrounding these projects, the subdistrict manager did not want to invite the media to the groundbreakings. The brigade did not press him on that point. While local media coverage would have been helpful, it was not necessary to overcome the identified problem and therefore not worth derailing ongoing progress. In terms of security, the police increased their patrolling, and time-sensitive operations removed some of the enemy cell leaders and motivated others to depart the area. Overcoming the impeding strategic factors in this subdistrict required 2 months of innovative targeting that did *not* include any lethal activities. No shots were fired. This targeting effort helped reduce enemy violence by almost 60 percent from summer 2011 to summer 2012.[14]

JIIM Engaging

Finally, a term other than *targeting* might be necessary to synchronize JIIM efforts. Organizations outside the military abhor it as it implies lethal activities. Nonmilitary actors sometimes go so far as to say, "We don't do targeting." A more appropriate term is *engaging*, which more broadly addresses the numerous options for overcoming strategic factors. Engaging may involve lethal force, but it more commonly involves diplomacy and development. By accepting a new term for the process, nonmilitary JIIM actors would find themselves more amenable to joining the process. Hence, the doctrinal Joint Targeting Decision Board would become the Joint Engagement Decision Board, with the JIIM stakeholders collaborating to approve courses of action to synchronize the activities to achieve desired effects. The intrepid reader will reread this piece substituting the conjugation of "to target" for "to engage" and realize that more comprehensive options are available.

Conclusions

Throughout recent history, but particularly over the last decade, incorporating JIIM organizations into the planning process has been critical to achieving national and strategic interests. To provide basic guidance, various publications and joint doctrine have evolved to incorporate JIIM organizations into the military planning process. One positive example is JP 5-0, *Joint Operation Planning*. However, the current edition of JP 3-60, *Joint Targeting*, neglects to address all the JIIM considerations required to synchronize activities to achieve desired targeting effects. To provide the requisite guidance to commanders and staff on fully examining both lethal and nonlethal activities and incorporating all of the JIIM partners, JP 3-60 needs further revising. Furthermore, recognizing that doctrine is only as effective as the people who implement it, the U.S. military should engender greater cross-organizational exposure to interagency, intergovernmental, and multinational partners to include greater integration of professional development/education programs and training exercises. This increased exposure should result in more understanding, which can become the foundation for more trust, which is a critical ingredient for more effectiveness.

America's military has an overwhelming advantage in planning and in the ability to incorporate JIIM actors into the planning process. While such collaboration is in the forefront of joint doctrine regarding planning, we fall short when planning meets execution. It is only when JIIM partners are fully synchronized in both planning *and* execution that we will realize the comprehensive effects necessary to achieve our national and strategic objectives. JFQ

Notes

[1] 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 December 15, 2012).

[2] JP 5-0, *Joint Operation Planning* (Washington, DC: Joint Chiefs of Staff, August 11, 2011), xiv.

[3] Ibid., II-8.

[4] Ibid., chapter II.

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

[6] JP 3-08, *Interorganizational Coordination During Joint Operations* (Washington, DC: The Joint Staff, June 24, 2011), I-6.

[7] U.S. Joint Forces Command, *Commander's Handbook for the Joint Interagency Coordination Group (JIACG)* (Suffolk, VA: Joint Forces Command, March 1, 2007), i.

[8] Ibid., vi.

[9] Ibid., II-1.

[10] JP 3-60, *Joint Targeting* (Washington, DC: The Joint Staff, January 31, 2013), vii.

[11] Ibid., III-19.

[12] Ibid., III-3.

[13] JP 5-0, III-15.

[14] *Report on Progress Toward Security and Stability in Afghanistan, Report to Congress* (Washington, DC: Department of Defense, December 2012), 23.

Air Force crews perform preflight checks as B-1 Lancer flies overhead during operational readiness exercise at Ellsworth Air Force Base (U.S. Air Force/Zachary Hada)

Airpower and Globalization Effects

Rethinking the Five Rings

By Michael W. Pietrucha

In 1988 Colonel John Warden, USAF, developed the "Five Rings" model, classifying a country as a system organized into five rings. Given traction in the Gulf War, the model has been a staple of airpower advocacy for two decades. The theory advocated airpower as a force that could bypass the outermost ring to achieve effects against the others, presumably with a decisive effect. But this model, which seemed perfect for Middle East autocracies, seems less applicable against modern peer competitors. What happens to the theory when the exploitable vulnerability is in another ring?

Two decades later, it seems that the interconnected web of international trade has changed the effects of certain warfighting strategies, rendering an integrated economy vulnerable to infrastructure (third ring) attacks. This target set is particularly attractive because in a globalized economy, the transport of materials and goods is a chain that lies partially outside the protection provided by the fifth ring. Nowhere is this more apparent than in the realm of maritime transportation, particularly in the Indo-Pacific region.

The implications for military strategy are profound. For the United States, it means that the force-on-force challenge of using advanced penetrating systems

Colonel Michael W. Pietrucha, USAFR, is the Individual Mobilization Augmentee to Pacific Air Forces.

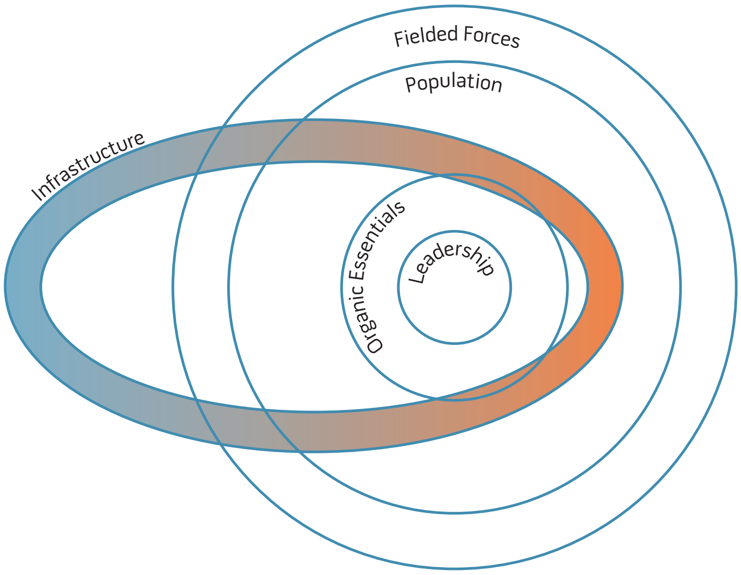
in the teeth of an advanced integrated air defense system may not be necessary. It also means that the characteristics of air forces, namely their speed, range, and flexibility, are well suited to an interdiction strategy intended to deprive a country of the materials needed to sustain day-to-day operations. It is time to reexamine the strategy assumptions that have served as the foundation for air campaign planning in the region.

Overview

With the pivot to the Pacific, the United States is staking its position as the primary exporter of Pacific stability. As a Pacific nation, it maintains a position as an explicit guarantor of freedom of access to the global commons. Accordingly, Washington faces several nations who understandably have differing foreign policy goals in a context that is rife with historical enmities, territorial disputes, and competition for resources, much like any other region of the world. The key difference lies in one overwhelming geographic factor: this region is greatly shaped by water and the lines of communication and commerce that overlay the maritime domain. Because of the geography of Asia, international road and rail links are inferior to maritime links for international transport and sometimes even for domestic movement. It might be overstating the case to assert that those transportation links are inherently fragile, but some are vulnerable to interdiction. The strategy is referred to here as *strategic interdiction*, a joint mission designed to prevent the movement of resources related to military forces or operations.

In figure 1, the Five Ring model is altered, keeping the view of a country as a system but changing the concentric structure of the rings because the transportation portion of the infrastructure has expanded globally beyond the protection of fielded forces.

Figure 1. Altered Five Ring Model



The Indo-Asia Pacific theater is largely maritime, and goods and energy travel mainly by sea. Certain countries are completely dependent on maritime traffic for international movement of economic essentials that cannot be sourced domestically. In 2011 Asia and Oceana accounted for 51 percent of the world's maritime cargoes loaded and 56 percent of the cargoes offloaded, dwarfing Europe at 19 percent and 23 percent, respectively.[1] Accordingly, any Pacific strategic interdiction will have a significant maritime interdiction component.

Relevant Air Force History

For the United States, the application of airpower against ships got off to a rocky start. Brigadier General Billy Mitchell participated in Project B in 1921, examining the effectiveness of bomber aircraft against warships. American planes sank two captured German vessels, followed by the much-heralded sinking of the battleship *Ostfriesland*. In 1923 Mitchell's bombers sank USS *Alabama*, *New Jersey*, and *Virginia*, conclusively demonstrating that aircraft could find, attack, and sink modern capital ships. Nevertheless, Pacific Fleet War Plan Orange exercises remained focused on the line of battle, failing to foresee that the airplane would define naval warfare in the Pacific.

World War II in the Pacific forever established the reach and lethality of airpower in the maritime domain as U.S. Army Air Force (USAAF) aircraft alone sank more than a million tons of shipping. Some 310 vessels (including 70 warships) went down due to the planes. Mines laid by the USAAF accounted for 257 vessels totaling 580,000 tons sunk, 36 times the number of ships sunk by mines laid by all other sources combined.[2] Navy and Marine Corps aircraft, mostly carrier-based, accounted for or assisted with another 653 ships. While submarines sank the vast majority of Japanese merchant vessels, aircraft counted for the majority of warships. Maritime interdiction was recognized as an air mission by the end of World War II.

In Korea the U.S. Navy successfully blockaded both North Korean coasts, preventing hostile naval forces from affecting the conflict. In 1972 the United States embarked on a mining campaign designed to shut off the flow of seaborne supplies to North Vietnam, totaling 80 percent of all war material and 100 percent of oil imports. The mining of Vietnamese ports, following efforts at river mining, was a key element of the endgame maneuvering that ended American participation in the war.

By 1975 the B-52 was the premier Air Force maritime interdiction asset. Capable of carrying large numbers of mines derived from Mk-82/83/84 bomb bodies, the B-52 also carried the AGM-84D Harpoon, a ship-killing weapon that could be employed against

Table. Removal of Japanese Merchant Marine by Mode of Attack

Mode of Attack	%
Submarines	54.7
Carrier-based aircraft	16.3
USAAF aircraft	10.2
Mines (mostly delivered by B-29)	9.3
Land-based Navy and Marine Corps aircraft	4.3
Naval gunfire	1
Maritime accident/mishap	4

Soviet ships from standoff positions. The B-52 remains the primary aerial minelayer, supplemented today by the B-1B and B-2A, although its standoff antiship missile capabilities have atrophied. With the focus on Iraq and Afghanistan, there was no constituency for retaining antiship weapons, and the capability of employing the Harpoon was allowed to slip away.

Case Study: Japan in World War II

The effects of interdiction were illustrated in the Pacific during World War II. Japan entered the conflict with in excess of 6 million tons of shipping over 500 tons displacement; another 4.1 million tons were built, captured, or otherwise taken into service.[3] Japan's Merchant Marine was *the* essential support pillar for its industry and for supporting the conquest of the Western Pacific.

Occupied Manchuria and China helped supply raw materials over short distances, namely coking coal, iron ore, foodstuffs, and salt. Unfortunately, oil, rubber, bauxite, and manganese were no closer than the Dutch East Indies and the United States. In 1941 the Japanese had stockpiled a 7-month supply of bauxite and 43 million barrels of oil, which turned out to be grossly insufficient:[4]

> *Japan's merchant shipping fleet was not only a key link in the logistical support of her armed forces in the field, but also a vital link in her economic structure. It was the sole element of this basic structure which was vulnerable to direct attack throughout a major portion of the war.*[5]

The U.S. campaign against Japanese shipping began 6 hours after Pearl Harbor when the Chief of Naval Operations authorized unrestricted submarine warfare, making the submarine initiative the only interdiction effort lasting the entire war. Carrier- and land-based aircraft pitched in soon after. In the Southwest Pacific, interdiction of Japanese naval supply lines was *the* primary mission for the bomber force, and General George Kenney's 5th Air Force developed light bombers as "commerce destroyer" aircraft, introducing skip bombing to the USAAF. This proved decisive in the Battle of the Bismarck Sea, when land-based airpower decimated a major troop convoy headed for New Guinea, losing merely four aircraft.

Called "starvation" missions, aerial mining of Japanese home waters commenced in March 1945 and was directed at the Shimonoseki Strait, the key remaining chokepoint in the Japanese maritime supply network.[6] The effort pinned down warships and merchant vessels of all sizes. Despite the short duration, aerial mining accounted for almost as many ships damaged as all USAAF land-based air during the entire war:

> *The 313th Wing got into the game late, operating with mines for only four and one-half months and at a period when the enemy's merchant fleet had contracted in size and in scope of its activities. During that short period, mines planted by the wing were more destructive than any other weapon, accounting for about half of the total tonnage disposed of. To accomplish this task, the 313th sent out 1,528 sorties and planted 12,053 mines, a much heavier effort than had been suggested by the Navy in the negotiations of 1944 and, indeed, the heaviest aerial mining campaign ever waged.*[7]

Japan's diversion of its Merchant Marine to support military operations, when combined with interdiction efforts, had a staggering effect on the Japanese economy as early as 1942, when submarine attacks forced the Japanese to resort to convoys. After September 1943, 72 percent of the petroleum shipped from the southern regions was interdicted, and the average rose to 91 percent after June 1944. In 1945 not a single ton of sugar or raw rubber got through.[8] Japanese positions across the Pacific were abandoned as the garrisons could neither be supplied nor evacuated. The effects of isolating the enemy maritime effort into small, disconnected bubbles deprived the Japanese navy of effective interior lines and the air force of the ability to patrol and defend. The strategic bombing campaign may have been the icing on the cake. The postwar Airpower Survey recognized as much:

> *It is the opinion of the Survey that by August 1945, even without direct air attack on her cities and industries, the over-all level of Japanese war production would have declined below the peak levels of 1944 by 40 to 50 percent solely as a result of the interdiction of overseas imports.*[9]

Of the total "large" (< 500 tons) Japanese Merchant Marine referenced earlier, 8.9 million tons were sunk or removed from use by the end of the War, as seen in the table.

Key Lessons

Four key lessons from World War II in the Pacific are applicable today:

- Maritime interdiction not only affects supplies coming *to* an adversary but it also affects export and power projection. Imperial Japanese garrisons on Pacific islands were isolated while the forces on the Chinese mainland and Korea were not.
- The approach was an asymmetric strategy for Washington both financially and operationally. The United States was immune to a reciprocal campaign, and the resources employed dwarfed the resources destroyed.[10]

- The vast majority of the interdiction efforts occurred outside the effective range of Japanese defenses. Typically, only the destination ports can be defended, and even escorted vessels travel a long, dangerous path to get there.
- This form of warfare is effective against an industrialized nation and the potential effects will be felt soonest by a well-integrated economy.

Pacific nations, unlike those in North America and Europe, are vulnerable to the disruption of maritime traffic and less able to guarantee favorable conditions on the high seas.

Current Implications

The geographic complexity of the Western Pacific is of key importance. Shipping routes to East Asia are constrained and long archipelagos provide a barrier to sea transportation even under ideal conditions. Like the Suez and Panama canals, the Malacca Straits are a limited capacity passage through otherwise impassible terrain that can be effectively interdicted. Alternative routes add time and distance, with additional complications. Deep-draft vessels that cannot pass through Malacca must pass sequentially through the Lombok Strait, Makassar Strait, Sibutu Passage, and Mindoro Strait, a route of 1,300 nautical miles from south to north. With these passages subject to interdiction, the only alternative is to swing around New Guinea and east of the Philippines. From the east, the vast majority of Asia-bound shipping passes between the Aleutians and Hawaii and must pass through the first or second island chains.

For the United States, these conditions are a blueprint for a strategy that can both serve as an effective deterrent and as a means to coerce an aggressor should deterrence fail. While the likelihood of a U.S. conflict with the People's Republic of China (PRC) seems remote, China provides fertile ground for comparison to Imperial Japan. The country is heavily industrialized, has a large and productive population, maintains a rough technological parity with its Western counterparts, and maintains a significant maritime presence. It has a modernized military with some limited ability to project power. Unlike Japan, it is a major land power and produces more of its own requirements for raw materials, fuels, and food.

The vast majority of seaborne imports come from well outside the capability of the People's Liberation Army or People's Liberation Army Navy to effectively project power. Unlike Japan and South Korea, which could reasonably expect to maintain northern supply routes to Alaska against Chinese opposition, the Chinese have no such geographical advantage or supporting alliance structure. The country imports a massive amount of raw materials by sea, most notably bauxite and iron ore, which drive heavy manufacturing. China is also a major energy importer, which opens up a significant vulnerability.

USS *Fitzgerald* and USS *McCampbell* maneuver with People's Liberation Army Navy destroyer *Guangzhou* off coast of North Sulawesi, Indonesia (U.S. Navy/Ian Schoeneber)

Energy: The Sixth Ring—Sort Of

Returning to the Five Rings model, it is obvious that it is simple and changes by country. Some countries may not have a second ring worth mentioning, the third ring may be rudimentary, the fifth ring irregular, and the first ring tribal or fragmentary. There may be significant overlaps between rings or ring relationships that blend. As shown earlier, a globalized country could have an oval third ring crossing outside the protection of the outer ring. For an industrialized nation, energy may be a sixth element in the model. The original Five Rings model considered energy and fuel as a second ring "organic essential." Here, the sixth ring is really the energy production of a modern country including electrical and motive power and the fuel and infrastructure required to extract, transport, refine, and burn it. Instead the modified model steals energy from the second ring and transmission infrastructure from the third ring, combining them into a single item and spreading it out. Since it is not really a ring at all, it becomes a connecting layer—the glue that both holds the individual rings together and makes enduring connections among the rings (see figure 2).

There is one more change to the model, intended to represent the power projection capability of the fielded forces.

Figure 2. Sixth Ring as Energy Production

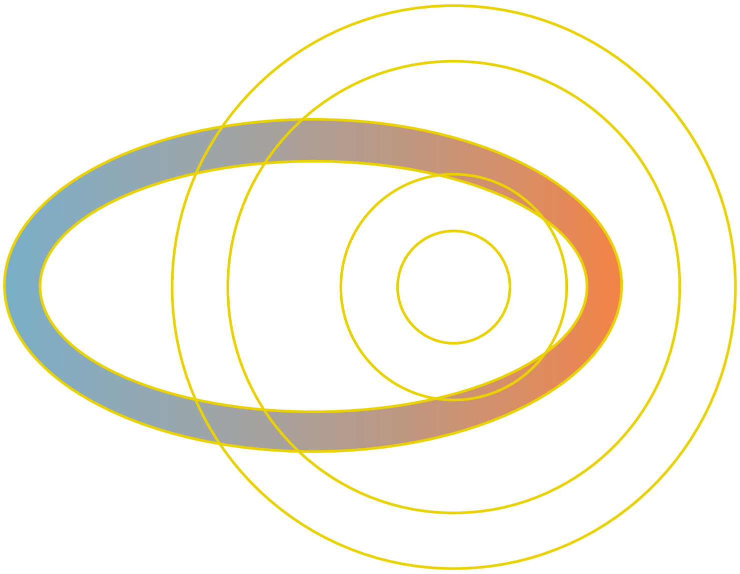
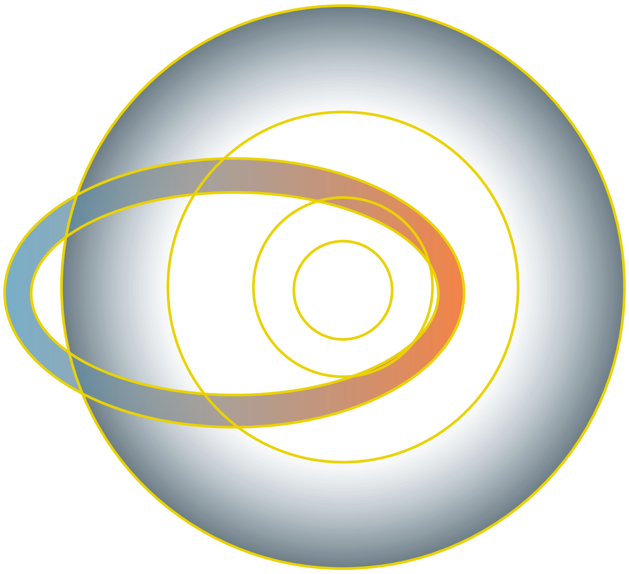


Figure 3. Power Projection Capability of Fielded Forces



Here, the outermost ring becomes like a planetary atmosphere, thinning out the farther away it gets and illustrating the difficulty of applying military power at a distance (see figure 3).

Consumption and distribution of energy change during wartime. While each of the rings is also affected by a transition from peacetime to war, the shift in energy usage by a modern military is substantial and literally instantaneous. While transportation is the foundation for shifting forces internally, energy is the major limiting factor for force projection. In the event of a conflict, the energy ring is likely disrupted from its peacetime state even if it is a planned disruption. A country's energy production and distribution, moved from their steady state, are vulnerable to further disruption by a prepared adversary.

Case Study II: PRC

China is the single largest consumer of energy in the world, deriving energy production from a number of sources, and a net importer of fossil fuels. The combination of its large size, high consumption, and limited energy related infrastructure makes the PRC an excellent case study.

Coal. Coal accounts for roughly 70 percent of China's total energy production and 65 percent of its electricity production.[11] The PRC is the world's largest producer of coal and its largest consumer, relying on imported coal for 7 percent of its energy requirements in 2012.[12] Steam coal is used for power generation and coking coal for industrial processes. Well over three-quarters of the energy produced goes to support commercial enterprises, especially industry. Some 70 percent of China's coal reserves and the majority of actual coal production are located in Shanxi Province, Shaanxi Province, and Inner Mongolia. Coal consumption is concentrated along the eastern and southern coastlines in the areas of highest population density. Thus, coal must be moved relatively long distances by road, rail, and both inland and coastal waters for a distance that has been steadily increasing even as the capacity to transport it has grown.[13]

Coal Transportation. Around 2005, the capacity of the railway system to move coal was exceeded, and the demand for coal transport has surpassed even new rail construction, and this condition is unlikely to change. In contrast to the capacity-limited rail lines, port capacity to handle coal has grown markedly. China currently has 24 coal terminals for offloading and loading coal. Most are adjacent to rail facilities, indicating that even coal shipped over water relies on rail transport at both ends.[14]

Over the past decade, Chinese coal movements shifted from a rail-only enterprise until more than a third of the country's domestic coal was transported via water for some of its route in 2010. Coal consumed in the northern coastal areas is supplied by a network of truck routes and railways, a method that is both insufficient and prohibitively expensive for serving the southeast. Instead rail lines move the coal to ports such as Qinhuangdao, Huanghua, and Rizao

Office of Naval Research head of C4ISR explains suite of information technology tools (U.S. Navy/ John Williams)

for transport by sea.[15] The rail lines are the main method for moving coal from Shanxi and Shaanxi provinces, and all 15 that cross provincial boundaries to the east and south rely on tunnels to get through the mountains. Accordingly, each line can be interdicted at a single point.

Most of the coastal traffic originates in the north and travels south from the Bohai Sea. This flow shows a steady increase and will continue to climb because the railways have little ability to add coal-carrying capacity.[16] Riverine transport is also growing, particularly along the Yangtze. Road transport is inefficient and equally subject to transportation bottlenecks. Coal shortages have become common since 2008, not for lack of coal but because it could not be moved where it was needed. For the foreseeable future, China's land-based coal distribution network will routinely operate at full capacity, magnifying the effect of any disruption. Notably, much of China's railroad transport is electric, which relies on energy produced by coal, which must be moved by the railways.

Oil. As coal drives electricity production, oil drives transportation. The two are not interchangeable. Coal cannot be used for transport, and oil only provides 19 percent of China's electricity production. The PRC is the second largest consumer and importer of oil, behind the United States, and its share is increasing rapidly, accounting for almost 40 percent of the worldwide growth in oil demand. In 2011 it imported over 5 million barrels of crude oil per day, accounting for 54 percent of its total demand. Only 10 percent of oil imports came overland[17] while more than 50 percent came from the Middle East. Half of China's total oil consumption comes by sea. There are only two oil pipelines for importing crude oil, one stretching through Siberia and terminating at the Daquing refinery and the other extending from the Caspian Sea coast in Kazakhstan to the refinery in Dushanzi. The total pipeline flow is roughly 800,000 barrels a day (bbl/day).

China is making an effort to establish a strategic petroleum reserve. In 2010 it had a commercial storage capacity of between 170 and 310 million barrels but no national strategic reserve. The 10th 5-Year Plan (2000–2005) marked the beginning of the government strategic petroleum reserve (SPR) program, planned in three phases. Phase 1 established a capacity of 103 million barrels at four sites; phase 2 (wrapping up) should expand that capacity to 315 million barrels at eight locations; phase 3, to be completed in 2020, should bring the SPR capacity to half a billion barrels. The SPR is for crude oil and not refined products, which are entirely reliant on a commercial storage capacity estimated at 400 million barrels for all types of refined fuel combined.[18]

Crude oil must be refined before it can be burned, and China does not have the domestic refinery capacity for its refined fuel requirements. For example, the PRC does not refine jet fuel domestically in sufficient quantities. In 2010 it produced 261,000 bbl/day while consuming 348,000 bbl/day, an imbalance that has steadily worsened since 2004.[19] In the past decade Beijing has undertaken an ambitious effort to increase refining activity. While capacity will increase to about 14 million bbl/day by 2015 (from < 6 million bbl/day in 2000), refinery operations are being consolidated into fewer refineries of much greater size.[20] Wartime jet fuel demand will rise well above peacetime levels even if civilian consumption is much reduced.

Oil Terminals. China has many ports including 7 of the 10 largest in the world.[21] Both oil and coal require highly specialized offloading and storage facilities, and China's oil import data from 2010 shows that of its top 20 oil terminals, 10 are large (offloading more than 20 million tons a year) and 10 are medium (offloading 8–20 million tons a year).[22] Only two of the large and four of the medium oil terminals are adjacent to the South China Sea. Those ports accounted for only 20 percent of the total offload; the vast majority of this oil was offloaded in the ports that are farthest up the coast. The major terminals at Nanjing and Shanghai and the medium terminals of Yangpu and Nantong are all Yangtze River terminals, together accounting for 14 percent of the 2010 offload from the terminals.

Energy Vulnerability and Strategic Interdiction. The vulnerability of a large industrialized economy to energy disruption is inarguable, but a strategic interdiction campaign will not be quick or easy. Targeting the sixth ring would take a campaign-level effort against a widely distributed target set. It is the wide distribution that makes this a particularly difficult problem for a defender; thousands of miles of pipelines, railways, and sea lanes cannot all be defended by surface-based air defense systems. Similarly, coastal facilities are not deep inside defended airspace and are among the most exposed and fragile elements of a country's infrastructure. The flammability of petroleum storage and refining poses difficulty even in peacetime. Refineries are also subject to single points of failure due to the nature of the refining process.

The conduct of a strategic interdiction campaign requires a modern military but puts a premium on the overall breadth of joint capabilities rather than a niche force designed to penetrate the worst of the air defenses. Instead it is a strategy intended to deter an enemy by posing a viable threat to critical parts of a national industrial machine that cannot easily be defended. It is essentially an indirect approach that avoids the necessity of penetrating enemy ground-based air defense and renders such an investment inherently less valuable.

The nature of the campaign can also be affected by an alliance structure and by the strategic depth of the competing sides. In this context, island bases too far away to employ aircraft against a mainland adversary serve well against distant vessels within the transportation network. Basing facilities on national territory or the territory of allied nations provides launch points for aerial surveillance, support facilities for naval vessels, and key nodes in a "web" designed to prevent certain types of vessels bound for an opposing nation from reaching their destinations.

A strategic interdiction campaign might have four elements:

- A *counterforce* strategy can be designed to attrit adversary naval forces (gray hulls) to the point where they can neither project military power nor defend against U.S. power projection.
- An *inshore* element can consist of operations to deny effective use of home waters including rivers and coastal waters.
- An *infrastructure degradation* plan could disrupt or destroy specific coastal capabilities such as oil terminals, refineries, repair facilities, locks, naval bases, and loading facilities that are directly supportive of, or replacements for, adversary maritime capabilities. Not to be overlooked in this category are overland oil pipelines and rail lines.
- A *distant* anticommerce strategy could occur out of effective adversary military reach. Such a strategy might not be lethally oriented, but rather directed toward the seizure and possible internment of national-flag vessels.

A counterforce strategy might be more accurately described as a strategy to counter adversary power projection. The air defense capabilities of modern surface combatants combined with the increasing capabilities of many a submarine force will make this a battle for capable joint and combined forces. That will require a robust and effective submarine force along with an Air Force contribution that includes combat aircraft that can detect, identify, and engage vessels from standoff ranges. Removal of even a limited blue-water threat will prevent effective use of escorted convoys and remove a reciprocal counterforce strategy from the table.

An inshore strategy is extremely difficult to execute because it is conducted within reach of hostile air defenses. The use of low-observable platforms is a key enabler for this part of the strategy, and some elements of an inshore strategy cannot credibly be contemplated without penetrating air defenses one way or another. However, the payoff is worth the risk because the effects ripple out through the target country. An inshore strategy might be enhanced by the use of air or subsurface-laid minefields in areas of the coast with high volumes of maritime traffic. Mining has massive effects on seaborne movement even when no mines are actually present; merely fear of mines is an effective deterrent to movement. Given China's riverine geography, river mining could be equally effective, if harder to accomplish. In the event that a large mine actually sinks a vessel in a shipping channel, clearing the channel becomes a very difficult endeavor. We should also not forget another set of lessons from Operation *Allied Force*: bridges dropped in major rivers are dual-purpose barriers; they both break roads or railways and block channels.

Attacks on maritime and supporting infrastructure might be conducted to further limit port capacity and reduce the ability of the adversary to turn to alternatives (however limited). Oil pipelines are effectively impossible to protect because of their length, and they typically cross the borders in areas that are undefended except by air. It is this kind of environment for which the B-2 or LRS-B might have been designed. Coal-loading facilities would be lucrative targets that might severely impede power generation in the short term while leaving the actual power generation facilities undamaged.

Last, the distant strategy is one intended to interdict energy at points far closer to the origin than the destination. It would include attack against oil pipelines and remote railway chokepoints but would focus on the maritime elements of the transportation network. The distant strategy can be conducted by a mix of forces far from hostile shores. Nations may do no more than enforce their traditional rights as neutrals and still impose an effective penalty by denying coastal routes that might ordinarily be open. Furthermore, this element of the strategy can be nonlethal; vessels can be interned rather than sunk. Internment of vessels takes those ships and crews off the seas as surely as sinking them, with the added advantages that internment can be reversed and no ecological threat is posed by an interned supertanker.

Final Thoughts

The Five Rings are classic airpower theory, highlighting the ability to overfly the outer rings to gain effects leading to a (presumed) short and decisive war. To assume that such a strategy could be conducted against a major industrial power is to ignore the 1999 example of *Allied Force* and the development of advanced air defense capabilities. In *Desert Storm* the technological advantages accrued to the attacker, while the pace of technological development in the wake of the U.S. victory now favors the defender. Despite that, the Air Force remains fixed in the belief that "the stealth fighter will always get through."

Even if true, any expectation that a repeat of the *Desert Storm* model would provide a quick victory should be dropped against a modern industrialized nation. Potential adversaries, bolstered by a great deal of research and development in Russia and China, have gone to great pains to prevent a recurrence, assisted by their own geography. *Allied Force* was conducted against a small country and matched a 1999 North Atlantic Treaty Organization air force against a 1969 air defense system. It lasted 78 days and took more than 38,000 sorties, a quarter of which were strike sorties, servicing a mere 421 fixed targets. The operation was conducted with minimal air opposition from the other side of the Adriatic Sea, bringing into question the idea that a similar broad application of destructive force can have a decisive effect in a large country.

A strategic interdiction strategy is intended to address operations against large, modern countries with advanced air defense systems, but it does not rely on deep penetration into defended airspace from distant bases, a significant force structure, and a design challenge that may be insurmountable. Instead it relies on the use of capable air and naval forces to affect the parts of a country "system" that are both the most exposed and the most critical for the functioning of the system. The strategy has wide applicability for a variety of crisis conditions and is well suited to an escalatory response because it contains several options that are both nonlethal and reversible. Finally, elements of the strategy can be conducted on short notice with limited forces and undertaken from substantial distances.

The implementation of an effective, obvious strategic interdiction strategy is well suited to the U.S. Pacific Command area of responsibility and should be a Department of Defense priority. It is a historically proven model of an effective strategy that has paid dividends for the United States in the Pacific before, requires no major investment in weapons systems, and can be conducted from long distances to significant effect. It is tailor made for achieving countrywide coercive effects against an industrialized country that is dependent on maritime trade. Perhaps best of all, it is a cost-imposing strategy for Washington to undertake against an adversary, for it pits U.S. strengths against adversary vulnerabilities in an arena where the adversary's ability to project sufficient power to prevent it is limited. **JFQ**

Notes

[1] United Nations, *Review of Maritime Transport 2011*, Report by the United Nations Conference on Trade and Development secretariat, New York and Geneva, 2011, available at <http://unctad.org/en/docs/rmt2011_en.pdf>.

[2] Joint Army-Navy Assessment Committee, *Japanese Naval and Merchant Shipping Losses During World War II by All Causes*, *Summaries*, table II, available at <www.history.navy.mil/library/online/japaneseshiploss.htm#pagevi>.

[3] Secretary of War, *United States Strategic Bombing Survey, Summary Report (Pacific War)*, "Summary Report" (Washington, DC: U.S. Government Printing Office, July 1, 1946), 12, available at <www.anesi.com/ussbs01.htm>.

[4] Ibid., 14.

[5] Ibid., 13.

[6] Wesley Frank Craven and James Lea Cate, eds., *The Army Air Forces in World War II, Volume Five, The Pacific: Matterhorn to Nagasaki, June 1944 to August 1945* (Washington, DC: Office of Air Force History, 1983), available at <www.afhso.af.mil/shared/media/document/AFD-101105-012.pdf>.

[7] Ibid.

[8] Ibid.

[9] *United States Strategic Bombing Survey,* 15.

[10] In a monograph titled *Results of the American Pacific Submarine Campaign of WWII*, Michel T. Poirier calculated that the Japanese spent $42 for antisubmarine warfare for every dollar the U.S. Navy spent and still suffered catastrophic defeat in this arena; available at <www.navy.mil/navydata/cno/n87/history/pac-campaign.html#N_8_>.

[11] U.S. Energy Information Administration, *China 2012* (Washington, DC: U.S. Energy Information Administration, 2012).

[12] "China's coal imports to maintain growth in 2013," Xinhua News Agency, December 24, 2012, available at <www.chinadaily.com.cn/business/2012-12/24/content_16056988.htm>.

[13] Kevin Jianjun Tu and Sabine Johnson-Reiser, *Understanding China's Rising Coal Imports* (Washington, DC: Carnegie Endowment for International Peace, 2012), available at <http://carnegieendowment.org/2012/02/16/understanding-china-s-rising-coal-imports/9ooh>.

[14] Freeman Spogli Institute for International Studies, *Industrial Organization of the Chinese Coal Industry* (Stanford: Stanford University Press, July 22, 2011).

[15] Richard K. Morse and Gang He, *The World's Greatest Coal Arbitrage: China's Coal Import Behavior and Implications for the Global Coal Market* (Stanford: Stanford University Press, August 2010).

[16] *Understanding China's Rising Coal Imports.*

[17] Zhou Peng, *China's Energy Import Dependency: Status and Strategies*, College of Economics and Management & Research Center for Soft Energy Science, Nanjing University of Aeronautics and Astronautics, 2011, available at <www.esi.nus.edu.sg/docs/event/zhou-peng.pdf>.

[18] Available at <www.eia.gov/countries/cab.cfm?fips=CH>.

[19] Available at <www.indexmundi.com/energy.aspx?country=cn&product=jet-fuel&graph=production+consumption>.

[20] Available at <www.eia.gov/countries/cab.cfm?fips=CH>.

[21] Measured in 20-foot equivalent units of cargo handling capacity, available at <www.marineinsight.com/marine/top-10-biggest-ports-in-the-world-in-2011/>.

[22] Data compiled by investment report, *The Chinese Oil Sector*, available at <www.port-investor.com/wp-content/uploads/2012/03/The-Chinese-Oil-Port-Sector.pdf>.

Statue of Sun Tzu in Yurihama, Tottori, Japan

Sun Tzu in Contemporary Chinese Strategy

By Fumio Ota

Dr. Fumio Ota, Vice Admiral (Ret.), Japan Maritime Self-Defense Force, was the Director of the Defense Intelligence Headquarters in the Japan Defense Agency. He is a graduate of the Industrial College of the Armed Forces and received his Ph.D. from the School of Advanced International Studies at The Johns Hopkins University.

Sun Tzu wrote 2,500 years ago during an agricultural age but has remained relevant through both the industrial and information ages. When we think about security, Japan's greatest strategic concern is China, and we cannot discuss Chinese strategy without first discussing Sun Tzu. In this article, I demonstrate how contemporary Chinese strategists apply the teachings of Sun Tzu and his seminal *The Art of War*.[1]

Why Sun Tzu?

Europe first discovered Sun Tzu during the late 18th century. Wilhelm II, the emperor of Germany, supposedly stated, "I wish I could have read Sun Tzu before World War I." General Douglas MacArthur once stated that he always kept Sun Tzu's *The Art of War* and Walt Whitman's *Leaves of Grass* on his desk. At the end of the Cold War, the United States borrowed from Sun Tzu when it created "competitive strategy," which aimed to attack the Soviets' weaknesses with American strengths.[2] This is exactly Sun Tzu's meaning when he said an "Army avoids strength and strikes weakness." I have also heard that this idea is referred to as a "net assessment" strategy in the Pentagon.

When I was a student at the National Defense University in Washington, DC, I studied Caspar Weinberger's "six tests." When I first considered his tests I immediately thought, "This is the teaching of Sun Tzu." Let us consider Weinberger's six tests and the comparable ideas found in *The Art of War* (see table).

General Colin Powell added a few tests of his own with the so-called Powell Doctrine, and his tests also have comparable passages in Sun Tzu. For instance, Powell's questions "Is there a plausible exit strategy to avoid endless entanglement?" and "Have risks and costs been fully and frankly analyzed?" are similarly mentioned in chapter 2 of *The Art of War*.

Contemporary Chinese Strategy

In 2001 I had some conversations with General Xiong Guankai, deputy chief of staff in Beijing. When I offered a phrase from Sun Tzu in conversation, the general recited the *whole* passage in Sun Tzu. I also visited the People's Liberation Army (PLA) National Defense University (PLANDU), the highest educational institute for the Chinese military, and asked the vice president how PLANDU teaches Sun Tzu. He answered that the ancient strategist is the centerpiece of the curriculum. According to the Chinese Information Bureau in 2006, the PLA decided to use *The Art of War* as the educational textbook not only for officers but also for all enlisted soldiers and sailors.

When I was invited by the PLA University of Science and Technology (PLAUST) to the Symposium for Presidents of Military Institutions in October 2011, I spoke to the president of PLAUST during the symposium. Whenever I mentioned a phrase from Sun Tzu's writing, he too responded with the entire passage. He had memorized the strategist's work.

I also had an opportunity to visit the PLA Army Command Academy in Nanjing where the academy's motto from a passage in chapter 5 of *The Art of War* appears on the library wall: "Use the normal force to engage; use the extraordinary to win." An American scholar pointed out that the Chinese concept of cyber attack is based on that phrase.[3] There were other framed phrases from Sun Tzu in the library: "All warfare is based on deception," and "There are strategist's keys to victory. It is not possible to discuss them beforehand."

A phrase of Deng Xiaoping's 24-Character Plan ("Hide our capabilities and bide our time"), which was a central tenant of Chinese strategy since the Tiananmen Square incident in 1989, is derived from Jiang Ziya's *The Six Secret Teachings on the Way of Strategy*, one of China's seven military classics. Some of Mao Zedong's characteristics of strategic secrets, such as "When an enemy advances, we will retreat," "When an enemy stays, we will disturb them," "When an enemy is tired, we will strike them," and "When an enemy retreats, we will chase them" are very similar to Sun Tzu's "When he concentrates, prepare against him; where he is strong, avoid him. Attack where he is unprepared; sally out when he does not expect you" (*The Art of War*, chapter 1).

Table.

Weinberger's "Six Tests"	Passages from Sun Tzu's *The Art of War*
The United States should not commit forces to combat overseas unless the particular engagement or occasion is deemed vital to our national interest or that of our allies.	"War is a matter of vital importance to the State; the province of life or death; the road to survival or ruin" (chapter 1).
If we decide it is necessary to put combat troops into a given situation, we should do so wholeheartedly, and with the clear intention of winning.	"A victorious army wins its victories before seeking battle; an army destined to defeat fights in the hope of winning" (chapter 4).
If we do decide to commit forces to combat overseas, we should have clearly defined political and military objectives.	"Now to win battles and take your objectives, but to fail to exploit these achievements is ominous and may be described as wasteful delay" (chapter 12).
The relationship between our objectives and the forces we have committed—their size, composition, and disposition—must be continually reassessed and adjusted if necessary.	
Before we commit combat forces abroad, there must be some reasonable assurance we will have the support of the American people and their elected representatives in Congress.	"The people [must] be in harmony with their leaders, so that they will accompany them in life and unto death without fear of moral peril" (chapter 1).
The commitment of forces to combat should be a last resort.	

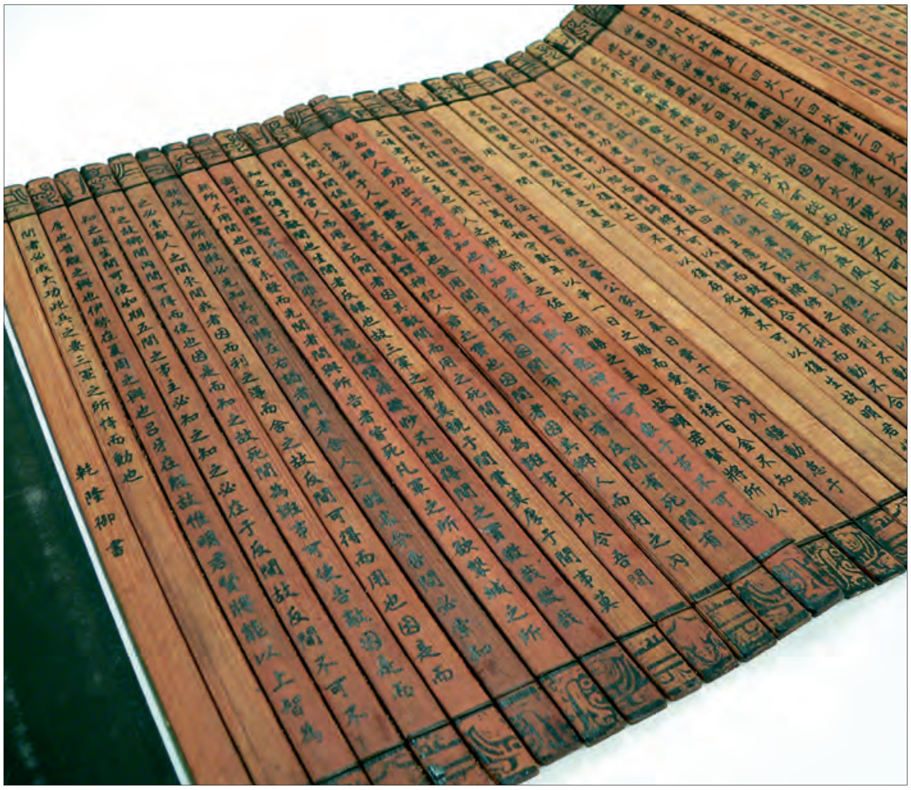
Since all Chinese military personnel seem to memorize Sun Tzu, it is possible that Chinese strategy is based on *The Art of War*. All Central Military Commission members except Xi Jinping are generals and admirals who have memorized his work completely. Even though PLA weapons and tactics are not as sophisticated as those of the major Western powers, this comprehensive strategy—which includes nonmilitary means—is clever, and we must understand how China has adopted Sun Tzu for its contemporary strategy.

What is Chinese contemporary strategy? It is not necessarily revealed in *China's National Defense*, which is published every 2 years. In the preface we read, "China will never seek hegemony."[4] According to reports by the Center for Strategic and Budgetary Assessments and RAND, by 2020 China will be well on its way to having the means to achieve its first–island chain policy. In May 2013 Chinese newspapers discussed possession of Okinawa. In 2012 a PLA think tank, the Military Science Academy, advocated a "strong military strategy" that insists that the PLA Navy must protect national interests west of 165 East and north of 35 South. On its maps, China portrays a three-line configuration that includes the Hawaiian Islands as the third–island chain.

In 2012 a Chinese delegation insisted on Hawaiian sovereignty to Secretary of State Hillary Clinton. Admiral Timothy Keating, commander of U.S. Pacific Command, was approached in 2007 by a Chinese admiral who advocated dividing the Pacific. Due to the declaration that "China will never seek hegemony," Chinese strategy is clearly deceptive. We have to look at their real intentions. The latest *China's National Defense* emphasizes "rapid assaults."[5] *Military and Security Developments Involving the People's Republic of China 2013* also states that the "PRC continues to pursue [the ability] to fight and win short duration [conflicts]."[6] This is contextually similar to "while we have heard of blundering swiftness in war, we have not yet seen a clever operation that was prolonged," which is found in chapter 2 of *The Art of War*.

"Three Warfares"

In 2003 the Chinese Communist Party Central Committee and the Central Military Commission endorsed the "three warfares" concept, reflecting China's recognition that as a global



Chinese bamboo copy of *The Art of War* with cover inscription suggesting it was either commissioned or transcribed by Qianlong Emperor (UC Riverside)

actor it would benefit from learning to use the tools of public opinion, particularly during the early stages of a crisis, as these tools have a tendency to bolster one another.[7] The PLA issued 100 examples each for psychological, media, and legal warfare. Psychological warfare examples cited Sun Tzu 30 times, media warfare examples cited him 6 times, and legal warfare examples cited him 3 times. The most cited phrase (from chapter 3) is "To subdue the enemy without fighting is the acme of skill," which appears 10 times. The next most repeated phrase (from chapter 1) is "All warfare is based on deception," appearing half a dozen times.

The *PLA Daily* reported that when 10 warships, including 2 *Kilo*-class submarines, passed through the Miyako Strait, they were to conduct exercises in the spirit of the three warfares concept. As it is not possible to conduct media and legal warfare as part of a naval exercise, we should understand that they conducted psychological warfare with the goals of the deterrence, shock, and demoralization of Japan.

Chinese leaders typically mention ideas such as "Chinese Military Buildup No Threat to the World" (Defense Minister Liang Guanglie's statement in November 2012), or "Peaceful Development" (*China's National Defense*), or "Harmonious Ocean" (the theme of the PLA Navy's multinational naval event in 2009). All of these are examples of media warfare or, in other words, propaganda. On March 8, 2013, the *People's Daily* reported that the sovereignty of the Ryukyu Islands is historically pending and not yet determined. This is still another example of media warfare. To Beijing, the Ryukyu Islands must represent "key ground, ground equally advantageous for the enemy or me to occupy" (chapter 11, *The Art of War*) because the North and East Sea Fleets can pass through the area into the Pacific with impunity. However, as Sun Tzu stated, "Do not attack an enemy who occupies key ground." China has instead supported Okinawa's independence activities, which were developed by pro-Chinese Okinawans and probably Chinese secret agents as well.

Moreover, Beijing has legislated many internal maritime laws to justify its maritime activities including:

- Law of the People's Republic of China Concerning the Territorial Sea and the Contiguous Zone (1992)
- Proclamation of Territorial Base Line (1996)
- Public Relation Marine Science Research Administrative Regulation (1996)
- Law of the People's Republic of China on the Exclusive Economic Zone and the Continental Shelf (1998)
- Marine Environment Protection Law of the People's Republic of China (1999)
- Law of the People's Republic of China on the Administration of the Use of Sea Areas (2001)
- Desert Island Protection Usage Administrative Regulation (2003)
- Law of the People's Republic of China on Island Protection (2009)
- National Mobilization Law (2010)
- Maritime Observation Forecast Administrative Regulations (2012).

Disintegration Warfare

The PLA International Relations Academy in Nanjing studied disintegration warfare from 2003 to 2009. Then in 2010 a PLA publisher issued *Disintegration Warfare*. A passage from chapter 3 of *The Art of War*, "To subdue the enemy without fighting is the acme of skill," appears on the cover of *Disintegration Warfare*. The idea of disintegration warfare includes politics, economy, culture, psychology, military threats, conspiracy, media propaganda, law, information, and intelligence. All these concepts are clearly building on Sun Tzu's ideas of deception, disruption, and subduing the enemy without fighting.

In 2012, for the first time since its establishment, the Minister of Foreign Affairs Conference of the Association of Southeast Asian Nations (ASEAN) was not able to announce a joint communiqué because China had given tremendous economic aid to Cambodia, the chair country of the conference. The tighter coordination of ASEAN over the issue of the South China Sea does not favor China. Therefore, China resorted to disintegration warfare to try to disrupt the ASEAN alliance by using economic manipulation. China has implemented many methods, including historic issues during World War II, in attempts to divide the United States and Japan as well.

Unrestricted Warfare

In 1999 two PLA colonels, Qiao Liang and Wang Xiangsui, published the book *Unrestricted Warfare*, which changed the definition of *unrestricted warfare* from "using armed force to compel the enemy to submit to one's will" to "using all means, including armed force or non-armed force, military and non-military, and lethal and non-lethal means to compel the enemy to accept one's interests."[8]

Non-armed force includes trade war, financial war, a new terror war, and ecological war.[9] As for trade war, China banned rare-earth mineral exports to Japan after a Chinese fishing boat skipper was arrested near Senkaku in September 2010. In October 2010, when Chinese dissident Liu Xiaobo was awarded the Nobel Peace Prize, Beijing reduced its imports of salmon from Norway. China also reduced banana imports from the Philippines when the two countries clashed over Scarborough Shoal in 2012.

In part two of the book *A Discussion of New Methods of Operation*, Qiao and Wang cite Sun Tzu: "As water has no constant form, there are in war no constant conditions. Thus, one able to gain victory by modifying his tactics in accordance with the enemy situation may be said to be divine" (*The Art of War*, chapter 6). Before this passage, there is the famous phrase: "An army avoids strength and strikes weakness." This is the substance of unrestricted warfare. Western militaries rely on information systems such as computer networks and space surveillance. Beijing wants to attack those weaknesses using cyber strikes as soft means and antisatellite weaponry as hard means.

The U.S. Secretary of Defense's annual report to Congress, *Military Power of the People's Republic of China* (2009), stated that China's leaders stress asymmetric strategies to leverage their advantages while exploiting the perceived vulnerabilities of potential opponents using so-called "assassin's mace" programs (for example, counterspace and cyber warfare programs).[10]

Japan Maritime Self-Defense Force destroyer JS *Kurama* under way with *Arleigh Burke*–class guided-missile destroyer USS *Gridley* during passing exercise (U.S. Navy/James R. Evans)

Intelligence Warfare

There are strategic documents other than Sun Tzu's that include the topic of intelligence. Carl von Clausewitz's *On War* has only a few pages mentioning intelligence. He writes, "In short, most intelligence is false."[11] B.H. Liddell Hart's *Strategy* perhaps intentionally has no discussion of intelligence at all. Sun Tzu spends the entire last chapter of *The Art of War* discussing intelligence.

Sun Tzu identifies five types of secret agents. The first is the native of the enemy's country. There is no doubt that countering the native agent is important for antiterrorism warfare. David W. Szady, a former assistant director for the Federal Bureau of Investigation (FBI), stated, "the Chinese . . . mastered the use of multiple redundant collection platforms by looking for students, delegates to conferences, relatives and researchers to gather information."[12]

The second secret agent is the one inside the organization. *The Art of War* states, "Of old, the rise of Yin was due to I Chih, who formerly served the Hsia; the Chou came to power through Lu Yu, a servant of the Yin." Paul D. Moore, the former FBI chief Chinese intelligence analyst, writes, "Some Americans of Chinese ancestry in sensitive research or defense-related positions now feel themselves to be under increased scrutiny as security risks."[13]

The third secret agent is the double agent. Katrina Leung provides a good example. A former high-value FBI and PRC Ministry of State security agent, Leung allegedly contaminated 20 years of intelligence relating to the PRC as well as critically compromising the FBI's Chinese counterintelligence program. In March 2013 Bryan Underwood, a former civilian guard at a U.S. consulate compound under construction in China, sold classified photographs, information, and access to the U.S. consulate to the Ministry of State Security.[14]

The fourth secret agent is the expendable type. Sun Tzu states that expendable agents are friendly spies who are deliberately given fabricated information (disinformation) that is related to the media warfare aspect of the three warfares concept. In September 2012 the *Global Times* reported the result of the March 2006 referendum of Ryukyu citizens. Seventy-five percent of them supported independence from Japan and reinstating free trade with China, and 25 percent supported remaining part of Japan.[15] There was in fact no referendum by Ryukyu citizens, and the vast majority of Okinawans want to be a part of Japan. This is a typical example of Chinese disinformation.

The last type of secret agent is the living agent, who collects information and returns with it. Most living agents today engage in cyber espionage. The U.S. Office of the National Counterintelligence Executive published the Counterintelligence Report (2011), which states, "Chinese actors are the world's most active and persistent perpetrators of economic espionage."[16] The U.S.-China Economic and Security Review Commission reported in 2009 that "U.S. industry and a range of government and military targets face repeated exploitation attempts by Chinese hackers as do international organizations and nongovernmental groups including Chinese dissident groups, activists, religious organizations, rights groups, and media institutions."[17] Despite the fact that *Military and Security Developments Involving the People's Republic of China* (2013) listed six specific names of spies,[18] the Ministry of Foreign Affairs spokesman denied China's involvement with cyber espionage. During the U.S.-China Defense Summit in August 2013, Minister of Defense General Chang Wanquan denied (unpersuasively) that China was a major source of pervasive global computer hacking. It has long been acknowledged that China is the greatest source of cyber attacks against the West.[19] That is exactly what Sun Tzu meant when he wrote, "When active, feign inactivity."

Conclusion

Contemporary Chinese strategy is heavily influenced by Sun Tzu, emphasizing everything from deception, which we find in chapter 1, to espionage, which we read about in chapter 8.

There are two final concerns. First, Sun Tzu ignores so-called civilian control. He writes, "There are occasions when the commands of the sovereign need not be obeyed" (chapter 8), and "If the situation is one of victory but the sovereign has issued orders not to engage, the general may decide to fight" (chapter 10). We have seen many indications of this including the *Han*-class nuclear submarine's intrusion into Japanese territorial waters in November 2004, the antisatellite weapon test in January 2007, and the revelation of the J-20 stealth fighter when Secretary of Defense Robert Gates visited China in January 2011.

Second, the main theme of the first half of chapter 6 of *The Art of War* is "initiative." China has made preemptive strikes since its establishment, such as in the Korean War in 1950; the Strait crises in 1954, 1958, and 1995–1996; against India in 1962; against the Soviet Union in 1969; and against Vietnam in 1974 (Paracel Islands), 1979, and 1988 (Spratly Islands). The first principle of the Chinese Air Force is securing initiative through offensive operations.[20] The *Military Power of the People's Republic of China* (2007) contained a side column that asked, "Is China Developing a Preemptive Strategy?"[21] But *China's National Defense* (2008) stated, "China pursues a national defense policy which is purely [deleted since the 2010 version] defensive in nature."

What should we do for countering Chinese strategy? We have to know and use Sun Tzu against China. The general stated, "The first five of the fundamental factors is moral influence which causes the people to be in harmony with their leaders" (chapter 1). In order to disintegrate Chinese moral influence, we must reveal its leaders' true activities as the *New York Times* did in October 2012 when it reported that Wen Jiabao's relatives had tremendous financial assets in the United States. This news damaged the legitimacy of the Communist Party. As a result, the PLA cyber force wanted to discredit the article by all means.

Sun Tzu's *The Art of War* is a double-edged sword. It is effective for opponents but may boomerang on its users. "He who is not sage and wise, humane and just, cannot use secret agents" (chapter 8). JFQ

Notes

[1] Sun Tzu, *The Art of War*, trans. Samuel B. Griffith (Oxford: Oxford University Press, 1963).

[2] *United States Military Posture for FY1989* (Washington, DC: U.S. Government Printing Office, 1989), 5–6, 93–94.

[3] J.P. London, "Made in China," U.S. Naval Institute *Proceedings* 137, no. 4 (April 2011), 59.

[4] *China's National Defense 2012* (Beijing: Ministry of Defense, 2013), preface.

[5] Ibid., chapter 2.

[6] Office of the Secretary of Defense (OSD), *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2013* (Washington, DC: OSD, 2013), i.

[7] OSD, *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2011* (Washington, DC: OSD, 2011), 26.

[8] Colonel Qiao Liang and Wang Xiangsui, *Unrestricted Warfare* (Beijing: PLA Literature and Arts Publishing House, February 1999), preface.

[9] Ibid., chapter 2.

[10] OSD, *Annual Report to Congress: Military Power of the People's Republic of China 2009* (Washington, DC: OSD, 2009), 20.

[11] Victor M. Rosello, "Clausewitz's Contempt for Intelligence," *Parameters* 21 (Spring 1991), 103–114.

[12] Neil A. Lewis, "Spy Cases Raise Concern on China's Intentions," *The New York Times*, July 10, 2008.

[13] Paul D. Moore, "How China Plays the Ethnic Card," *Los Angeles Times*, June 24, 1999.

[14] Narayan Lakshman, "U.S. jails China-based double agent," *The Hindu*, March 6, 2013.

[15] See <http://mil.huanqiu.com/history/2012-09/3122927.html>.

[16] Office of the National Counterintelligence Executive, *Foreign Spies Stealing U.S. Economic Secrets in Cyberspace: Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009–2011* (Washington, DC: Office of the National Counterintelligence Executive, October 2011), i.

[17] U.S.-China Economic and Security Review Commission, *2012 Report to Congress* (Washington, DC: U.S. Government Printing Office, November 2012), 7.

[18] OSD, *Military and Security Developments Involving the People's Republic of China 2013*, 51–52.

[19] Richard D. Fisher, Jr., "China's 'New Relationship' Trap," *Washington Times*, August 26, 2013, B4.

[20] Zhang Yanbing, "Air Force Campaign Principles," *Chinese Air Force Encyclopedia* (n.c.: Aviation Industry Press, 2005), 95–96.

[21] OSD, *Annual Report to Congress: Military Power of the People's Republic of China 2007* (Washington, DC: OSD, 2007), 12.

Chairman and General Fraser briefed on U.S. Army Military Surface Deployment and Distribution mission (USTRANSCOM /Bob Fehringer)

Geography Matters in Maintaining Global Mobility

By William M. Fraser III and Marshall N. Ramsey

All strategy is geostrategy: Geography is fundamental.

—Colin S. Gray[1]

General William M. Fraser III, USAF, is Commander of U.S. Transportation Command. Colonel Marshall N. Ramsey, USA, was Chief Strategy Officer for the command.

Advancements in transportation technology have seemingly collapsed the world's vast distances. In this century we have witnessed the first commercially operated 500-kilometer-per-hour (km/h) magnetic levitation trains and the first privately owned space transport shuttle.[2] In the future we may see a "hyperloop," a partial vacuum tube that carries passengers in

USNS *1st Lt. Jack Lummus* prepares to dock at causeway for vehicle unloading during maritime prepositioning force offload for exercise Cobra Gold (U.S. Marine Corps/Nathaniel Henry)

capsules at speeds up to 1,220 km/h.[3] But such technological change does not eliminate geography as an important factor either in commercial or in military strategy and operations.[4]

Geographic characteristics are often constraining. Nations and significant players on the world stage compete in the domains of land, sea, air, space, and cyber, and ungoverned areas in these domains invite bad actors.[5] Weak and failed states often lack critical transportation infrastructure that would help them overcome their geographic limitations and support their populace during super typhoons, floods, tsunamis, and other natural or manmade disasters. These states frequently lack good governance of their geographical area and have porous borders allowing groups to train, transit, or provide logistics to carry out transnational threats. Strong states may possess the critical transportation infrastructure required for humanitarian assistance/disaster relief operations. However, even strong states have waged war in the realm of geography and about geography.

To meet its international security commitments and protect its national interests, the U.S. military must remain rapidly mobile and expeditionary, supplying and resupplying itself once it is committed. U.S. Transportation Command (USTRANSCOM) provides the rapid positioning of expeditionary forces. Even with distances collapsed by technology, geography matters for our strategy and operations. We have to span the globe and surmount geographical constraints to execute both peacetime and wartime missions and be more responsive to those we support.

Maintaining our global mobility capability in a fiscally constrained environment has required the command to engage in the most comprehensive and collaborative strategic planning endeavor in its 26-year history. The result of our "journey of discovery" is a new strategic plan recommitting us to our ends, ways, and means. We at USTRANSCOM have determined that the "ends" are rapidly projecting power and sustaining it, "ways" are achieving and maintaining global mobility, and "means" are assured access and a well-developed and synchronized distribution network.

Ends

In *Joint Force of 2020*, the Department of Defense (DOD) values global agility, with a premium placed on swift and adaptable military responses.[6] In this context, the United States will seek to mitigate conflict escalation or achieve deterrence by focusing on the decisive and quick employment of essential and relevant forces. These forces may be positioned forward, partnered with capable allies, or based in the United States. In each case, strategic mobility is the key element for power projection.

USTRANSCOM has recognized that the ends—superior support to warfighters to *project power and sustain operations*—must not and will not change. Most important, we recognized the need to develop and implement bold and innovative ways to adapt to the future operating environment. At the same time, we realized that our means—fiscal, materiel, and personnel—will experience increased pressure for more efficiency for the foreseeable future. During development of USTRANSCOM's strategic plan, we focused on developing processes, adapting structures, and reinforcing an enabling culture.

The command will deliver the transportation and enabling capabilities that make America a global power by preserving our readiness capability, achieving information technology management excellence, aligning our resources and processes for mission success, and developing customer-focused professionals. The vision is to become the transportation and enabling capability provider of choice.[7]

Ways

Global mobility supports the future joint force and globally integrated operations as described in *Joint Force 2020* by providing adequate transportation and distribution capabilities and capacities.[8] In addition to readily deployable joint forces and sufficient lift, there must be a supporting global network.

The foundation of DOD's global mobility capacity is the organic capabilities provided by USTRANSCOM's Army, Navy, and Air Force component commands using Active-duty and Reserve component forces. However, integral to the global mobility capacity needed by the Nation are the additional capabilities gained through our commercial transportation providers. The assets and networks of our commercial partners are absolutely critical in fulfilling global demands, especially during surge operations. Through this optimal balance of Total Force organic and commercial lift, we can quickly pivot transportation resources wherever and whenever needed.

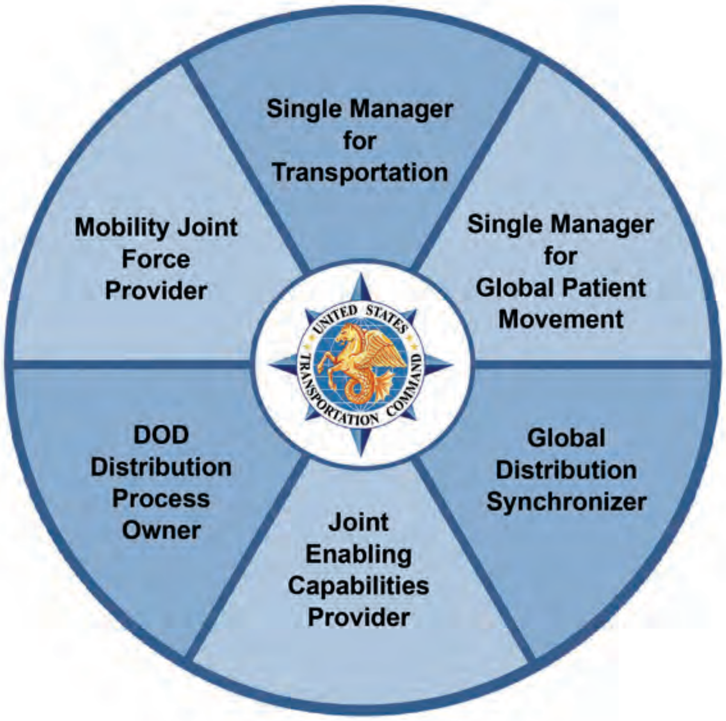
Improving strategic mobility will also require decreasing lift and sustainment requirements and making intelligent use of prepositioned equipment in coordination with the Services and the Defense Logistics Agency.[9]

Acting in our role as the Mobility Joint Force Provider (see figure), USTRANSCOM advises and guides mobility force sourcing solutions to best effect for the supported geographic combatant command.[10] This enables us to quickly reallocate mobility capabilities where they are needed while mobilization of surge capacity of both organic and commercial partners occurs. We can also rapidly open aerial and seaports in or near the joint operational area.

Maintaining global mobility is the way to project power rapidly and sustain operations. It is also achieved and maintained through freedom of action from assured access to the global commons, a viable global distribution network, and the ability to rapidly transition from steady state to contingency or crisis response operations. All of these capabilities mitigate the time and distance constraints imposed by geography on USTRANSCOM's worldwide mission.

Means

Global mobility for rapid power projection requires *assured access* to the global commons (relevant maritime, air, and space domains outside any country's national jurisdiction), as well as access to a viable distribution network and cyberspace. Assured access often requires multiple paths to preclude a single point of failure, which is true not only for our physical networks but also for operations in the contested cyber domain. The global commons are part of USTRANSCOM's end-to-end distribution network, which includes ports of embarkation, en-route nodes, and ports of debarkation. DOD relies on friendly nations and allies for the use of en-route and destination infrastructure to facilitate the global surface and air corridors that comprise the distribution network. Conversely, allies depend on U.S. mobility capabilities for combined operations. DOD must be free to


Single Manager for Transportation
Single Manager for Global Patient Movement
Global Distribution Synchronizer
Joint Enabling Capabilities Provider
DOD Distribution Process Owner
Mobility Joint Force Provider
United States Transportation Command

Sailor monitors flights in Joint Operational Support Airlift Center Execution Team area of USTRANSCOM Fusion Center (USTRANSCOM/Bob Fehringer)

operate across the entire distribution network with surety. This was true in the past, is true today, and will be true in the future.

World War II's historic airlift operation over "the hump" of the Himalayas kept China in the fight against Japan and contributed significantly to the U.S. victory in the Pacific. In the China-Burma-India theater of operations, harsh weather, severe terrain, the enemy, and host nation sovereignty were all challenges that airlift had to overcome, especially while waiting on construction of the Burma road.[11] Similarly, the Hindu Kush, the lack of seaports in land-locked Afghanistan, the limited number of useful roads and airfields, and other nations' sovereignties are challenges the command must overcome today when delivering, sustaining, and redeploying forces for Operation *Enduring Freedom*.

Initially USTRANSCOM airlifted troops, their combat equipment, and their sustainment materiel until ground lines of communication could be established. Assured freedom of action and global mobility allowed the command to quickly deploy and employ mobility forces seamlessly. Our commercial partners played a critical role by providing extended "reach" within their broader network of capabilities and trade relationships. This extended reach gave the command flexibility and access it did not otherwise possess.

Access to the cyber domain is critical for global mobility. We execute logistics, transportation in particular, through information systems operating largely on unclassified but protected networks and include participation of our commercial partners and others through their information technology systems. Adversaries understand that transportation activities can signal operational intent, so our information networks provide a lucrative target and a vulnerability we must address. In addition our decisive and reliable command and control of strategic mobility operations is a capability our adversaries would like to acquire. Protecting, defending, and mitigating adverse operations in cyber space is a key focus area for USTRANSCOM along with its component commands and commercial partners.

The Global Distribution Network (GDN) is the foundation of our Global Campaign Plan for Distribution (GCP-D). The health of the network is integral to strategic readiness and rapid projection of power for many combatant commands and their operational plans. Through it we provide responsive and agile support through DOD and commercial partners.

As USTRANSCOM commander, my primary objective for engaging leaders within and outside DOD is helping set the conditions for the GCP-D. We are meeting with key leaders in geographic combatant command areas of responsibility to discuss existing diplomatic agreements, sustain partner-nation relationships, secure conditions for retrograde operations in Afghanistan, and explore infrastructure improvements that can serve our strategic requirements. At each stop we engage with U.S. country teams and host nation ministers of defense, foreign affairs, and transportation. Economic development is often discussed. Partner nations view being part of the GDN as a source of revenue for their countries, and they frequently invest money and political capital to further this objective.

Many of our partner nations have plans to develop transportation-related infrastructure that will improve their capabilities. These plans are frequently unsynchronized and focus on a single node such as airfield construction, but without an associated road network. As the responsible agent for the GDN, the command collaborates with partners to coach them in the development of a comprehensive vision for their transportation networks. An infrastructure plan that is comprehensive, prioritized, and phased will achieve far greater success, and this approach aligns well with our global transportation and commercial network objectives.

We will continue to foster these partnerships to maintain the readiness of the GDN and its ability to respond to future requirements. For example, the viability of the Northern Distribution Network (NDN) infrastructure—sea and aerial port facilities and road and rail networks—will remain vital after the conclusion of *Enduring Freedom*. Learning from NDN's successful support of deployed forces when ground lines of communication through Pakistan were interrupted, we are already partnering with U.S. Pacific Command (USPACOM) to lay the foundation for a Pacific Distribution Network as well as with U.S. Africa Command. The Pacific Rim is one part of a complex network of bilateral and multilateral relationships that spans vast distances with minimal basing. Intratheater movement in the USPACOM area of responsibility is similar to intertheater movement globally and is often referred to as "the tyranny of distance." We must be smart and efficient about the way we use our scarce resources to achieve readiness for the Pacific Distribution Network. As a baseline we will nest our efforts within USPACOM's strategy to ensure we remain responsive and ready to perform them. The African continent has equally daunting distance and access challenges.

We also discuss aerial refueling interoperability during our engagements. Many allied partners use the same platforms we do. We have developed standardized procedures, but there is a lack of synchronized certifications. We will continue to contribute to the DOD effort to improve aerial refueling interoperability with our partners. More must be done in this area and lessons learned must be turned into future solutions. In many cases, our partners' preparedness to support coalition operations may hinge on this unique ability to fully employ their capabilities.

But assured access to the global commons and a viable distribution network are not enough. While it is clearly our components and commercial partners who successfully deliver the goods, USTRANSCOM develops optimal end-to-end distribution processes and solutions across various transportation modes and nodes. Our third means of rapidly projecting power is our unique ability to synchronize plans, coordinate, and align transportation operations around the world, which is where our true value-added is achieved. USTRANSCOM's role will continue to be integral to overcoming geographical constraints.

The command's recently assigned Global Distribution Synchronizer role (see figure) ensures that geographic combatant commands' transportation-related posture plans are synchronized and mutually supportive to achieve seamless global mobility. We do this by participating in planning conferences and exercises. USTRANSCOM's en-route infrastructure master plan is also synchronized with combatant commands to ensure capabilities exist at various ports, airfields, and multimodal sites when required.

In particular, USTRANSCOM will assess the GDN vis-à-vis the strategic environment. The heart of the GCP-D is developing all the requisite elements of a "warm" network to operate anywhere on the globe, so when the time comes we can quickly respond to it to meet the Nation's needs. Synchronization of the efforts to set the conditions for future distribution operations is where USTRANSCOM, with the help of others, ensures that efforts are mutually supporting and achieve the desired objectives for strategic mobility.

Lastly, in the past, USTRANSCOM operated in the individual land, sea, and air segments of transportation. However, through our years of experience in our Distribution Process Owner role (see figure), we realized we could move combat equipment via surface land/ocean and air routes through multimodal hubs and not only meet required delivery dates, but also be more cost-effective. Multimodal is increasingly becoming our operational norm as is the ability to coordinate and synchronize movements end-to-end.

The ability to decisively engage globally—literally overnight—hinges on the mobility and transportation assets USTRANSCOM coordinates and synchronizes to rapidly project power and sustain a global presence. Leaders at all levels of government tell me that USTRANSCOM makes mobility look easy, knowing full well it is not.

Our command overcomes geographic constraints and rapidly projects power through global mobility, assured access, a viable GDN, and global synchronization of distribution. The extraordinary ability to rapidly project national power and influence—anywhere, anytime—is unique to the United States. Modern means of transport alone cannot eliminate the strategic significance of terrain, environment, and vast distance.

We must remember that the challenge of geography is compounded by the twin tyrannies of time and cost. By nature, crises develop quickly, and we are pressured to respond faster. Military personnel resources are expensive, and the cost of transporting them and their sustainment increases with distance.[12] When effectiveness and responsiveness are not paramount, warfighters and customers need more cost-conscious transportation solutions, preferably a range of costed options.

All strategy must contend with geography even when it is not about contested geography.[13] Together we are working toward a more effective and efficient command to provide America's global mobility and enable its capabilities wherever and whenever needed. Together with our components, the Defense Logistics Agency, and commercial partners, U.S. Transportation Command will continue to deliver the mobility and transportation options that bolster our nation's power. Together, we deliver. JFQ

Notes

[1] Colin S. Gray, *Fighting Talk: Forty Maxims on War, Peace, and Strategy* (Westport, CT: Praeger Security International, 2007), 78.

[2] See "Shanghai Maglev Train," available at <http://en.wikipedia.org/wiki/Shanghai_Maglev_Train>; "Falcon 9," available at <www.spacex.com/falcon9>.

[3] See "Hyperloop," available at <http://spacex.com/hyperloop>.

[4] Colin S. Gray, *Modern Strategy* (Oxford: Oxford University Press, 1999), 40.

[5] Gray, *Fighting Talk*, 78, 80. Mankind does not live at sea or in cyberspace. Most wars entail where belligerents live, and therefore, land matters most. Even though air and sea may dominate the conduct of a war, conflict's likely objective is to influence the enemy's behavior on the ground and often requires that the final blow be delivered by ground forces.

[6] *Capstone Concept for Joint Operations: Joint Force 2020* (Washington, DC: The Joint Staff, September 2012), available at <www.jcs.mil//content/files/2012-09/092812122654_CCJO_JF2020_FINAL.pdf>, 4–7.

[7] See "Our Story: 2013 to 2017," available at <www.ustranscom.mil/strategy/v1.cfm>.

[8] *Capstone Concept for Joint Operations,* 12.

[9] Ibid., 1.

[10] *Unified Command Plan 2011* (Washington, DC: The Joint Staff, April 6, 2011, with Change-1 dated September 12, 2011), 29–31.

[11] William H. Tunner, *Over the Hump: Berlin Airlift 50th Anniversary Commemorative Edition* (Washington, DC: Air Force History and Museums program, 1998).

[12] Joseph S. Nye, Jr., *The Future of Power* (New York: PublicAffairs, 2011), 27.

[13] Gray, *Fighting Talk,* 79.

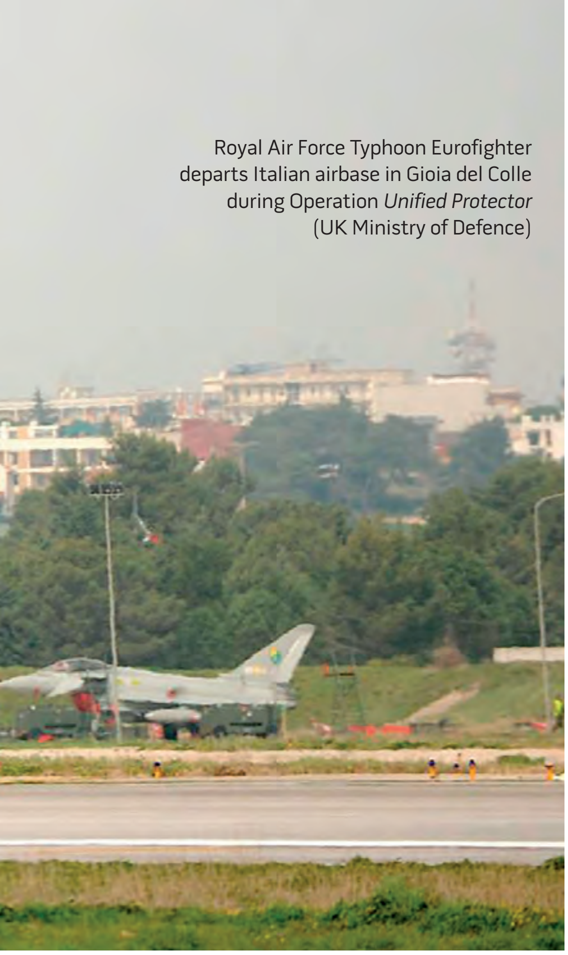
Reflections on Operation *Unified Protector*

By Todd R. Phinney

As 2010 ended, few in the North Atlantic Treaty Organization (NATO) would have predicted that the Alliance, with assistance from four partner nations, would be leading an air-heavy joint operation in North Africa. However, as the Arab Spring swept across the region, NATO was rapidly drawn into the unfolding events in Libya. What followed over the next 7 months within the Combined Force Air Component (CFAC) warrants discussion because what was learned can help prepare future military leaders as well as highlight the effect of civilian policy decisions.

The Libyan uprising was enabled by social media on February 14, 2011, with a freedom movement erupting in Benghazi shortly afterward. The rhetoric and violence of the regime quickly galvanized the United Nations into passing two Security Council Resolutions (UNSCRs) that described the mandate for the military action that followed. The first, UNSCR 1970 (February 26), imposed an arms embargo and froze regime assets.[1] The second, UNSCR 1973 (March 17), authorized a no-fly zone over Libya as well as the use of "all necessary means" to protect Libyan civilians.[2] After initial rebel military successes in late February, regime forces regrouped and began to crush rebel forces and population centers across the country. Significantly, regime forces appeared poised to retake the resistance "capital" in Benghazi, putting more civilian lives at risk. The U.S.-led coalition Operation *Odyssey Dawn* (OOD) began on March 19, 2011, when a French air force strike package attacked regime mechanized forces approaching Benghazi. The OOD air campaign, executed from Ramstein Air Base, lasted until March 31. NATO then took command with the Combined Joint Task Force (CJTF) positioned at

Colonel Todd R. Phinney is the Combat Air Forces Chair at Air University and teaches leadership and warfighting at the Air War College, Maxwell Air Force Base, Alabama. During Operation *Unified Protector*, he was a Combined Force Air Component Deputy Director.



Royal Air Force Typhoon Eurofighter departs Italian airbase in Gioia del Colle during Operation *Unified Protector* (UK Ministry of Defence)

Naples, and the air component eventually located at Poggio Renatico,[3] both in Italy.

In contrast to operations in Iraq and Afghanistan, Operation *Unified Protector* (OUP) was unique in its relatively short duration and lack of a "blue" land component. In total, the OUP CFAC planned and executed 218 air tasking orders (ATOs),[4] flew over 26,500 sorties including 9,700 ground attack sorties,[5] destroyed over 5,900 military targets, and deconflicted over 6,700 humanitarian aid flights and ground movements.[6] Compared to the 38,000 sorties flown during the 78-day NATO air campaign over Kosovo, OUP's air planners had fewer assets with which to execute their task in a much larger area of responsibility—a region comparable to Alaska.[7] Of NATO's 28 member nations, all provided staffing and 12 provided air assets. Sweden also provided tactical reconnaissance aircraft. Key to legitimacy in the Arab world, Jordan, Qatar, and the United Arab Emirates also contributed personnel and aircraft. This involvement created the first-ever NATO-Arab combat partnership and is best described as an Alliance effort with four partner nations.[8]

NATO's underlying strength is underscored by the contribution and commitment of its members. However, complete consensus by NATO nations normally limits the speed at which the Alliance operates. The pace at which NATO accepted and executed OUP created daunting challenges. As discussed, the first OOD aircraft struck on March 19. NATO accepted the no-fly zone mission on March 24, and on March 31 the NATO CFAC took command of the entire air mission over Libya. While prudent thinking had occurred, NATO did not officially begin planning until the North Atlantic Council (NAC) agreed to take over from the coalition.[9] The resulting challenges of this quick pace were significant. While beginning to plan and execute combat operations, the OUP CFAC faced internal challenges that significantly hampered its ability to execute air operations.[10]

The first challenge was to overcome structural impediments hampering mission execution. At the beginning of OUP, NATO Air comprised two distinct geographic regions north and south of the Alps. U.S. Air Force Lieutenant General Ralph Jodice commanded the Southern region, Air Component (AC) Izmir, located at Izmir, Turkey. The Izmir concept of contingency operations was for the commander/CFAC commander (CFACC) to remain in place along with the strategy division, the majority of the intelligence, surveillance, and reconnaissance (ISR) division,[11] the "upper" portion of the plans division (guidance, apportionment, and tasking), and the director of staff. Meanwhile, the NATO Combined Air Operations Centers (CAOC)[12] in the Southern region would execute the air operation with the resident "lower" half of the plans division, producing the master air operations plan and ATO, while executing the ATO with the operations division. This distributed mode of operations was in place at the beginning of OUP but was essentially stillborn from the beginning. Myriad problems arose with the CFACC not being physically present with the entire entity to provide unity of command. As kinetic operations were executed from the CAOC at Poggio Renatico,[13] the CFACC found himself often on the phone with the CAOC Poggio director of operations working to link strategy to the task and the task back to strategy.[14] While attempting to build the CFACC's awareness, the CAOC Poggio director of operations was himself losing awareness and the ability to lead the fledgling and hastily assembled team on the operations floor. Recognizing the untenable nature of this virtual presence, the CFACC flew to Poggio on April 1, taking a handful of his direct staff. Moving forward improved the air effort.[15] This was critical as each tactical bomb had a very real strategic importance for the unity of the Alliance. Importantly, the NAC mandated a zero civilian casualty allowance for NATO fires. Early on, General Jodice identified the unity of the Alliance and partner nations as the "blue" center of gravity and one errant bomb with civilian casualties could have splintered cohesiveness.

Other problems arose from a geographically split CFAC structure. Not enough legal advisors were available to support both Izmir and Poggio, and they were initially sent to the CFAC at Izmir. As a result, the quickly formed team at Poggio, now executing combat operations, did not have legal advisors for rules of engagement (ROE) and collateral damage estimate advice on the combat operations floor. In one case, Poggio elected to delay a strike and roll it onto a subsequent ATO. However, the reporting cell at Izmir missed that and reported the target as struck. NATO Public Affairs released targeted information the next morning, compromising the target. The CFAC's ability dramatically improved once all key elements finally collocated at Poggio. The problems discussed make clear the importance of establishing the correct organizational structure at the onset and that the geographically split OUP CFAC structure significantly degraded operations.

Exacerbating the CFAC structural problem was an immediate lack of skilled staffing across each of the CFAC divisions. That was made worse by the need to create a new initial estimate of manning because recent AC Izmir exercises

KC-10 Extender takes off to provide air-refueling assets to NATO aircraft during Operation *Unified Protector* (U.S. Air Force/Andra Higgs)

were strictly humanitarian rather than kinetic. Also, a single versus geographically separated CFAC structure—the structure envisioned and planned for—changed manpower requirements. To accomplish its air-policing mission, Poggio had approximately 94 personnel who trained and operated with a defensive mindset. Once leadership determined that the new staffing requirement was roughly 400 members, a call went out for augmentation from other NATO and national entities.[16] The same cadre of leadership trying to concurrently prepare for and execute combat operations built this staffing requirement. They also had to expend precious time and focus on processing new arrivals—triaging capabilities, skill sets, and maintaining awareness on the needs and current staffing within the divisions.[17] It also became apparent that the skill sets necessary to fill a peacetime air operations center position such as chief of intelligence were significantly different from those needed for planning high-end airpower strategic and interdiction missions.

Ensuring proper manning of skilled personnel in the CFAC was a continuous struggle. Financial constraints and national political contexts were the two most common inhibitors. The CFACC established 45 days as the minimum time an augmentee should be present for duty. In reality, nations determine deployment length, so many arrived late and left early, compounding training, continuity, and turnover problems. Additionally, nations expected NATO to fill the operational needs with members assigned to Alliance billets. However, some nations prevented NATO from declaring a crisis establishment, summer leaves remained, and members accrued overtime hours at peacetime rates. All these factors made it difficult to execute missions at the NATO organizations that provided staffing to OUP because they had to continue home station tasks. Additionally, some members suffered financially when their governments adjusted their basic housing allowance rate to Italy. The CFAC never received sufficient staffing and as a result never used the normal 24-hour strategy for its ATO production planning schedule. Rather, limited-skilled manning drove a decision to operate on extended days, reducing planning capability.

The U.S. policy decision to take a secondary role in OUP exposed NATO ISR shortcomings and initially hampered mission accomplishment. On March 28, 2011, the President addressed the Nation and indicated that the United States would take a supporting role.[18] Much has been written about the CFAC's initial inability to properly man and equip an ISR division. These accounts are true. As augmentees arrived at Poggio, they began to fill the fledgling intelligence entity, which was still split because the original ISR division was at Izmir. Compounding issues, the small intelligence cell permanently assigned to the air policing CAOC at Poggio was insufficient in skill set and number for the new task of running a sophisticated kinetic air war.

At the core of this limitation is the fact that few countries have the national capability to collect intelligence, analyze it, share it on classified architecture, and then develop the high-fidelity targeting materials necessary for an aerial campaign where collateral damage is a concern. As the United States stepped back to a supporting role following the handover to NATO, the CFAC's ISR division capability for Operation *Unified Protector* suffered when it was needed the most. Largely absent were U.S. national feeds providing critical knowledge and the current imagery and trained personnel necessary to make collateral damage estimate determinations to prosecute dynamic targets. Most important, the United States did not immediately provide trained personnel to augment NATO's nascent ISR division.[19] A perfect storm existed from the beginning: NAC guidance for zero civilian casualties and damage to civilian infrastructure, strong political pressure for the Alliance to take over the mission, the urgency to prevent Benghazi from being overrun, and the CFAC shackled by lack of a functional ISR division. From his OUP experience, General Jodice stated, "ISR is a driver, not an enabler for airpower."

Within days, the CFACC director asked for help from NATO's Northern Air Component at Ramstein Air Base. A U.S. Air Force intelligence colonel who was weapons school–trained arrived at Poggio to lead the ISR division. She worked informal networks and a handful of U.S. intelligence officers began to appear within days. Some were Reservists who, through creative efforts on securing funding and orders, answered the distress call and made their way to Poggio. Facing challenges and frustrations from the monumental task at hand, the ISR division chief late one night sent an email outlining, in blunt terms, the consequences of the lack of U.S. support. This email went viral within the Pentagon and was read well beyond the level originally intended; however, the ultimate impact was positive. The message was clear: NATO needed multilevel U.S. ISR support to succeed in the mission. This will be true in future NATO missions and should temper U.S. voting on future NATO operations requiring high-end ISR support, especially if the United States lacks an appetite for involvement, or to support staffing needs.

Formulating an initial air strategy was also difficult. A lack of clear political guidance and trained strategists along with differing views between the CFAC and the CJTF made initial strategy formulation difficult. Beginning with political guidance, the flash to bang period between UNSCR approvals and NATO taking the mission was very short—essentially 1 week. This period left little time to design a comprehensive strategy. Additionally, the 28 Alliance nations each saw the situation and potential Libyan endstates differently. With this, planners only received broad political guidance. OOD planners have since expressed that they also suffered from a lack of clear political guidance that carried into OUP.[20] The CJTF Naples no-fly zone operations plan on March 27 stated that the assigned mission for the air component was to "enforce a no fly zone" and "to help protect civilian or populated areas under threat of attack." Translating the broad strokes of this last phrase when matched with the UNSCR phrasing of "all necessary means" left the CFAC leaders grappling to determine the accepted left and right limits of the Alliance mandate. The Berlin Ministerial Conference on April 14 did provide further clarification by stating that the desired objectives were for attacks on civilians to cease, the regime to withdraw military forces, and a "credible and verifiable ceasefire, paving the way for a genuine political transition" to take place.[21] On August 23, the NAC further refined the NATO endstate by establishing three key conditions for success. First, Libyan civilians would no longer require NATO to protect them from the threat of or an actual attack; second, an external entity such as a stabilization force could ensure stability inside Libya without NATO support; and third, regime and rebel forces would adhere to the terms of a cease-fire, and military and security forces would be back in designated locations.[22] Fortunately, guidance became clearer over time as the nations built consensus.

A clear vision of the endstate and trained strategists are key elements in creating a winning air campaign plan. Early on, the strategy division suffered from a lack of formally trained and experienced strategists. In truth, the ownership of this error fell with the sending nations filling posts for which their members were not prepared.[23] Few nations possess the training programs and opportunities to groom fully capable strategists, and they were absent in NATO Air prior to OUP. Moving the strategy function to Poggio under the leadership of a British group captain (colonel) recruited from the Royal Air Force liaison team, with strategy experience from the Kosovo campaign and the International Security Assistance Force, eventually helped create a functional strategy division at Poggio.

Once functional, the CFAC strategy division had to create a strategy complementary with the CJTF's plan. Unclear guidance, the quick tempo, no-land component, and a stand-alone maritime mission resulted in a CJTF campaign plan based on airpower, but not an air campaign.[24] The CFACC made two decisions instrumental in developing an air strategy. First, he directed the air component to create its own strategy within a campaign plan with the intent of vertically influencing the CJTF strategy and complementing the CJTF plan. Second, he directed the formation of a "red team" within the strategy division that was instrumental in gaming possible strategies and perceived outcomes. Libya is a large country spanning almost 1,000 miles from east to west and 500 miles from north to south. The size of the country and limited CFAC assets constrained what the air campaign could accomplish per each ATO period. For instance, the CFAC had only enough E-3s to ensure 24/7 coverage with one aircraft on station. Other large ISR division platforms were limited to one flying period per day. This forced planners either to saturate a specific area for an extended period or to methodically rove across Libya and capture as many snapshots of prioritized areas as possible. Early remotely piloted aircraft coverage consisted of two Air Force MQ-1s, and these missions necessitated careful planning as their slow groundspeed prevented rapid repositioning for new priorities.[25] At the high water mark, the CFAC could launch just below 70 offensive strike sorties during an ATO cycle to cover an area equivalent to the size of Alaska.[26] The strategy that eventually emerged divided Libya into nine regions.

This division fostered a geographically based awareness with a usable lexicon shared by the Airmen at the CFAC and the CJTF staff. The CFACC's guidance to marshal efforts toward coercing combatants harming civilians drove initial center of gravity analysis. The United Nations mandate and NATO leadership did not limit strikes to regime forces. NATO forces could engage any military force threatening civilians. The reality on the ground was that Muammar Qadhafi's forces matched action to the regime's rhetoric. Rebel forces entering a previously threatened town were welcomed as liberators. Thus the strategy division focused on Qadhafi's regime cohesion as the primary center of gravity to exploit. Strategists emphasized disrupting regime command and control as well as military and paramilitary forces.

This geographic focus combined with the center of gravity analysis yielded four regional approaches with the intent of protecting civilians.[27] Around the Greater Tripoli region, NATO focused on disrupting command and control and regime forces. These efforts would marginalize the credibility of the regime and reduce its ability to threaten the populace. In the Jalu Brega region, NATO focused on engaging the forward elements of the regime forces between Brega and Ajdabiya. This was critical as Ajdabiya was the remaining impediment between the regime and Benghazi. In the northwest region adjacent to the Tunisian border, NATO focused on understanding what was occurring on the ground to deter further advances by the regime against the encircled rebel towns. Finally, in the southern part of the Jalu Brega region, NATO focused on understanding military activities in order to prevent fielded forces from flowing toward the battle area near Ajdabiya. As available air assets were limited, the initial air strategy relied on regional pulsing. The intent was to maximize limited ISR across the battlespace and provide kinetic activity when and where it was most needed. As with any campaign, fog and friction continually challenged execution.

Discussions to this point focused on the challenges during the few months of OUP. As time progressed, the CFAC organization matured and became a cohesive team. Needed external national support became available, at least to the minimal level necessary to plan and execute a successful campaign. Both deliberate and dynamic targeting processes evolved, and by mid-June the CFAC effectively and rapidly applied fires across the battlespace. Deliberate target sets ranged from isolated military sites in the badlands to urban installations in downtown Tripoli requiring sophisticated planning and delivery. The ISR division chief overcame initial reservations about preplanned targets by including the senior national representatives[28] in the initial efforts of the joint targeting working group. This initiative ensured that by the time the CJTF commander approved a target and put it on the joint prioritized target list, national questions and concerns had normally been addressed and the striker nation was prepared to engage the target. Many of the smaller striker nations deservedly received accolades because they did indeed punch well beyond their weight. Planners and aircrews took exhaustive measures to ensure that every strike was required and was free of civilian casualties. As an example, an aircrew member terminally "drug off" a laser-guided bomb when a civilian approached the target. In another, the aircrew did not release on a re-attack when Libyan emergency responders became a collateral damage concern. The discipline of OUP aircrews was commendable, enabling the cohesion of the Alliance and ensuring continued international support for the mission. This highlights the importance of training to all spectrums of conflict.

Dynamic targeting also matured, and the CFAC team became more adept at effectively solving higher collateral damage estimate scenarios. This was possible through the selection of weapons and a developed and seasoned approval process in combat operations.[29] Positive identification of regime elements became more difficult as they quickly shed standard military vehicles for Toyotas, learned the art of concealment, and did their best to exploit ROE limitations set in place to protect nonmilitary personnel, infrastructure, schools, and mosques. Using a restricted fire line aided aircrews in knowing where within the ROE they could engage without CFAC approval. Conversely, the CFAC had to approve targets on the restricted side of the restricted fire line. Whether aircrews or CFAC approved, due to the fluidity of the battlespace, limited ISR assets, and the strategic nature of every bomb, leadership and aircrews exhaustively weighed each engagement decision. The U.S. decision to allow employment of the Hellfire II missile from MQ-1 Predators helped immensely.[30] Remotely piloted aircraft with precise small weapons were an invaluable asset when attacking targets difficult to find or strike, or targets that required heavy scrutiny to ensure ROE requirements.

Airpower had multiple accomplishments believed to be firsts in OUP. Often, the limited assets on hand drove the CFAC to creatively maximize and employ each airborne asset. Strategically, this operation was the first NATO-Arab military operation. Also, France was deeply involved in the leadership, planning, and execution of OUP, a significant milestone as France had just returned to the military portion of the Alliance. Both Qatar and the United Arab Emirates dropped their first bombs in combat over Libya. The British Typhoon also dropped its initial combat weapons and flew its first combat pairings with the GR-4 Tornado. French and British rotary attack helicopters, normally land component assets, flew jointly from naval platforms while operating under CFAC command and control. OUP saw the first U.S. MQ-1 "buddy-lasing" for a foreign attack helicopter as well as regularly for foreign jet fighters. The MQ-1 became indispensable as a deep radio relay, on-scene commander in case of an ejection, and aerial coordinator for time-sensitive dynamic attacks on behalf of the CFAC. U.S. rescue helicopters staged aboard Alliance naval vessels to get them closer to recovery locations in case of ejections deep in hostile territory. Finally, fire support teams operated aboard two different maritime patrol aircraft platforms and effectively scoured assigned areas of the battlespace and directed precise fires against hostile forces.

What ultimately led to the success of OUP were the people involved from top to bottom. The speed at which the Alliance took on the mission and

French corvette FS *Commandant Birot*, attached to NATO Maritime Task Force 455, operates in Mediterranean Sea during Operation *Unified Protector* (Italian Navy)

structural, manning, and national support challenges created a serious problem with little time to solve it. The importance of the leadership of the CFACC and his director during the early days cannot be overstated. NATO and partner nation personnel of all ranks arrived at the CFAC and gave their all. In some cases, skills did not match positions and members willingly accepted unanticipated roles. General Jodice made it a point to know the name of every staff member at Poggio. His care for personnel was sincere and was appreciated at all ranks. He also recognized departing members at each shift change briefing. Many members met their national limits on deployment length, went home, and found a way to return to Poggio. National representatives quickly adorned their flight suits with CFAC OUP patches and became genuine members of the CFAC effort. Strong leadership in a national endeavor is critical. In multinational operations with a unified chain of command where the unity of the nations is a center of gravity, effective and inclusive leadership by the commander is essential.

OUP was executed concurrently with NATO planning to reduce the size of the Alliance's force structure. AC Izmir took down its flag last summer and a singular NATO air component will exist at Ramstein Air Base in Germany. As members of OUP returned to their regular NATO locations, they took with them the lessons of the Libyan operation. The current NATO joint force air component (JFAC) organization structure is largely set and doctrinally sound. A key takeaway is the importance of kinetic exercises. Senior air leaders must defend these because training opportunities are limited. AC Ramstein is configuring the JFAC facility with proper communications equipment and life support. There is an awareness that NATO, U.S., and European national JFACs need to train, exercise, and be prepared to execute together. Looking forward, it will once again be up to nations to determine if they will send trained and ready augmentation to the NATO CFAC. Failure to do so will cause the same problems created during OUP. Finally, in the future, key nations possessing unique enabling capabilities and personnel cannot "hand over the mission to NATO" and expect success without their involvement.

At 2200Z on October 31, 2011, General Jodice gave permission for the last OUP aircraft, fittingly a NATO

AWACS, to depart Libyan airspace. Over the satellite radio, he dismissed the aircraft by saying, "For the past 7 plus months, you were bold, aggressive, relentless but never reckless, and made the success of Operation *Unified Protector* possible. I am proud of you all. On behalf of a grateful Alliance and partner nations, I thank you for your professionalism and tremendous effort. Job very well done!" For the members of the OUP CFAC team crowded into the operations room that evening, this radio call culminated 218 days of executing an unexpected air campaign that saved thousands of Libyan lives. **JFQ**

Notes

[1] United States Mission to the United Nations (UN), Fact Sheet, "UN Security Council Resolution 1970, Libya Sanctions," February 26, 2011, available at <http://usun.state.gov/briefing/statements/2011/157194.htm>.

[2] UN Security Council (UNSC), Press Release for UNSC Resolution 1973, "Security Council Approves 'No-Fly Zone' Over Libya, Authorizing 'All Necessary Measures' to Protect Civilians, by Vote of 10 in Favour with 5 Abstentions," available at <www.un.org/News/Press/docs/2011/sc10200.doc.htm>.

[3] Hereafter referred to as CAOC Poggio.

[4] An *air tasking order* is a detailed flying plan for a 24-hour period.

[5] Known as offensive counterair sorties in the North Atlantic Treaty Organization (NATO).

[6] NATO Fact Sheet, *Operation UNIFIED PROTECTOR Final Mission Stats*, November 2, 2011, available at <www.nato.int/nato_static/assets/pdf/pdf_2011_11/20111108_111107-factsheet_up_factsfigures_en.pdf>.

[7] Central Intelligence Agency, *The World Factbook* (Libya entry), available at <www.cia.gov/library/publications/the-world-factbook/geos/ly.html>.

[8] Ralph Jodice highlights that Operation *Unified Protector* (OUP) was not a coalition operation, but rather an Alliance-led operation joined by four non-NATO partner nations. Ralph Jodice II, USAF, OUP Combined Force Air Component (CFAC) commander (CFACC), interview by author, January 17, 2013. For more on the significance of Arab involvement, see Massimo Calabresi, "Head of State," *Time* (November 7, 2011), 15–21.

[9] Ancel Yarbrough, OUP CFAC director, interview by author, January 11, 2013.

[10] Ibid.

[11] In fact, the intelligence, surveillance, and reconnaissance (ISR) division was more of an ISR module. Rachel McCaffrey, ISR division chief, email to author, January 3, 2013.

[12] The NATO Combined Air Operations Centers (CAOCs) are air-policing centers, not a standing joint force air component.

[13] For brevity, Poggio Renatico will be referred to as Poggio.

[14] The CAOC Poggio director of operations became the OUP CFAC director in late June 2011. Yarbrough, interview by author, January 11, 2013. Jodice, interview by author, January 17, 2013.

[15] In retrospect, Jodice believes that moving forward was helpful in many ways. First, as already highlighted, this helped him link strategy to task and then the task back to the strategy vertically. Second, by collocating the CFAC in one location, all senior leaders had access to the CFACC and vice versa. Having senior leaders in the same location allowed face-to-face discussion, which improved clarity and reduced time spent on background discussions prior to decisionmaking. Third, it helped him see the limitations of the initial CFAC structure and make adjustments.

[16] The CFAC never received more than 75 percent of its requested staffing.

[17] The task of transforming the Poggio physical complex from supporting 94 members to over 450 was difficult. This number (450) represents the CFAC staff and national liaison teams all collocated at Poggio. These were the same trailers used during the NATO Kosovo operation and required continuous care. Power, water, communications, office space, and negotiating for the placement of new buildings were all tasks required at the onset of the operation.

[18] Remarks by the President in Address to the Nation on Libya, National Defense University, March 28, 2011, available at <www.whitehouse.gov/the-press-office/2011/03/28/remarks-president-address-nation-libya>.

[19] McCaffrey, email, January 3, 2013, and multiple discussions with author.

[20] For greater clarity, see Joe Quartararo, Michael Rovenolt, and Randy White, "Libya's Operation Odyssey Dawn: Command and Control," *PRISM* 3, no. 2 (Washington, DC: NDU Press, March 2012), 141–156.

[21] NATO Secretary General Fogh Rasmussen, "NATO to maintain high operational tempo as long as necessary in Libya," April 14, 2011, available at <www.nato.int/cps/en/natolive/news_72549.htm?>.

[22] Ralph Jodice, "Operation *Unified Protector* Mission Brief," lecture, Air War College, Maxwell Air Force Base, October 9, 2012.

[23] This was a common problem in NATO Air in strategy and intelligence positions.

[24] The CJTF Headquarters had a limited number of senior Airmen on the staff to help provide an airpower perspective, which was significant as this was an air-centric campaign. Yarbrough, interview by author, January 11, 2013.

[25] For military assets available, see Adrain Johnson and Saqeb Mueen, eds., *Short War, Long Shadow: The Political and Military Legacies of the 2011 Libya Campaign*, Whitehall Report 1-12 (London: Royal United Services Institute, 2012), available at <www.rusi.org/downloads/assets/WHR_1-12.pdf>. For discussions on platform coverage issues, see McCaffrey, email January 3, 2013, and multiple discussions with author.

[26] On average, the number of strike sorties flown was in the mid 40s.

[27] These regional divisions were not independent strategies. Rather, this strategy sought to apply limited resources to protect civilians while coercing hostile forces to cease attacking civilians.

[28] The senior national representatives (SNRs) were also known as "Red Card Holders" for their ability to raise the "red card" and stop national involvement if they were asked to exceed their national mandate. The CFACC and CFACC director did their best to turn this into a "Green Card" relationship using inclusion, transparency, and regular SNR/CFAC meetings. The national level of responsibility held by these officers, often colonels and lieutenant colonels, was substantial and their dedication and conduct is noteworthy.

[29] U.S. tools and weaponeers were eventually located in the combat operations division and NATO largely adopted U.S. Collateral Damage Estimate methodology. Standard operating procedures were developed and guided the chief of combat operations, senior intelligence duty officer, legal advisor, and National "Red Card Holder" in quickly assessing a situation and, when warranted, asking for senior officer approval for target engagement.

[30] For information on the Hellfire II missile, see Lockheed Martin, "Hellfire II Missile," available at <www.lockheedmartin.com/us/products/HellfireII.html>.

Patriot Missile operator adjusts launcher settings during field training (U.S. Air Force/Maeson Elleman)

Silent Watch
The Role of Army Air and Missile Defense

By Michael S. Tucker and Robert W. Lyons

On March 29, 2013, North Korean President Kim Jong Un continued his public provocation and stated that it was time to "settle accounts" and directed his missile units to prepare to strike U.S. mainland and Pacific military bases. The next day North Korea declared it had entered a state of war with South Korea and had already deployed missile units to the North Korean coast.[1] Roughly 7,000 miles away, these North Korean declarations generated action in the Pentagon and across the Department of Defense (DOD). Officers from the Office of the Secretary of Defense, Joint Staff, and Army were called to assess the situation and suggest potential solutions. Other key players in the planning process included the 32nd Army Air and Missile Defense Command (AAMDC) and 94th AAMDC teams that perform the missile defense planning, integration, and coordination for theater missile defense operations. The planning resulted in the Secretary of Defense deploying A Battery, 4th Air Defense Artillery (A-4 ADA) Terminal High Altitude Area Defense (THAAD), to Guam. THAAD is a unique and cutting-edge missile defense system that provides persistent defensive

Lieutenant General Michael S. Tucker, USA, is Commander of First Army, Rock Island, Illinois. Colonel Robert W. Lyons, USA, is Chief of Staff, 94th Army Air and Missile Defense Command. When this article was written, Lieutenant General Tucker was serving as Deputy G-3/5/7 Headquarters, Department of the Army (HQDA), and Colonel Lyons was serving as Air and Missile Defense Director, HQDA, G-3/5/7.

Two THAAD interceptors launched during test, which resulted in intercept of one MRBM target by THAAD and one MRBM target by Aegis Ballistic Missile Defense (DOD)

capabilities to defeat a wide range of stressing ballistic missiles in either the exoatmosphere (outer space) or the endoatmosphere. This capability was so new that only two THAAD batteries existed. Though A-4 ADA was maintained at heightened alert status, the order directed the battery to deploy in significantly less time. As a testament to the high degree of proficiency and professionalism of the Soldiers and leaders involved, A Battery, 4th Battalion successfully deployed in 7 days and attained full operational capability in 15 days—weeks ahead of predicted planning cycles.

The effect of the ongoing THAAD deployment to Guam cannot be overstated, as it assures U.S. allies and partners by demonstrating commitment to a country or region. THAAD provides critical persistent ground-based homeland missile defense for Guam and its key civilian and military sites. Additionally, it enables dual-mission *Aegis* ships to perform air and missle defense (AMD) and other critical missions for the geographic combatant commanders. No other Service has this capability or can achieve this effect. DOD understands that Army AMD remains the cost-effective, persistent solution to address the enduring requirements of the new DOD strategy.[2] This one event and its effect illustrate both the strategic importance and the increased operational demand for AMD. Chief of Staff of the Army General Raymond T. Odierno stated, "Whether it's missile defense, whether it's to build partner capacity, whether it's to put some small element on the ground to do work or operationally employ it to protect some U.S. interest, that's what we're looking to do."[3]

Events in North Korea and Syria are only the most recent demonstrations of the critical role AMD plays in today's strategic environment. The deployments of THAAD to Guam coupled with the Patriot missile system to Turkey further validate the thinking that Army missile defense systems are key strategic (or geopolitical) tools for the geographic combatant commands. Army AMD Soldiers provide an enduring presence to "1) demonstrate U.S. commitment to a region, 2) create the ability to partner with allies there, and 3) provide a deterrent or calming perspective."[4] Additionally, as the wars in Iraq and Afghanistan wind down, the Army and other Services are transitioning from a combat force to a force of deterrance. Army AMD is central to the deterrence mission, providing persistent and credible defensive capability, assuring allies with U.S. presence, and providing operational access for the joint team.

A combination of strategic factors has elevated the importance of Army AMD capability. They include threats that have evolved in capability, complexity, and capacity; a defense strategy and policy that place a high value on an enduring deterrence capability; and an increasing need to maintain joint operational access to distant regions of the world. These strategic factors have increased the operational demand on the Army's existing AMD force. In the Army's G-3/5/7, we have a front-row seat to those demand signals through the Global Force Management Board process and other forums. We work with the Army staff, Missile Defense

Agency (MDA), combatant commanders, and others to ensure the Army will continue to provide the capability needed.

It has been more than a year since Army Secretary John McHugh and Chief of Staff General Odierno approved the AMD strategy, which was written to synchronize the stakeholders' efforts in developing the future AMD force. Since then, the Nation and the Army entered a time of sequestration, continuing resolutions, and increasing conflicts around the world. For Army AMD, what should have been a straightforward year of executing the approved strategy has additionally become a year of reacting to ever-increasing demands for AMD in a time of increasingly constrained resources:

> *The United States faces profound challenges that require strong, agile, and capable military forces whose actions are harmonized with other elements of U.S. national power. Our global responsibilities are significant; we cannot afford to fail. The balance between available resources and our security needs has never been more delicate.*[5]

A new set of AMD capabilities is being developed and will significantly change the way Army AMD forces deploy, employ, and fight. Game-changing systems such as the Integrated Air and Missile Defense (IAMD) Battle Command System (IBCS) and Indirect Fire Protection Capability Increment 2 Intercept Multi-Mission Launcher (MML) weapon system will allow us to be more globally responsive, less constrained by command and control linkages, and better able to organize forces at the component level.

The Army AMD force is changing to meet the increasing demands of the joint warfighter. This article examines the strategic environment and the role of the Army's AMD team, reviews the Army's AMD strategy one year later, and considers the implications for the joint force.

Army's Directed Role

Providing AMD for the joint force has long been an Army mission. DOD Directive 5100.01, "Functions of the Department of Defense and Its Major Components," directs the Army to "Conduct air and missile defense to support joint campaigns and assist in achieving air superiority."[6] Significantly, no other Service is so charged. The Navy is directed to "Conduct ballistic missile defense,"[7] and the Air Force to "Conduct offensive and defensive operations, to include appropriate air and missile defense."[8] This is not to imply the other Services have small roles. Indeed, the Navy and the MDA have invested billions and achieved incredible capability to destroy ballistic missiles before they reenter Earth's atmosphere. The Air Force often serves as the higher headquarters for AMD operations, integrating Services, systems, fighters, radars, and even coalition partners to protect against an array of threats on a global scale. Nevertheless, only the Army is charged "to provide air *and* missile defense to support joint campaigns." That straightforward charge has become increasingly important in the current strategic environment.

The title of this article is deliberate. "Silent Watch" speaks to the critical and enduring role our AMD forces execute: deploy to faraway lands, often in or near harm's way, continuously "watching" for the first shot of the next war. When that shot comes—sometimes after months or even years—defeating the enemy can lead to greater operational and strategic flexibility for our leaders, greater control of escalation, maintaining coalitions, and even possibly helping to prevent that war. Every day, AMD forces are on Silent Watch around the world and at home. In addition to those deployed around the globe, 350 Soldiers of the Army National Guard protect 314 million Americans 24/7 from the threat of a rogue or accidental nuclear launch against the United States. Despite budgetary pressures, according to the recently released Quadrennial Defense Review 2014, the number one priority is defense of the homeland, which further highlights the criticality of the global missile defense mission area and directs increasing our capability and capacity with additional sensors and interceptors.

Defense Strategy

At a symposium in April 2011, Commander of U.S. Central Command General James N. Mattis stated:

> *We can reduce the desire for any nation to threaten our nations and our people, reminding adversaries that offensive plans with missiles cannot succeed, so don't even try. IAMD serves as an important manifestation of our collective protection and deterrent posture, and increases deterrence by reducing vulnerabilities.*[9]

In January 2012, the President and Secretary of Defense released the new defense guidance, *Sustaining U.S. Global Leadership: Priorities for 21st Century Defense*. It charted significant changes to defense policy including a rebalancing toward the Asia-Pacific region, a focus on preparing for asymmetrical warfare to include antiaccess/area-denial (A2/AD), a renewed emphasis on building partner capacity, and an acknowledgment of today's fiscally constrained environment. The defense guidance also highlights the following challenges relevant to Army AMD:

> *The United States must maintain its ability to project power in areas in which our access and freedom to operate are challenged. In these areas, sophisticated adversaries will use asymmetric capabilities, to include electronic and cyber warfare, ballistic and cruise missiles. . . .*[10] *With the diffusion of destructive technology, these extremists have the potential to pose catastrophic threats that could directly affect our security and prosperity.*[11]

This policy shift is taking place within the context of a global security environment that presents a multitude of security challenges for the Nation, the Army, and the Army's AMD forces. It also manifests a new concept called Joint Operational Access.

The Concept

The Joint Operational Access Concept (JOAC) focuses on how the joint force will achieve operational access against armed opposition that possesses A2/AD capabilities. A core component to achieving global access is the importance of setting preconditions, which could be forward deployment of forces, multinational exercises, or support agreements. The JOAC identifies one of the required capabilities as the ability to provide expeditionary missile defense to counter the increased precision, lethality, and range of enemy A2/AD systems.[12] "The U.S. requires a more geographically distributed, operationally resilient, and politically sustainable posture that allows persistent presence and, if needed, power projection. . . . This rapid response hinges on flexibility and forward positioning of permanent and rotational forces."[13] Army AMD has a significant role in setting preconditions for given regions and countering A2/AD capabilities in a nonescalatory manner, especially in early phases of conflict. For example, in the U.S. Pacific Command (USPACOM) area of responsibility there are three Patriot battalions, one THAAD battery, an Army AMD command center, and an Army Navy/Transportable Radar Surveillance (AN/TPY-2) radar forward stationed. These AMD units engage in multiple exercises with partners and allies. In the USPACOM region alone, we participate annually with the Republic of Korea's forces in Ulchi Freedom Guardian and Key Resolve exercises, with Japan's forces in Keen Edge and Keen Sword, and with our multinational partners in Terminal Fury and Talisman Saber. These AMD assets are on Silent Watch, providing force protection over critical power projection, command and control, and other strategic locations.

Threat

These challenges, as they relate to AMD, include a danger that has evolved in both capability and employment. The threats from rockets and unmanned aerial vehicles (UAVs) to cruise and ballistic missiles are increasingly more capable, longer range, and more precise. Ten years ago, the "circular error probability" of where an enemy missile would land was often measured in kilometers or tens of kilometers; in the future, Global Positioning Satellites and improved navigation will reduce that error to mere meters. UAVs are increasingly becoming "near real time" targeting devices capable of bringing lethal missiles on our forces in short order. The thinking enemy is increasingly practicing "complex integrated attacks," where multiple capabilities are brought to bear against a single target in a simultaneous raid to defeat air defenses.

Many countries view ballistic and cruise missile systems as cost-effective weapons and symbols of national power. In addition, they present an asymmetric threat to U.S. airpower. Key findings from the National Air and Space Intelligence Center's unclassified 2013 report *Ballistic & Cruise Missile Threat* highlight the evolution of threat capabilities. North Korea has unveiled the new road-mobile Hwasong-13 intercontinental ballistic missile (ICBM) while continuing to develop the Taepodong-2. Also in development are an intermediate-range ballistic missile and a solid propellant short-range ballistic missile (SRBM). By 2015 Iran could develop and test an ICBM capable of reaching the United States. In 2010, Iran revealed the Qiam-1 SRBM, the fourth generation Fateh-110 SRBM, and now claims to be mass-producing antiship ballistic missiles. It has modified its Shahab-3 medium-range ballistic missile (MRBM) to extend its range and effectiveness and also claims to have deployed the two-stage, solid-propellant Sejjil MRBM.

China has the most active and diverse ballistic missile development program in the world. It is developing and testing offensive missiles, forming additional missile units, qualitatively upgrading missile systems, and developing methods to counter ballistic missile defenses. It continues to field conventionally armed SRBMs opposite Taiwan and is developing a number of mobile, conventionally armed MRBMs. Missiles such as the Dong-Feng 21D ASBM are key components of a military modernization program specifically designed to prevent adversary forces' access to regional conflicts. Russia still has over 1,400 nuclear warheads deployed on ballistic missiles capable of reaching the United States, and although the size of the Russian strategic missile force is shrinking (with arms control limitations and budgetary constraints), development of new ICBM and SLBM systems is proceeding.

Land-attack cruise missiles (LACMs) are highly effective weapons systems that can present a major threat to military operations. At least nine foreign countries will be involved in LACM production during the next decade, and many missiles will be available for export.[14] These advances in threat capability and capacity have significantly increased the operational demand for AMD capability.

Demand

On July 17, 2013, in testimony before the Senate Appropriations Defense Subcommittee hearing on MDA's fiscal year 2014 budget, Vice Admiral James D. Syring stated, "I am working hard, as the new director, with the Army to find a way to the seventh and possibly eighth THAAD batteries. The system is needed, and the system is needed in more numbers, in my assessment and discussion with the combatant commanders."[15]

The demand for Army AMD is outpacing supply. During recent Congressional testimony, Lieutenant General Richard P. Formica, former Commanding General, Space and Missile Defense Command, commented that "Our analysis, reinforced by the 2012 Global BMD [Ballistic Missile Defense] Assessment [a recent senior-level tabletop exercise], reinforces the fact that GCC demands for missile defense capabilities will always exceed the available BMD inventory."[16] In addition to the aforementioned THAAD and Patriot units in Guam and Turkey, we had counterrocket, artillery, and mortar capabilities in the Iraq and Afghanistan conflicts, Patriot units in Poland and Jordan, and AMD sites in Japan and Israel. AMD forces will continue to be forward stationed and deployed in Korea, Japan, throughout the Gulf, and in Europe according to the President's priorities and Phased Adaptive Approaches for Europe, Asia-Pacific, and the Middle East. AMD's Patriot force is currently more than 40 percent forward deployed or forward stationed, and global demands for Patriot units continue to increase. Four of our five Joint Tactical Ground Station systems currently support overseas combatant commanders. As THAAD and AN/TPY-2 forward-based mode radars are fielded, requests for their deployment remain high as well.

We ask Soldiers to deploy to obscure sites, often with little preparation, in many cases breaking new ground for the Nation. They are as much diplomats for U.S. values as protectors of cities. Deployments are never rote; they require intensive command and leadership from all levels with extensive coordination between staffs and the host country to execute successfully. These deployments often call for nonstandard actions that speak to initiative and quick, effective decisionmaking to establish or sustain operations. Once deployed assets are operational, the pace remains at a high level with continual improvements to site security and procedures coupled with system maintenance to ensure units maintain a ready status. In addition, these deployments are not just 3- or 6-month tours: AMD units are some of the few remaining units that still deploy for 12-month rotations. Once employed, they normally stay and provide an enduring presence. Silent Watch becomes a lasting U.S. "foot in the door" for improved relations with host countries. We face a long-range threat with the knowledge that many lives are at stake if we fail. Thus we do everything within our power to ensure that failure is not an option.

Patriot missile mobile launcher and air defense equipment deployed to U.S. and NATO Patriot missile batteries at Incirlik Air Base, Turkey (U.S. Air Force/Charles Larkin, Sr.)

AMD Strategy

As noted, the Army published its first Service-wide AMD strategy in 2012. Its purpose is to articulate an overarching AMD framework that synchronizes Service functions in support of Army and joint missions. It describes where the Army plans to be in the future, how the AMD force is shaped to support the Army and the joint force, and what must be accomplished to succeed in the future operational environment. The AMD strategy is informed by the new defense guidance, resource challenges, proliferation of threat technology, and an era of persistent conflict. It also articulates expectations for 2016 and 2020 to aid DOD in keeping the AMD force and Army staff within this framework in the near- and midterm years. The strategy's desired outcomes are AMD's three imperatives: to defend the homeland, defend the force and critical assets, and assure access for our forces. To achieve these, the AMD strategy has four Lines of Effort:

- attain networked mission command
- enable defeat of the full range of air and missile threats
- build partner capacity and maintain forward presence
- transform the AMD force.

Innovation Is Key

With increasing threats and decreasing resources, the Army needed to develop significant new AMD capabilities quickly and affordably. The prior approach of developing stand-alone systems (for example, Medium Extended Air Defense, Surface Launched Advanced Medium Range Air-to-Air Missile, and Joint Land Attack Cruise Missile Defense Elevated Netted Sensor) was no longer affordable; we had to "break the mold" with AMD and develop capabilities that were integrated, joint, and multimission.

This led the Army to pursue an ambitious networked solution called Army IAMD. At the center of this effort is the IBCS program, which will not only serve as the Patriot's next generation command and control (C2) system but act as the single mission command system for all Army AMD. IBCS will also enable systems to work together, share data, and employ assets in new and more efficient ways.

IBCS will provide enhanced mission command capability for AMD leaders. It will increase the range of options available to the commander on the ground as he tailors the defense design down to component level employment rather than emplacement of whole batteries and systems. This IBCS-driven evolution will allow leaders to better manage the battle, with increased operational flexibility resulting in the right capability at the right location, enhanced ability to manage missile inventories, and added decision time for leaders to improve their ability to execute engagements. Army AMD is inherently a joint (and coalition) mission area—Air Force fighters and Navy *Aegis* ships team with Army AMD Patriot and THAAD systems to complete actions across the joint engagement sequence. When enabled, IBCS will network across the joint community and provide an exponential increase in integrating our joint fire control capability. The Army is working with the other Services to bring this capability to fruition. In addition, an IBCS-equipped force will potentially be able to leverage coalition AMD systems and further strengthen our efforts to build partnership capacity.

Like many Army and joint systems, today's AMD systems are "system centric," so each system has its own sensors, shooters, and C2. Patriot, for example, has Patriot launchers, Patriot missiles, and Patriot radar and is controlled by a Patriot Engagement Control Station at the battery level. IBCS will allow us to break that mold by putting individual platforms—launchers and radars—on the network. Each component will "join the fight" as it joins the network, and will allow innovative pairings of components. For example, an MML weapon system, Sentinel radar, or a Patriot battery could be paired together on the network to defeat a variety of threats.

Of the many capabilities that will benefit from IBCS, the MML deserves special mention as it will be loaded with several types of munitions. This single platform, coupled with Sentinel and other radars and commanded by IBCS, will address threats ranging from cruise missiles to UAVs to rockets, artillery, and mortars. The MML will become a critical complement to Patriot and provide the warfighter tremendous capability even in a resource-constrained environment.

Resource Constraints and AMD

On February 13, 2013, General Odierno, in testimony before the Senate Armed Services Committee, stated, "We are very focused on forward air and missile defense capability in our key theaters, both Asia-Pacific and other areas, to include the Middle East."[17]

As stated earlier, we are entering a prolonged period of constrained resources. No mission area is ever completely immune to across-the-board budget cuts. And the combined effects of sequestration and Continuing Resolutions will affect the AMD force more than the Army would like.

We offer that budgets are only one measure of priority. As the Army downsizes, force structure (that is, units and organizations) becomes a more visible indicator. By this metric, Army AMD is widely recognized as one mission area of a very select few that will grow in the coming years. Over the last few years, the Army has grown from one AAMDC to four, from zero THAAD batteries to seven, from 13 Patriot battalions to 15, and from zero counter-rockets, artillery, and mortar battalions to two. The AMD force is a very efficient use of manpower because it provides a strategic capability for the Nation at a very small investment in our most expensive resource, people. From tooth to tail the AMD force is less than a division's worth of military manpower across all components, which is very economical in a resource-constrained environment.

Army AMD is well postured to meet the current and emerging threat. We in the Army's G-3/5/7 have the privilege of representing Army AMD interests in a number of forums with the Office of the Secretary of Defense, MDA, the Joint Staff, and combatant commanders, as well as chairing monthly General Officer Steering Committees focused on the subject. Army leadership understands the strategic importance of AMD and is allocating resources in accordance with those priorities. This same leadership understands better than most the unique contributions and demands we ask of the AMD force. We all sleep better knowing that across the globe, tonight and for many nights to come, Army AMD professionals will maintain the Silent Watch. JFQ

Notes

[1] "North Korea: Timeline of Escalating Threats," *The Telegraph*, March 30, 2013, available at <www.telegraph.co.uk/news/worldnews/asia/northkorea/9962442/North-Korea-timeline-of-escalating-threats.html>.

[2] *Sustaining U.S. Global Leadership: Priorities for 21st Century Defense* (Washington, DC: Department of Defense, January 2012), available at <www.defense.gov/news/defense_strategic_guidance.pdf>.

[3] General Raymond T. Odierno, comments, American Enterprise Institute, July 28, 2013, available at <www.aei.org/events/2013/07/29/squaring-the-circle-general-raymond-t-odierno-on-american-military-strategy-in-a-time-of-declining-resources/>.

[4] Admiral Samuel J. Locklear III, interview, *Joint Force Quarterly* 69 (2nd Quarter 2013), 66.

[5] *Sustaining U.S. Global Leadership*, 8.

[6] Department of Defense (DOD) Directive 5100.01, "Functions of the DoD and Its Major Components," December 21, 2010, 29, available at <www.dtic.mil/whs/directives/corres/pdf/510001p.pdf>.

[7] Ibid., 31.

[8] Ibid., 34.

[9] General James N. Mattis, International Symposium on Air Defense 2020, remarks, April 17, 2011, available at <www.centcom.mil/press-releases/u-s-central-command-commander-addresses-international-symposium-on-air-defense-in-saudi-arabia>.

[10] *Sustaining U.S. Global Leadership*, 2.

[11] Ibid., 3.

[12] Chairman of the Joint Chiefs of Staff, "Joint Operational Access Concept," Version 1.0, January 17, 2012, 35, available at <www.defense.gov/pubs/pdfs/joac_jan%202012_signed.pdf>.

[13] Samuel J. Locklear III, "Testimony on U.S. Pacific Command in Review of the Defense Authorization Request for Fiscal Year 2014 and the Future Years Defense Program," 113th Cong., 1st sess., April 9, 2013, available at <www.pacom.mil/commander/14-us-pacific-command-review-defense-auth-request-fiscal-2014.pdf>.

[14] *Ballistic & Cruise Missile Threat* (Wright-Patterson Air Force Base, OH: National Air and Space Intelligence Center, 2013), 3, available at <www.afisr.af.mil/shared/media/document/AFD-130710-054.pdf>.

[15] Vice Admiral James D. Syring, director, Missile Defense Agency, testimony before the Senate Appropriations Defense Subcommittee, 103rd Cong., 1st sess., July 17, 2013, available at <www.hsdl.org/?view&did=740609>.

[16] Lieutenant General Richard P. Formica, statement before the Senate Armed Services Committee, Strategic Forces Subcommittee, 113th Cong., 1st sess., May 9, 2013, available at <http://missilethreat.wpengine.netdna-cdn.com/wp-content/uploads/2013/05/Formica_05-09-13.pdf>.

[17] General Raymond T. Odierno, testimony before the Senate Armed Services Committee, 113th Cong., 1st sess., February 13, 2013, available at <www.army.mil/article/96868/Feb__13__2013____CSA_Testimony_before_the_Senate_Armed_Services_Committee/>.

Citizens unload relief supplies in Gonaives, Haiti, from landing craft utility embarked on USS *Kearsarge* (U.S. Navy/Joshua Adam Nuzzo)

Leveraging U.S. Civilian Capabilities in Africa

By Charles D. "Buck" McDermott

> [A]*s currently structured, the international system for responding to natural disasters is neither as timely nor equitable as it could be. Funding is secured on a largely ad-hoc basis after disaster strikes.*
>
> —African Risk Capacity Response to the Cost-Benefit Analysis of the African Risk Capacity

Captain Charles D. "Buck" McDermott, USNR, is a graduate of the U.S. Naval War College Senior Course and U.S. Army School of Advanced Military Studies. He is also a retired captain in the U.S. Merchant Marine.

Development gains in Africa suffer major setbacks when governments are unable to respond effectively to crises. To address this concern, the U.S. military conducts regular exercises with partner nations that provide valuable training for U.S. and partner nation forces, improve interoperability, provide valuable services to the local communities, and build mutual trust and goodwill among participants and between nations. Regrettably, the U.S. budget crisis caused the Navy to cancel Continuing Promise 2013, U.S. Southern Command's biennial humanitarian assistance exercise. The irony in the name of this exercise—*Promise*—was likely not lost on the eight Caribbean and Latin American nations slated to participate. Will Africa Partnership Station exercises be canceled too?[1] What do these cancelations say about the United States as a reliable partner in Africa, and what or who will fill the void?

While the U.S. Government cannot afford to continue to engage as it has, to return to a policy of isolationism would be catastrophic. To maintain global stability, improve governance and economic opportunity in Africa, and spur its own economic growth, the United States "[has] to think." The Nation will reduce reliance on certain military capabilities and as a result will need to leverage civilian capabilities in unique and innovative ways. To that end, this article examines U.S. emergency response capability at all levels as a key strength of U.S. governance. The National Response Platform (NRP) and National Response Force (NRF) concepts are presented as means to "export" that strength to Africa. In addition these new tools of diplomacy will improve public-private partnerships to rebalance a whole-of-nation approach to stimulate economic growth and ensure long-term stability and security in Africa, the United States, and elsewhere.

Background

The United Nations (UN) Commission on Human Rights includes "responsiveness to the needs of the people" among its five key attributes of "good governance."[2] Not surprisingly, the governments of many African nations lack the capacity to meet even the most basic human needs much less the advanced capabilities necessary to respond effectively in the wake of disaster. In contrast, the United States has robust emergency response capabilities at the local, state, and Federal levels. Moreover, an equally robust legal architecture provides for rapid and effective coordination between levels of government and between departments and agencies at each level. Therefore, in domestic emergencies the military plays an important but supporting role limited by the Posse Comitatus Act, other U.S. laws, and military regulation. In foreign disaster assistance, however, the military often plays a crucial and highly visible role.

President George W. Bush was praised for his resolute leadership in the immediate aftermath of the September 11, 2001 terrorist attacks. The vast majority of responders at those sites were from the respective cities and states. While the President's support was welcome, local and state officials led the response and recovery—the mayor, the governor, the police and fire chiefs, hospital administrators, religious leaders, and nearby charities. The Bush administration also received international accolades for its rapid and perhaps overwhelming response to the December 2004 Indian Ocean tsunami, while only 8 months later, the administration was criticized for its response to Hurricane Katrina in New Orleans where the city's poorly maintained pumping system resulted in flooding and inadequate levees were breached by the tidal surge.

New Orleans was aware of the hurricane threat and had ample notice of Katrina's approach but was still woefully unprepared. Public perceptions of the Federal response to Hurricane Katrina and to the 9/11 attack in New York City were radically different. Did the failure in Louisiana occur in Washington, or in New Orleans or Baton Rouge? Thankfully, the massive Federal response in New Orleans resulted in only 1,833 lives lost.[3] That was tragic, but how many more would have died in similar circumstances in Africa? What would have been the consequences for governments able to provide only a limited response, a biased response, or no response at all? The solutions start at the local level.

It is said that "Every disaster is a local disaster [because] it is at the local level that the greatest challenges are faced and the toughest decisions are made."[4] That may be true, but in the aftermath of Katrina, it was the Federal Government, specifically the Federal Emergency Management Agency (FEMA), that was most severely criticized. Following the terrorist attacks of 9/11, FEMA had transitioned from an independent Federal agency to falling under the authority and direction of the newly created Department of Homeland Security (DHS). After Katrina, cooperation between the states, among the local, state, and Federal levels of government, and between the many departments and agencies at each level of government improved dramatically, leveraging preexisting frameworks.

Established in 1996, the Emergency Management Assistance Compact (EMAC) is an agreement by 54 states and territories to offer mutual assistance during governor-declared states of emergency.[5] EMAC allows states to send personnel, equipment, and commodities across state lines with credentials, licenses, and certifications honored in the supported state. EMAC also clarifies issues of liability and reimbursement.[6] Additionally, most sizable communities and all states have a designated Emergency Management department or agency. These local and state offices follow the guidelines established by DHS/FEMA in the National Incident Management System, National Response Framework, and the Incident Command System.

Indeed, there has been tremendous Federal investment in building local and state capabilities to ensure that, to the fullest extent possible, "local disasters" can be managed at the local level. When local capacities are overwhelmed or a unique capability is required, local authorities request assistance from the state. If the state is unable to meet the requirements of the local authorities in responding to a specific emergency, the governor of the state seeks the assistance of the Federal Government by making an official request, in writing, to the President.

The President might then make an Emergency or Major Disaster declaration and designate DHS/FEMA as the lead Federal agency for the response with other departments and agencies directed to support. This was the case in the Katrina response when FEMA assigned the Department of Defense (DOD) a mission for "full logistics support" at a cost FEMA estimated would be $1 billion.[7] Despite how it may have appeared in the media to outside observers, FEMA was in charge and the military had a supporting role. As a lesson learned, however, military officers and senior enlisted personnel now undergo extensive Defense Support of Civil Authorities (DSCA) training wherein they learn the importance of deferring media inquiries to public officials to avoid even the appearance of loss of civilian control and to facilitate the military's earliest possible withdrawal.

FEMA in turn recognized that it had to develop its own logistics capabilities relying on civilian government agencies and the private sector. As a result, the agency greatly increased the number and capacity of its warehouses and distribution centers. It also established retainer contracts with multiple transportation providers such as short- and long-haul trucks, buses, ambulances, passenger and cargo trains, and airlines. These providers agree to make assets available for hire under contract if a disaster is declared and FEMA or a subordinate agency identifies a requirement. This civilian-based response architecture promotes entrepreneurship, small businesses, and an increased capacity at the lowest possible level of government—a multilayered civilian approach to emergency response much needed in Africa.

Many recent changes within FEMA are a consequence of the Post-Katrina Emergency Management Reform Act of 2006, Title VI of P.L. 109-295 (H.R. 5441).[8] In conjunction with the Robert T. Stafford Disaster Relief and Emergency Assistance Act (Stafford Act), the Post-Katrina Act authorizes and funds FEMA to "lean forward" and position assets *in anticipation of* state requirements. As a result, the response to Hurricane Ike in 2008 was dramatically different.

As Ike advanced and its intensity and location of landfall were known to a reasonable degree of certainty, hundreds of trucks were put under contract. They were loaded at FEMA distribution centers and deployed to predetermined parking areas in an arc around the anticipated area of impact. Other assets were made ready at Federal airfields, typically on DOD installations, to be flown in by commercial or military airlift. As another lesson learned from Katrina, it was anticipated that rotary airlift would be in high demand in the first days of the response.

Senegalese marine commandos and U.S. Marines conduct martial arts training during Africa Partnership Station 13 (U.S. Marine Corps/Marco Mancha)

Two days prior to landfall, FEMA tasked DOD to operate USS *Nassau* (LHA 4) off Galveston Island for 17 days at a cost of $20 million—or a daily operating cost of $1.2 million.[9] In addition to helicopter support, USS *Nassau* utilized landing craft to transport vehicles and heavy equipment—Humvees, backhoes, and front-end loaders—and about a thousand Sailors and Marines to support debris clearance and other requirements.[10] USS *Nassau* had been specially outfitted prior to her departure from her home port in Norfolk. Still, due to configuration as a naval combatant, the ship carried relatively little of the supplies and equipment needed for a disaster of this type and magnitude. Accordingly its overall contributions were limited, particularly given the costs.

The tremendous cost of using naval combatants in disaster response must be taken into consideration with the frequency, intensity, and predictability of disasters that come from the sea. Further, populations living on or near the coast are growing globally to say nothing of the unique challenges of responding to island disasters. For example, FEMA's response to the tsunamis that struck American Samoa in September 2009 exemplifies the problems of relying on airlift. These include the enormous cost of air transportation, aircraft availability, cargo volume and weight limitations, airfield congestion, and fuel consumption rates. In the likely event that aircraft fuel is limited or not available at the disaster site, aircraft cargo capacity is further limited by the necessity to carry sufficient fuel for the return flight. Otherwise, military aircraft with aerial refueling capacity are required.

In the American Samoa tsunami response, U.S. military C-17 aircraft delivered 667.5 tons of supplies in 10 days from Hawaii to American Samoa, a straight-line distance of 2,560 miles. The cost was $2.35 million, which translates to $235,000 per day, or $3,521 per ton.[11] For comparison, 667.5 tons would fill 28 standard 20-foot ocean shipping containers.[12] That is less than 1 percent of the "average" merchant container ship capacity of 3,000 to 7,000 containers. Steaming at 15 knots, a merchant ship could have delivered tens of thousands of tons of disaster relief supplies and equipment in just 6 days. If the ship was carrying only those 28 containers, the cost would still have been only about $120,000—around $20,000 per day or $180 per ton—a savings of over $2 million, or more than $3,000 per ton.

Similarly, in response to the Haiti earthquake on January 12, 2010, there was again tremendous reliance on airlift. A great number of naval combatants from the United States and other nations responded as well. However, many nations including America also sent merchant ships that carried vastly more supplies and equipment than responding aircraft and, as discussed in the previous case, were far more economical. Because the seaport at Port-au-Prince had been rendered inoperable by the earthquake, several vessels used onboard cranes, barges, and other small craft to discharge cargo from sea to multiple points ashore. Some ships also provided substantial sustainment for responders and survivors.[13] As impressive as the global response to Haiti's earthquake may have been, it was nonetheless ad hoc and expensive, and resulted in questionable long-term success.

National Response Platforms

In view of these recent cases, discussions at various levels of the U.S. Government and the private sector have generated many concepts for a capability to improve the effectiveness and efficiency of disaster response "from the sea." One such concept, National Response Platforms, is modeled on the U.S. Marine Corps Maritime Prepositioning Force program wherein a number of specially constructed ships are strategically located and loaded with the supplies and equipment necessary for the Marines to respond rapidly to any number of national security contingencies.

Put simply, the NRPs are "floating warehouses": U.S.-flag merchant cargo ships manned by U.S. merchant mariners and loaded with U.S.-manufactured disaster response supplies and equipment. They are able to self-offload in port or at sea, support helicopter operations, and provide additional communications, berthing, and messing capacity. NRPs would be located near areas prone to or threatened by disaster: the Gulf Coast during hurricane season, Presidential inaugurations, meetings of global leaders, or humanitarian crises. They might eventually be purpose-built ships, but there are numerous vessels owned by the U.S. Government or available on the global market that could suffice as interim platforms for proof of concept.[14] Still, obtaining the ships is perhaps the easier problem to solve.

The more challenging issues are likely to be getting the money for operation and maintenance of the ships, the supplies and equipment to make up the cargo, and the manpower to operate the ships and to load, unload, and employ the cargo. Limited Federal funds currently allocated to strategic assets and engagements could be supplemented by contributions from corporate and private donors. The cargo likewise might include government items but would ideally be made up primarily of items contributed by private and corporate entities to include nongovernmental organizations (NGOs). Creating these public-private partnerships would be no small feat and would directly challenge existing paradigms. Any necessary legislation would be equally complex, if not more so, as it would cross into foreign affairs, homeland security, and defense. Still, some might argue that organizing the *people* would be the greatest challenge. The NRP concept provides one possible solution.

National Response Forces

There are about 1.5 million NGOs operating in the United States.[15] Roughly 64.5 million citizens volunteered at least once in 2012.[16] Americans donated $298.42 billion to charity in 2011.[17] As DOD budget constraints necessitate reductions in military force structure, tens of thousands of veterans—disciplined, dedicated, and highly skilled in expeditionary operations—will be entering the civilian workforce. These facts notwithstanding, it seems very unlikely that the American public would support the creation of a new national force to respond to problems in Africa or elsewhere overseas with so many problems at home such as crime, poverty, access to health care, education, and infrastructure.

The NRF concept proposes a civilian *reserve* force that would focus on ongoing domestic issues but would also be utilized for foreign planned engagements and disaster response. Teams would be made up of professionals from the public and private sectors that might include current and past mayors, city council members, police and fire chiefs and their administrative staffs, hospital, school, and court administrators, small business and franchise owners, and countless volunteer organizations. Teams would include doctors, nurses, lawyers, policemen, firefighters, construction workers, teachers, clerks, and others. NRF teams would be based in major U.S. cities with a core cadre of foreign service, emergency management, and military veterans that would coordinate and lead these local professionals.

One possible framework for resourcing NRF teams requires partnerships, cooperation, and cost-sharing among the levels of government. To retain NRFs as a Federal asset through DHS, the Federal Government could pay wages and the cost of interstate and international travel. State governments could provide housing and intrastate and local transportation. Local governments could provide health care and the supplies and equipment needed to conduct the necessary work on local projects.

Modeled on the military's Reserve force structure, NRF teams would be in an Active, standby, or Reserve status. Indeed, DOD experience and infrastructure could be leveraged in standing up this civilian capability. NRF team core cadres would facilitate training specific to interstate or foreign deployment in coordination with the appropriate local, state, and Federal departments and agencies. Training in a specific skill or trade would not be required because team members would be recruited specifically for already having the required skills.

NRF teams would perform Active service in a domestic problem area identified by DHS in coordination with the states. Other teams would support planned foreign engagements facilitated by interagency agreement with the Department of State and U.S. Agency for International Development (USAID). In either case, due consideration would be given to the length of these assignments to balance costs in terms of travel and the requirement for more team members against the stress on team members and their families, communities, and civilian employers. Finally, other teams in their year of Active service might be held in "Reserve" to respond rapidly to domestic or foreign crises.

NRP and NRF Teams in Africa

While Africa's future is indeed uncertain, its people can be assured of some things. There will be times of instability. There will be natural disasters, some minor and easily manageable and others catastrophic. There will be manmade disasters, some caused by accident and others by intent. Kenya's National Disaster Response Plan (2009) recognizes a number of risks common to African nations to include "drought, famine, food insecurity, floods, epidemics, landslides, sea waves, tsunamis and technological hazards, deforestation, desertification, transport accidents, conflicts, pollution, structural failure, terrorism, fires, and others."[18] NRP and NRF teams, through planned engagement and in responding to crises, will help African nations build up their own strong civilian institutions to ensure continued good governance during peaceful times and in crisis.

Some have argued that the United States should assist African governments in increasing civilian skills for their military officers and senior enlisted so each country's military can resolve infrastructure, development, and stability crises.[19] While this might improve response capacity at the national level in the short term, it is not the right answer. It deprives the larger population of economic opportunity and eliminates future employment options for military members transitioning out of the military into civilian life. It also denies local leaders the capabilities necessary to respond to their own emergencies and could thereby undermine the authority of civilians at all levels of government.

Others might say the NRP and NRF concepts are too complex or even naïve to be executed. Given the current dysfunction of the U.S. Congress, that may well be true. Still others might offer that private entities such as the Bill and Melinda Gates Foundation, the Howard G. Buffett Foundation, or similar philanthropic organizations would be more successful in distilling the vision and putting together the relevant stakeholders to pull off a project of this scale. This may also be true. But the result would increase capability in NGOs that by definition cannot be directed by the U.S. Government to achieve national security objectives. Consequently, U.S. foreign engagement would continue to be haphazard and would further undermine confidence in the U.S. Government.

Many benefits can be derived from the NRP and NRF concepts. First, media images of American citizens helping African citizens in this way provide good press for the United States and restore confidence in America's ability to lead. NRP and NRF teams would reduce reliance on U.S. military forces and capabilities and would fill the voids left as a result of military budget constraints. NRPs could create or sustain thousands of American jobs in manufacturing and transportation and might also provide overseas business opportunities for U.S. manufacturers. Importantly, NRPs could "shore up" the American merchant marine, shipbuilding, ocean shipping infrastructure, and other national strategic capabilities that are so vital to a maritime nation.

Likewise, NRFs would reduce misperceptions about U.S. forces being employed in sovereign countries or U.S. naval combatants "lurking" offshore. In Africa, where so many nations have extensive experience with coup d'états and military-backed dictatorships, NRFs might serve to strengthen public confidence in civilian institutions. As African governments build emergency response capabilities at the local, state, and national levels, they improve their responsiveness to their people's needs. Political stability ensues followed by economic investment, economic growth, and improvements to infrastructure, healthcare systems, education, etc.

Vignette: U.S. NRFs in Africa

A hypothetical scenario describes how African nations would benefit from the NRP and NRF concepts. At some future point, NRPs are located here at home and around the world. NRPs in U.S. ports fall under the authority of DHS/FEMA. NRPs in foreign ports come under the authority of State/USAID. All NRPs are loaded with the supplies and equipment primarily intended for State/USAID-led planned engagements but equally useful for humanitarian assistance, disaster response, and civil support operations, to include theater-opening capabilities should normal sea- and airports prove inadequate, not available, or nonexistent. Increased reliance on commercial air carriers to transport NRF teams has allowed U.S. carriers to increase commercial aircraft capabilities, perhaps to include aerial refueling, and to expand business domestically and abroad.

In this near-future world scenario, two NRPs are in the Africa region. Each is operated by a U.S. shipping company under contract to the Department of Transportation's Maritime Administration (DOT/MARAD), Department of the Navy's Military Sealift Command, or perhaps even American Red Cross. A standby ship is in Monrovia, Liberia, supporting routine partnership engagements and training. The second NRP is on a State/USAID–planned development engagement in Dar es Salaam, Tanzania.

This hypothetical scenario continues with a pipeline explosion in Lagos, Nigeria.[20] Hundreds are killed and thousands are injured. Many more are displaced or otherwise affected. There is widespread social unrest. The government has insufficient resources to adequately respond to the crisis and requests international assistance. The UN requests that the United States employs the Standby NRP and the ship departs Monrovia for Lagos. NRF standby forces depart from the United States. In addition, State and USAID surge select personnel from Tanzania.

State, USAID, and NRF personnel respond to the crisis in support of the Nigerian government and in coordination with the UN and other contributing nations. U.S. military forces are not required because providing civilian capabilities to support the disaster response has freed up sufficient Nigerian forces to maintain security. However, neighboring militaries are put on alert. If additional forces are required over the next several weeks, they will be provided by African nations under the auspices of the Economic Community of West African States, the African Union, or the United Nations.

As our fictional crisis moves from response to recovery, NRF teams return to the United States. Personnel from State and USAID continue to assist Nigerians with long-term recovery. NRPs return to the United States for maintenance, repairs, and reload, but the supplies and equipment it delivered remain in Nigeria. U.S. private-sector partners engage with Nigerians on training, maintenance, future sales, and possibly future manufacturing contracts to enable Nigerians to respond more effectively to disasters in their country and throughout the region.

The United States has remarkable capabilities at all levels of government to respond effectively to domestic emergencies. To improve governance and economics in Africa, Washington needs to "export" those capabilities. The Department of State, DOD, USAID, various other Federal and state departments and agencies, and multitudes of NGOs often present a disjointed U.S. foreign policy. The NRP and NRF concepts provide an opportunity to coordinate these efforts into a more focused whole-of-nation approach. As standards of living improve across Africa, its nations become thriving markets for U.S. products and services. Moreover, African nations become net contributors to global stability and economic growth. As they have throughout the history of this great nation, unique and innovative ideas combined with Americans' determination will secure the U.S. position as the economic, ethical, and moral leader of the world. JFQ

Notes

[1] U.S. Africa Command's annual African Lion exercise, involving 1,400 U.S. Servicemen and 900 Moroccan troops, was canceled not for budgetary reasons but by the Moroccan government in protest over U.S. support of a United Nations (UN) effort to monitor human rights in the disputed territory of Western Sahara. "Morocco cancels war games with U.S. over rights," *USA Today*, April 16, 2013, available at <www.usatoday.com/story/news/2013/04/16/morocco-cancels-war-games-with-us-over-rights/2089089/>.

[2] UN Human Rights, Office of the High Commissioner for Human Rights, "Good Governance and Human Rights," available at <www.ohchr.org/EN/Issues/Development/GoodGovernance/Pages/GoodGovernanceIndex.aspx>. Transparency, responsibility, accountability, participation, and responsiveness are the UN's key attributes of good governance.

[3] Richard D. Knabb, Jamie R. Rhome, and Daniel P. Brown, "Tropical Cyclone Report: Hurricane Katrina: 23–30 August 2005," (National Hurricane Center: December 20, 2005; updated September 14, 2011), 11, available at <www.nhc.noaa.gov/pdf/TCR-AL122005_Katrina.pdf>.

[4] W. Nim Kidd, Chief, Texas Division of Emergency Management, "Texas Emergency Management Executive Guide, Revised 3/5/2013," available at <www.txdps.state.tx.us/dem/GrantsResources/execGuide.pdf>.

[5] Emergency Management Assistance Compact (EMAC), P.L. 104–321, 104th Cong., 2nd sess., October 19, 1996.

[6] "What Is EMAC?" EMAC Web site, available at <www.emacweb.org/index.php/learnaboutemac/what-is-emac>.

[7] U.S. Senate, "Statement by Paul McHale, Assistant Secretary of Defense for Homeland Defense, Before the 109th Congress Committee on Homeland Security and Governmental Affairs," February 9, 2006, 8. The symbol "$" in this report indicates U.S. dollars.

[8] U.S. Congress, "Post-Katrina Emergency Management Reform Act of 2006," Title VI of P.L. 109-295 (H.R. 5441), October 4, 2006, available at <www.gpo.gov/fdsys/pkg/PLAW-109publ295/pdf/PLAW-109publ295.pdf>.

[9] Federal Emergency Management Agency (FEMA), Mission Assignment #3294EM-TX-DOD-06, September 11, 2008, "Assistance Requested: Request DOD provide large platform ship capable of supporting 24/7 disaster recovery operations. Should be capable of handling both civilian and military helos, capable of refueling helos, possess landing craft to move USAR assets, have comms capability, and be able to provide temporary medical facilities with 500 beds. Request asset be available in 48 hours of landfall. Total Cost Estimate: $20,000,000."

[10] Nicholas J. Sabula, "USS *Nassau* Delivers Critical Help to Galveston," *Air Force News Agency*, September 19, 2008, available at <www.af.mil/news/story.asp?id=123116146>.

[11] U.S. Pacific Command, "HA/DR Samoa SAAM Missions" spreadsheet and "Disaster Relief–Samoa (30 Sept—UTC)" briefing slides. Cost estimates include return trip, empty or with return cargo or personnel. This does not include, nor is it intended to negate, the relief supplies flown in by FEMA; contracted, other government, intergovernmental organizations; or nongovernmental organizations (NGOs).

[12] The capacity of a standard shipping container, a 20-foot equivalent unit, is 48,000 pounds (21,600 kilograms).

[13] Mike Neuhardt, "Lummus and JLOTS Lift Hearts in Haiti," *Sealift*, March 2010, available at <www.msc.navy.mil/sealift/2010/March/lummus.htm>.

[14] Department of Transportation Maritime Administration, "The Maritime Administration's Ready Reserve Force," available at <www.marad.dot.gov/ships_shipping_landing_page/national_security/ship_operations/ready_ reserve_force/ready_reserve_force.htm>; Gavin Van Marle, "More and more container ships idling in Singapore," *Shipping News and Views*, November 14, 2012, available at <http://shippingnewsandviews.wordpress.com/2012/11/14/more-and-more-container-ships-idling-in-singapore/>. The U.S. Government owns 46 merchant cargo ships that are largely sitting idle in the Ready Reserve Force fleet. The current economic slowdown has left many owners with their ships underutilized.

[15] Department of State, "Fact Sheet: Non-Governmental Organizations (NGOs) in the United States," available at <www.humanrights.gov/wp-content/uploads/2012/01/Fact-Sheet-NGOsInTheUS.pdf>.

[16] Department of Labor Bureau of Labor Statistics, "Volunteering in the United States, 2012," February 22, 2013, available at <www.bls.gov/news.release/volun.nr0.htm>.

[17] Michelle Nichols, "U.S. charitable giving approaches $300 billion in 2011," Reuters, June 19, 2012, available at <www.reuters.com/article/2012/06/19/us-usa-charity-idUSBRE85I05T20120619>.

[18] Republic of Kenya, Office of the President, "National Disaster Response Plan 2009," Ministry of State for Special Programmes and Ministry of Provincial Administration and Internal Security, National Disaster Operation Centre, available at <www.sprogrammes.go.ke/index.php?option=com_content&task=view&id=265&Itemid=162>.

[19] Diane E. Chido, *Civilian Skills for African Military Officers to Resolve the Infrastructure, Economic Development, and Stability Crisis in Sub-Saharan Africa* (Carlisle, PA: U.S. Army War College, Strategic Studies Institute, March 2011), available at <www.strategicstudiesinstitute.army.mil/pdffiles/pub1047.pdf>.

[20] A pipeline explosion in Nigeria is not outside the realm of possibility as this did occur on December 26, 2006.

Army corporal explains Standard Army Retail Supply System to Albanian army officers at U.S. Property and Fiscal Office warehouse in Lawrenceville, New Jersey (U.S. Air Force/Mark Olsen)

The Case for the Junior Joint Logistics Officer Training Program

By Wilson T. VornDick

Roughly 1,700 junior officers (O1-O3) matriculate annually into one of five Service-specific logistics officer-training courses. Each course has its own staff, support, curriculum, budget, travel funding, and school. But with reduced resources during the multiple-year Continuing Resolutions, sequestration, and long-term declining budget horizon, the Department of Defense (DOD) needs to recognize that resources allocated in otherwise redundant processes are a waste. These costly redundancies can drain the overall health of the national security budget environment and create resource imbalances.

DOD already has been on a steady trajectory to become more streamlined, joint, and efficient since the Goldwater-Nichols Department of Defense Reorganization Act of 1986 required more joint doctrine, training, and policy.[1] If the axiom "business is business" applies to DOD, then why does the department allow five distinct business models and curricula to exist where there is currently redundancy of effort? Why is there not combined or joint junior-level logistics training among

Lieutenant Commander Wilson T. VornDick, USNR, is a Supply Corps Officer. He previously served on the Director of the Navy Staff and at the U.S. Naval War College while completing separate advanced degrees at Harvard University and the U.S. Naval War College.

the Services if 1) the Defense Logistics Agency (DLA) and U.S. Transportation Command (USTRANSCOM) are logistics *headquarters* with intermediate- and senior-level logisticians completing one or multiple joint tours there, and 2) the current model gears its graduates toward that same professional objective?[2]

There are significant differences in the ranks, tasks, and courses that each Service assigns its organic logisticians, but there are still *core business fundamentals* and *competencies* that are shared. These include but are not limited to food service operations, contracting, inventory control, supply chain management, environmental procedures, procurement, accounting, and disbursement. Ethics, stewardship, and accountability apply to each logistics professional and should not require distinct instruction—no matter whether the student wears a khaki, blue, or green uniform. At first glance it would seem that each Service is basically operating its own business school even though the graduates eventually end up at the same professional endstate with only different entry-level instruction. DOD has instituted mid-level and senior-level logistics training with varying degrees of success in the past. However, this cross-Service article proposes that DOD should institute a holistic and unified approach to training from the entry level up through the Junior Joint Logistics Officer Training program (J2LOT) instead.[3]

Status Quo of Logistics

Logistics is no longer a second-rate community or subspecialty. It is not the refuge of last resort for flight school and infantry washouts. Over the last few years, each Service has methodically and purposefully enhanced its logistics community standards by raising the bar of admission. Active and Reserve logistics selection communities currently require previous business coursework, MBAs, a unique logistics skill set, or significant prior business experience among the qualifications for a competitive application package. The Services' positions have only been enhanced by the weakened economy and attractiveness of skilled veterans in both the private and public sectors.

Logistics Officer Matriculation. The nearly 1,700 Reserve and Active-duty officers who matriculate annually come more highly qualified than previous entrants. Surprisingly, the Army makes up almost two-thirds of this number with about 900 training at the Army Logistics University in Fort Lee, Virginia.[4] The Army is unique in that it subdivides logisticians into three main support roles under the Sustainment umbrella: Transportation, Ordnance, and Quartermaster. It is important to point out that the Army dwarfs the other Services precisely because it rolls up the National Guard and Army Reserve into its training progression. Meanwhile, the Navy trains around 380 Supply Corps officers, or "chops" as they are affectionately called, at its education center in Newport, Rhode Island.[5] After completing the Basic School, nearly 200 Marine officers attend the Basic Logistics Training portion of the Marine Corps Combat Service Support School at Camp Lejuene, North Carolina. The Air Force's 37th Training Wing, based at Lackland Air Force Base, Texas, trains approximately 150 officers for three logistics communities: Logistics Readiness, Financial Management, and Force Support. Finally, the Coast Guard instructs the smallest number of officers (fewer than 40) through its Acquisition and Engineering community.

Duration and Progression of Training. The length for course completion ranges from 55 days for the Marines to over 5 months for the Navy, with the length of the Army and Air Force programs falling in between. The curriculum duration is completely dependent on each Service's combination of courses, timing of candidate matriculation, and curriculum length.[6] The Army is very specific in breaking its overall training into various segments throughout the first few years of its officer continuum; the Army's training command has various requirements beyond just logistics training to incorporate in its Army officer corps. The Navy, however, takes a more direct route. Once the initial officer accession/indoctrination is completed either through the Naval Academy, Officer Candidate School, Reserve Officer Training Corps, or other accession program, an officer is then enrolled in the 5-month Supply Corps Basic Qualification Course. The graduate will then "roll" to the first 2–3 year tour[7] in the fleet unless that supply officer is filling a more senior or technical position. In that case the officer will receive follow-on training such as the Supply Officer Department Head Course. This situation is rare and only applies to a handful of officer selectees annually. Otherwise, most graduates will go on to complete their first tour and will not receive any additional formal training in Newport.

The Air Force training method echoes the aforementioned Navy process. Once logisticians are accepted into the community, they begin the 5-month Logistics Readiness Officer Orientation Program (LOOP), which incorporates sequential training modules intended to prepare logistics officers for their first tours as well as completion of a core logistics competency. After graduation, Air Force logistics community members will continue with their own unique check-in-the-box, follow-on training, and milestones. These include qualification pins, specialty codes, MBA programs, internships, joint assignments, and placement at DLA, USTRANSCOM, or with the Joint Chiefs of Staff (JCS). This progression is replicated in the other Services. Each follows the same general professional and career progression despite their different approaches in training length and placement. This replication and redundancy of effort is also manifested in the training material.

Training Material. The overall training substance among the Services has remained generally the same despite the fact that each Service's publications would seem to hide their similarities behind their distinct formats and styles commensurate with their Service traditions. Food service operations, contracting, inventory control, supply chain management, logistics analysis, environmental procedures, procurement, accounting, fuels management, and disbursement have a place in each Service's entry-level publications and training material. These materials are synced or piggybacked with the initial training received at the entry-level training center, follow-on training, or hands-on training conducted during the first few assignments. Often these same materials are reincorporated later for more senior and specialized logistics positions at DLA, USTRANSCOM, or JCS.

Most of the training materials are synonymous with other Services concerning the actual logistics job functional areas. To clarify, aviation is a component of each Service. As a result, each Service exposes its logisticians to some form of aviation supply chain management. The actual personal qualification standards (PQS) and approach to training may vary, but aviation supply chain fundamentals are relatively the same. This is also true with food service operations. The *Army Food Program* and the Navy's *Food Service Operation Handbook* and *Food Service Management* (P-486) are cases in point.[8] There are cosmetic differences such as acronyms usage and military roles and responsibilities, but the guidance and instructions are in line. The various logistics officer communities may have different accession numbers, training locations, uniforms, and PQS, but the job requirements and training material are equivalent. Once again *core business fundamentals* and *competencies* are mirrored in each Service's entry-level training program.

Short-term Gains with Long-term Efficiencies

Millions are spent annually in operating each Service's entry-level logistics officer training pipelines. The most expensive variable is the fixed cost of operating and maintaining the training commands (salaries, installation maintenance, and support). While the disparity in per diem rates and other support costs per student could be significant depending on location, some costs are uniform among the Services such as baseline military salaries. Yet it is almost impossible to capture the full cost of the programs because each Service utilizes its own accounting methodology and informatics to account for its footprint.

Associated Costs for Training. A standardized accounting methodology and informatics would be invaluable for the Services moving forward, and not just in greater ease for assessing J2LOT cost considerations. For example, the Air Force estimated that in fiscal year 2012, a logistics readiness officer costs $27,514 to train over 22 weeks.[9] The Naval Center for Cost Analysis uses manpower-per-day/under-instruction formula of $123 a day.[10] Under this formula, a Navy supply corps officer would cost an estimated $13,000 to train over 22 weeks. The Army's Analysis Installation and Personnel Costing Division projects that a 2nd lieutenant quartermaster could cost as little as $1,622.66 for one segment of training.[11] But Army statisticians further estimate that if other benefits, pays, initial officer acquisition, and support costs are factored in, a quartermaster jumps to $124,769.72. The overwhelming conclusion from the data is that there are tremendous short-term and long-term cost considerations in training an entry-level logistician. However, these costs could be dramatically lowered through a unified or partially unified J2LOT approach.

Long-term Cost Savings. The essential financial considerations for DOD to judge in weighing the cost-benefit analysis of implementing J2LOT are the unrealized benefits, efficiencies, and gains that DOD stands to lose if it does *not* act. The personal connections, long-term efficiencies, and "jointness" that J2LOT would spawn are an incredible windfall for the whole government. First, J2LOT would create a *wholeness of logistics* effect at the O1-O3 level by increasing interoperability. This would not only fill the Active-duty forces but spill over into the Reserve forces as well. J2LOT could embolden new personal qualification standards with a pin or certificate that would provide an easily recognized yardstick of logistical expertise for the combatant commanders and Services to measure. Meanwhile, J2LOT could also add valuable Joint Qualification System credit, which is required for future advancement.[12] Second, J2LOT offers the next generation of military logisticians the opportunity and forum to network and seek efficient solutions in their careers sooner rather than later. Officers today wait as long as a decade into their career to begin this synergy. It is not far-fetched to envision a scenario in the near future in which officers who previously trained together at J2LOT work together in solving a complex logistics problem during a joint humanitarian operation in Africa. Finally, J2LOT would foster further coordination and integration of legacy Service-specific logistical chains, administrative processes, and informatics. Regrettably, most of these intangible benefits cannot be readily quantified or manifested immediately.

Begin the Transformation Now

The time is ripe for J2LOT's synchronization and savings to be realized. This concept is not new. During World War II the Army, Army Air Corps, and Navy all had their logistics officer courses tied to the Harvard Business School.[13] From 1943 to 1946, thousands of logisticians learned in a hybrid environment of civilian professors and military officers as instructors taught through case-study methodology.[14] This process was disbanded in favor of a Service-specific process that was responsive to the Services' individualized needs after World War II. Now, more than 70 years later, the current model is becoming increasingly unsustainable in a modern warfare environment that makes joint and cost-sensitive requirements of utmost concern for combatant commanders.

Lessons Learned and Efforts Under Way. The Services have seen the writing on the wall and have responded to this demand signal with various approaches. Each Service is in the process of or has just concluded efforts at refining its overall logistics training. The Army reformatted its logistics community training and career progression in 2007, which includes Logistics Officer (MOS #FA 90) mid-level training at the Army Logistics University.[15] The Marine Corps fused its Logistics Officer (MOS #0402) with Motor Transport Officer (MOS #3502). Air Force logisticians are in the process of reviewing and streamlining their logistics

Airmen from 380th Expeditionary Logistics Readiness Squadron hold pump under F-15 Eagle aircraft for hot-pit refueling in southwest Asia, March 2012 (U.S. Air Force/Arian Nead)

training with ideas to incorporate interoperability with other Services. While the Navy has not drastically restructured its supply corps officer community in decades, the enlisted ratings have undergone tremendous streamlining and consolidation.[16] The logistics specialist rate is a case in point;[17] it is basically tasked with maintaining the Navy supply system and inventory. It underwent two major consolidations in 2003 and 2009.[18] It is clear from the various logistics personnel transformations and consolidations that the Services are capable of making the switch to the J2LOT approach.

There already is joint training and harmonization of efforts among Service communities such as medical, special operations, and combatant commands. Some Services cross-train their personnel when there is no organic Service-equivalent training available (common between Marine Corps and Army logistics). Meanwhile, several Services have cut out duplicitous training processes in one Service to combine it with a capability in another, resulting in cost savings. This is the current flight training arrangement between Naval Air Training Command and the Air Force's Air Education and Training Command. But a prime example of both joint efforts working in synergy is the Uniformed Services University for Health Services in Bethesda, Maryland. This institution has prepared both military and Uniformed Public Health Service medical officers under one roof using a general program of study since 1972.[19] Upon graduation, medical officers are farmed out to a smorgasbord of government and military entities. In a similar manner, J2LOT would build on these previous synchronization efforts with the critical goal of providing a standardized level of training for the military's emerging business leaders.

Implementation

Government analysts, private sector consultants, and the Services' logistics leaders have already taken a stab at better coordinating joint logistics and training. These efforts were stymied primarily because they focused on a top-down or middle-out approach. DOD might be best served by focusing on the J2LOT bottom-up approach while continuing to advance the top and middle approaches. There are a variety of internal and external options for DOD to institute J2LOT. Within the department there is the option for inter-Service memorandums of agreement, JCS instructions, and Office of the Secretary of Defense (OSD) policy directives. Alternatively, congressional legislative changes to Title 10 or Presidential directives could mandate J2LOT as well.

Title 10 grants the combatant commanders the authority to oversee all aspects of military operations, joint training, and logistics using the forces assigned to them, while the military Service secretaries are generally responsible for recruiting, organizing, supplying, equipping, and training their Service personnel.[20] The Chairman of the Joint Chiefs of Staff and Joint Staff are responsible for formulating joint training policy and doctrine.[21] U.S. Joint Forces Command was DOD's lead in providing joint training until it was disestablished in 2011 and its functions were divvied out to other commands.[22] In light of these legal structures, the most realistic approach for implementing J2LOT would be for DOD to identify the Office of the Under Secretary of Defense for Personnel and Readiness (OUSD-P&R) with the overall responsibility as was done in previous joint training initiatives.[23] The example process that follows has worked with some fruitful albeit slowly manifested results.[24] Typically, OUSD-P&R eventually assigns one of its principals or deputies to act as the executive agent. To carry out that responsibility, the executive agent would then establish three standing groups: the Executive Steering Group, Senior Advisory Group, and Joint Integrated Process Team. Consisting of Senior Executive Service civilians and senior flag officers, each group would have its own unique set of tasks and responsibilities in order to plan, support, collaborate, and implement J2LOT in a time-phased approach. An initial pilot program would be recommended, and, if successful, it would transition into a rollout period of 2 to 3 years. This hybrid and complex method is preferable for DOD because it allows the Services the opportunity to properly address grievances, assuage concerns, build consensus, and evaluate and execute J2LOT.

Approach to Training

The optimal construct for the J2LOT would be a combined or hybrid training program. The first option would be to create one unified school with a core curriculum in conjunction with follow-on, Service-specific onsite training. A second option would be to mirror the first option and then conduct follow-on, Service-specific offsite training at each Service's current logistical training command. The final option would incorporate holding both the combined curriculum and the Service-specific follow-on training at the current logistical training commands' education centers. Each option presents its own unique set of obstacles. However, J2LOT's benefits would dwarf any of these initial challenges.

An Inclusive and Viable Construct

It would be feasible, efficient, and fiscally inviting to train other Federal agencies that have similar logistics courses under the J2LOT umbrella. Logisticians from the Department of Homeland Security, Department of State, and U.S. Agency for International Development would be ideal candidates because of the increasing amount of interagency responsibilities that are now shared in the hybrid environment of modern conflict and crisis management. It would also be possible for the interagency or one of its members to create its own organic logistics-training program similar to J2LOT. It is conceivable that any entry-level officer or administrator with logistical duties from across the government spectrum could be a candidate. DOD could expand J2LOT enrollment to include international members as well. North Atlantic Treaty Organization members, United Nations, and other partner-nations' military logisticians could all train side by side. The recent logistical cooperation among the U.S. interagency community, nongovernmental organizations, U.S. military, and other nations after the 2010 earthquake in Haiti highlights this possibility.

J2LOT also raises the specter of whether a similar method and model could apply to other military Service-specific support communities where the training and positions are analogous or overlap significantly. The military's various intelligence communities are a case in point since their junior officer training is both resource-intensive and redundant. Could the J2LOT framework be applied among the military intelligence communities? Could that same joint military intelligence training incorporate entry-level analysts from other intelligence community members such as the Defense Intelligence Agency? Finally, could public affairs, chaplain corps, and the judge advocate general each fashion its own combined training pipeline in the future?

Conclusion

J2LOT is not intended to destroy any Service-specific community or unique logistics ability though it may cause controversy among and between the various Services, OSD staffs, and the Joint Staff. Upon completion of the training, it is not the intention of J2LOT to begin swapping Army 2nd lieutenant transportation officers in a Ranger battalion with Navy supply corps ensigns from the fleet, just as it is not proposed that an Air Force 2nd lieutenant logistics readiness officer replace a Marine Corps 2nd lieutenant logistics officer in a Marine Expeditionary Unit. On the contrary, J2LOT reinforces the different Services' ancillary roles and identities. J2LOT is not a revolution against the various Services or DOD writ large. Instead it is a movement that is part of a gradual evolution of DOD into a more lean, mean, and *purple* force. Simply put, J2LOT seeks a harmonization where redundancy of training effort or curriculum exists. At the same time it carries forward *core business principles* and *competencies*, saves scarce resources, and increases efficiencies.

One of the 1,700 logistics officers in training this year could well be the flag officer in charge of USTRANSCOM or DLA in 2040. DOD's current trajectory indicates that the operating environment in 2040 will be even more "joint" than it is today. There is a window of opportunity for DOD to begin joint logistics training and harmonization efforts. But this window is closing. Waiting for most officers to enter their intermediate and advanced career phases before learning joint logistics is too late. The incentives exist now for DOD to create a curriculum and school at the basic officer level. DOD needs to get its logistics training more *joint* and *whole* because, as U.S. Navy Captain Alfred Thayer Mahan noted, "Logistics [is] as vital to military success as daily food is to daily work."[25] JFQ

Notes

[1] Goldwater-Nichols Department of Defense Reorganization Act of 1986, P.L. 99-433, U.S. Code 10, § 151–155.

[2] U.S. Defense Logistics Agency, available at <www.dla.mil/Pages/default.aspx>; U.S. Transportation Command, available at <www.transcom.mil/>.

[3] See U.S. Joint Forces Command and the Joint Staff, *Joint Logistics Education, Training, and Experimentation Transformation (JLETT) Working Group* presentation, August 26, 2009, available at <www.dtic.mil/doctrine/training/conferences/wjtsc09_2/wjtsc09_2wg_jlett_readahead.ppt>; *JLET Way-Ahead Open Forum Discussion*, March 31, 2010, available at <www.dtic.mil/doctrine/training/...1/wjtsc10_1wgjlet_wayahead.ppt>; Department of Defense (DOD), *Joint Concept for Logistics*, August 6, 2010, available at <www.dtic.mil/futurejointwarfare/concepts/jcl.pdf>; Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 1800.01D, *Officer Professional Military Education Policy (OPMEP)*, September 5, 2012, available at <www.dtic.mil/cjcs_directives/cdata/unlimit/1800_01.pdf>; and CJCSI 3500.01G, *Joint Training Policy and Guidance for the Armed Forces of the United States*, March 15, 2012, available at <www.dtic.mil/cjcs_directives/cdata/unlimit/3500_01.pdf>.

[4] Logistics Training Command, Service Web sites, and personal qualification standards (PQS). Matriculation numbers and curricula are based on cursory interviews with each Logistics Training Command as well as consulting their Web sites and PQS. See U.S. Army, available at <www.almc.army.mil/index.asp>; U.S. Marine Corps, available at <www.mccsss.marines.mil/>; U.S. Navy, available at <www.netc.navy.mil/centers/css/nscs/>; and U.S. Air Force (USAF), available at <www.37trw.af.mil>. Because of its small program size, the U.S. Coast Guard does not have a comparable command or Web site.

[5] The Navy Supply Corps School was moved from Athens, GA, to Newport Naval Station in Newport, RI, in 2011. It is now known as the Wheeler Center.

[6] Logistics Training Command, Service Web sites, and PQS.

[7] "Tour" is analogous with assignment or position.

[8] U.S. Army Regulation 30-22, *Army Food Program* (Washington, DC: Headquarters Department of the Army, July 24, 2012, updated August 24, 2012), available at <www.apd.army.mil/pdffiles/r30_22.pdf>; U.S. Navy, *Food Service Operation Handbook*, 1st ed. (Mechanicsburg, PA: Naval Supply Systems Command (NAVSUP), January 2010), available at <http://navybmr.com/study%20material/Food%20Service%20Operation%20Handbook.pdf>; and NAVSUP, *Food Service Management*, NAVSUP Pub. 486 (Mechanicsburg, PA: NAVSUP, January 2010, updated), available at <www.cs1dino.com/cstraining/wp-content/uploads/2012/06/P486-Food-Service-Management-JAN-2010.pdf>.

[9] See USAF Air Education and Training Command, available at <www.aetc.af.mil/>. USAF notes that these estimates should not be used for budgeting purposes.

[10] See Naval Center for Cost Analysis, available at <www.ncca.navy.mil/index.cfm>.

[11] U.S. Army's Analysis Installation and Personnel Costing Division, available at <http://asafm.army.mil/>.

[12] John Warner National Defense Authorization Act of 2007, P.L. 109-364, § 516–519.

[13] "HBS Archives Photograph Collection: Wartime Schools, 1942–1945: A Finding Aid," Harvard Business School Online Archives, available at <http://oasis.lib.harvard.edu/oasis/deliver/~bak00087>.

[14] Primus V, "Statistics, No Lies," *Harvard Magazine*, March–April 2013, available at <http://harvardmagazine.com/2013/03/statistics-no-lies>. Upon completion, graduates received a Harvard certification. As a side note, Robert McNamara taught courses and supervised the Office of Statistical Control for the Army Air Corps. This office sought to increase the efficiency of aerial bombing through applied statistics.

[15] Military Occupational Specialty (MOS) is used for both Marines and Army. The Air Force uses the Air Force Specialty Code (AFSC). The AFSC uses 21R1 for a Logistics Readiness Officer. The Navy uses a four-number officer designator starting with 31; therefore, a Supply Officer is designated as a 31XX.

[16] A *rate* or *rating* is the Navy term for MOS.

[17] U.S. Navy, "Navy Logistics Jobs," available at <www.navy.com/careers/business-legal/purchasing-supply-logistics.html>.

[18] The storekeeper rate absorbed the aviation storekeeper rate in 2003. The new storekeeper and postal clerk rates fused into the logistics specialist rate in 2009.

[19] Uniformed Services University of Health Service, Web site, "About," available at <www.usuhs.mil/>.

[20] Commanders of combatant commands: assignment; powers and duties, U.S. Code 10, § 164. See also Joint Publication 1-02, *Department of Defense Dictionary of Military and Associated Terms* (Washington, DC: The Joint Staff, November 8, 2010, as amended through December 15, 2013), available at <www.dtic.mil/doctrine/new_pubs/jp1_02.pdf>.

[21] U.S. Code 10, §§ 3013(b), 5013(b), and 8013(b).

[22] Chairman of the Joint Chiefs of Staff Instruction 3500.01B, *Joint Training Policy for the Armed Forces of the United States*, U.S. Code 10, § 153. See also U.S. Government Accountability Office (GAO), *Military Training: Actions Needed to Enhance DOD's Program to Transform Joint Training*, GAO 05-548 (Washington, DC: GAO, June 21, 2005), 4, available at <www.gao.gov/products/GAO-05-548>.

[23] Ibid., 6. See also GAO, *Military Training: Funding Requests for Joint Urban Operations Training and Facilities Should Be Based on Sound Strategy and Requirements*, GAO 06-193 (Washington, DC: GAO, December 8, 2005), available at <www.gao.gov/products/GAO-06-193>.

[24] GAO, *Actions Needed to Enhance DOD's Program to Transform Joint Training*, GAO-05-548, 7.

[25] Alfred Thayer Mahan, *Armaments and Arbitration* (New York: Harper and Brothers, 1912).

Canadian soldier armed with Thompson submachine gun guides German prisoner captured during Operation *Jubilee* (Library and Archives Canada)

Dieppe All Over Again

The Quandaries of Combined Joint Operations

By Harald Høiback

Lieutenant-Colonel Harald Høiback, Ph.D., Royal Norwegian Air Force, is an Associate Professor at the Norwegian Defence University College in Oslo.

The raid on Dieppe in August 1942 is still controversial to the extent that "The waters have since been muddied so successfully that today hardly anything about the raid is undisputed."[1] The aim of this article is not to purify the muddy water but to draw attention to some enduring facts of war. Many of the quandaries and predicaments the Allies experienced before, during, and after the raid are not unique to this operation. The faith of Operation *Jubilee* is thus still relevant for today's military planning, combined joint operations, and postdisaster blame gaming.

The article first recapitulates *what* happened; second looks at *why* it happened, which is where the muddy water begins; and finally discusses why it went wrong.

What Happened?

The raid, originally planned under the codename *Rutter*, was to take place in early July 1942. Operation *Rutter* was disbanded primarily due to bad weather but was reinstated with some small but significant changes as Operation *Jubilee*.

In short the operation was to be a "reconnaissance in force," and according to the combined plan its aim was as follows:

> *Operation 'Jubilee' is a raid on JUBILEE* [Dieppe] *with limited air and military objectives, embracing the destruction of local defences and power stations, etc., in JUBILEE, the capture of prisoners, the destruction of aerodrome installations near the town, and the capture and removal of German invasion barges and any other craft in JUBILEE Harbour.*[2]

The key consideration during the planning stage was the element of surprise. The raid had to come as a bolt from the blue and disappear again almost as swiftly. Hence the attack had to be frontal. Fortunately, intelligence showed that "Dieppe was lightly held by a single low-category battalion."[3] A frontal assault thus seemed both necessary and feasible. The alternative would have been to land the main forces on the flanks and take

Disembarkation of British commandos on return to England (Library and Archives Canada)

Dieppe in a pincer movement from the rear. However, that would have given the Germans ample time for moving up reinforcements.

Another important issue during planning was the extent to which Bomber Command should "soften up" the target by a preliminary attack. The whole idea was rejected, however, because reducing the streets of Dieppe to rubble could actually have made it easier for the Germans to defend it and even harder for Allied tanks to maneuver. Besides, the landing would have come as no surprise if it were "announced" by a heavy air raid. Furthermore, as the Royal Navy (RN) would not risk a capital ship, it supported the operation only with destroyers and smaller ships.

All in all the attack consisted of around 5,000 Canadian and 1,000 British troops, while the Royal Navy supplied 237 ships and landing craft and the Royal Air Force (RAF) 74 squadrons, 66 of which were fighter squadrons. The raid also included 50 American Soldiers belonging to U.S. 1st Ranger Battalion. This was a rough kind of on-the-job training for the Rangers. Indeed, the first Americans killed on European soil during World War II belonged to this group.

The operation was a disaster, particularly for the land forces. Of the 6,000 troops who participated, only about 2,000 returned to England.[4] Even Lord Louis Mountbatten, who saw great benefit from the raid in the long run, admitted that the operation, on its own merit, had been a failure: "The frontal assault on the town itself failed, as everybody knows."[5]

Why Did It Happen?

After the fall of France it was hard to see what options Great Britain had left: "Churchill's poor excuse for a victory strategy, apart from the hope of rescue by the Americans and the Russians, was to peck at the periphery of *Festung Europa*, foment insurrection in the occupied countries, and pray for a coup in Berlin."[6] A series of raids and pinpricks was thus undertaken, and when Mountbatten was appointed advisor on combined operations, the Prime Minister's message was hard to miss: "You are to give no thought to the defensive. Your whole attention is to be concentrated on the offensive."[7]

Second, both Washington and Moscow pressed hard for more British action. When Roosevelt had accepted "Europe first" after the Japanese attack in December 1941 and the ensuing German declaration of war, he also implicitly wanted "Europe soon."[8] Moscow's pressure on London for opening a second front in the west, in order to give the Red Army crucial breathing space or at least show British resolve through a "sacrificial gesture," was also getting intolerable.[9] In this light a dismal failure could at least silence those who clamored for a second front in 1942.

Third, in addition to substantial external forces that pulled Britain into the action, there was also considerable pressure domestically. Many have emphasised that it was the Canadians who bore the brunt of the operation. They had been in the United Kingdom for more than 2 years, producing little but trouble, even to the extent that their "main enemy was boredom."[10] Hence the mix was apparently perfect. A job had to be done, and there were people on hand eager to do it.

Far less has been made of the fact that not only Canadians, but most military men, desperately wanted their share of the action. In his comments to an assessment dated June 29, 1942, concerning the grave consequences that could arise from the capture of some of the central planners, Captain John Hughes-Hallet, RN, responded with the following outburst:

> *I can find no words to express my complete disagreement with the Minutes on this paper sufficiently strongly. They all spring from the idea—new to this country—that war can be waged without risk, to be more particular my views are as follows: (i) Officers of the type who are suitable for serious operation planning, soon become useless for this purpose unless they see actual war*

close at hand. (ii) Such Officers also find it intolerable to sit at Whitehall month after month, while their contemporaries have the fortune to be waging war and earning all the distinctions etc.[11]

In other words, warriors make war if only for the simple reason that there is a war going on.

So far the most basic facts about the operation have been established. Churchill was under considerable pressure to do something, and sometimes it is better to do something hasty than nothing at all. But what should this *something* be? Now things become a bit more complicated.

A German officer who interrogated prisoners captured at Dieppe remarked, "*Jubilee* appeared to be too large for a raid and too small for a lodgement."[12] That hit the nail on its head. The operation can be explained along both lines of reasoning, and that has caused much confusion ever since.

Usually the Dieppe operation is portrayed as a raid that had slightly outgrown its feasibility—a "beach too far," so to speak.[13] When we reach the summer of 1942, combined operations (amphibious operations against the German-controlled periphery) had achieved some significant successes. Therefore one of the driving mechanisms behind Operation *Jubilee* was a kind of incrementalism where raids steadily grew larger and more ambitious. Hughes-Hallet, one of the operation's fiercest advocates, explained the operation along this line:

> *We therefore decided upon the age old policy of raiding. Experts have always differed about the efficacy of amphibious raids—and they certainly differed* [in] *1942. (As we now know their effect on the Germans was greater than had been expected.) Be this as it may—Dieppe as originally conceived was merely one of this series of raids.*[14]

However, this time a bigger concern piggybacked on this line of action: "But there was a difference inasmuch as when first planned it was designed to test the tactical plan for invasion currently popular with the top Staffs."[15] Indeed, in retrospection, this turned out to be the main aim: "I have not come here to apologise for what was done. I have never doubted that the operation was a necessary step in the preparations to invade France—and that for this reason alone it was justified."[16]

Many later claimed that the idea of Operation *Jubilee* as a preparation for an invasion was an ex post facto justification. However, regarding the operation as vital training is not a concept that surfaced *after* the fact. Indeed, already in May, Mountbatten had justified the operation along this line:

> *This operation will be of great value as training for Operation "Sledgehammer" or any other major operation as far as the actual assault is concerned. It will not, however, throw light on the maintenance problem over beaches.*[17]

It is also a challenge in that the operational objectives stated in the combined plan are rather incoherent. Robert Neillands thus wrote, "The problem that confronts historians is what this motley collection of *objectives* adds up to in the way of an *aim*."[18] Apparently, there is nothing there about training, testing, or rehearsal for later operations. On the other hand, the objectives could hardly have been to gain experience. In order to produce concrete plans you need concrete objectives. An athlete does not have to prepare for the Olympics on his daily schedule. The aim of that particular day's training is, perhaps, to win the gold medal, but the objective has to be something concrete, attainable, and measurable. The same goes for Operation *Jubilee*. Even if the aim was to prepare for the big invasion, the objectives had to be something more tangible.

Moreover, when Andrew Roberts states, "Dieppe contributed nothing to the 'mosaic of victory' and taught military planners hardly anything that common sense and normal research and development would not anyhow have dictated" and that a "lance corporal could have told Mountbatten not to attack a well-defended town without proper air and naval cover,"[19] I believe he misses an important point. A lance corporal could also have told Hitler that Operation *Weserübung* was impossible due to the Royal Navy's command of the sea, and that MacArthur's Operation *Chromite* against Inchon in 1950 was impossible due to the condition of the beaches. Likewise, would it be possible to capture a French harbor without destroying it completely in the endeavor? Could one figure that out on paper alone? In the words of the chief of the imperial general staff, "The object of the operation was precisely to find out whether or not success would result."[20]

Even on the tactical level little compares to learning by doing, and for most military men the baptism of fire cannot be substituted by anything. As a Canadian soldier put it, "I learned more at Dieppe than the Army could learn [*sic*] me in ten years."[21] Churchill underlined this message: "Tactically it was a mine of experience. It shed revealing light on many shortcomings in our outlook."[22] To conclude this particular point: "[Dieppe] taught perhaps the most crucial lesson of World War II. . . . If the Western Allies were to beat the Germans, they would have to revise radically their approach to modern combat."[23]

So far we have seen why *something* had to be done, and why this ended up as something between a raid and an invasion. The last question in this section is Why Dieppe?

First of all, the port had to be close enough to British shores to allow for the naval approach to take place under the cover of darkness.[24] Second, the port also had to be within the protective range of Fighter Command. An important spin-off effect of the raid was that Germany's Luftwaffe would be forced to encounter the Allies. Air Vice-Marshal Leigh-Mallory's appeal to 11 Group on the eve of battle was enthusiastic:

> *We are about to take part in the first assault delivered by the combined forces of the three Services against the Continent of Europe in this war. It is an honour to take part in so momentous an operation. . . . The responsibility is great, but I*

am confident that every pilot will do his damndest to destroy any enemy aircraft that may attempt to attack either our ships or our fighting men. GOOD LUCK TO YOU ALL.[25]

Leigh-Mallory's first impression after the operation was also grandiose: "It has been said—and, I think, rightly so—that the Dieppe operation produced the greatest air fight the world has ever known."[26] How great a success the air battle was is still contested. What is important here is that Operation *Jubilee* was much more than the disaster at the beaches.

The last reason Dieppe was chosen was allegedly because the terrain was so difficult that the real invasion, when it eventually came, could under no circumstances have taken place at Dieppe. Hence, the "final reason for choosing Dieppe was the fact that the planners had already ruled it out as a desirable place to capture in the early stages of a real invasion, and we should therefore be giving nothing away by raiding it now."[27]

To sum up, Robin Neillands claimed that the raid has "been a potent cause of controversy ever since, not least because no one has ever come up with a satisfactory, controversy-killing explanation of what it was actually *for*."[28] I do not pretend to have solved this riddle. What I have tried to do, however, is to show that there is no riddle to solve. The operation was over-determinated, so to speak, in the sense that it had multiple causes, many of them sufficient in themselves.

Why Did It Go Wrong?

Since the lessons drawn are not restricted to this particular case, the explanations are grouped into 10 categories, which are of contemporary and enduring relevance.

Bad Strategy? Perhaps the blame for the disaster should go to the very top. The Prime Minister did not get the balance right among the ends, means, and ways of war. Perhaps the ultimate aim was wrong and he instead should do as Liddell Hart suggested a few weeks after Dieppe: "Any wise statesman should be disposed to consider the possibility of ending the war by agreement."[29] Or maybe the means were wrong. Britain should have put even more effort into the bomber offensive, and not, for political reasons within the Alliance, be pushed into a half-baked land operation: "Perhaps no other Allied battle of World War II could be said to have been undertaken for such political rather than military aims."[30]

Conceivably it was the chosen way that was wrong. The half-unconscious mix of raid and invasion addressed previously was particularly unfortunate: "These two remits—raids and invasion studies—of Combined Operations should never have been run together."[31]

Thus the first explanation is Operation *Jubilee* failed because of a lack of strategic skills on the highest level.

Bad Timing? Churchill was certainly not happy with the cancellation of Operation *Rutter*:

The Prime Minister expressed his disappointment very forcefully to me [Mountbatten], *and enquired how soon I could organise another raid on this scale, as he was extremely anxious to have an operation of this nature as soon as it could be mounted* [and] *the only way to do this would be to re-mount RUTTER under a different name.*[32]

This was a bold move. Thousands of soldiers had been briefed about the original plan, and common military sense would have been to shelve it for good. However, according to Montgomery:

Combined Operations Headquarters thought otherwise; they decided to revive it and got the scheme approved by the British Chiefs of Staff towards the end of July. When I heard of this I was very upset; I considered that it would no longer be possible to maintain secrecy.[33]

Consequently, and paradoxically since so many people knew about the original Operation *Rutter*, it was important to keep the new thrust especially secret: "Such absolute secrecy that not only would the Germans not learn of the raid's resurrection, but neither would the British."[34] Indeed, the Germans were not the operation's greatest threat, but reluctant British strategists. They had to be kept in the dark. Mountbatten's later hyperbole surprised no one:

There is no doubt that this was one of the very best guarded secrets of all time, because nothing was put in writing and because nobody except the minimum number of senior officers who were indispensably concerned in the operation were told anything about it.[35]

The ensuing lack of printed documentation, and Churchill's struggle to get to grips with the operation during his writing of *The Second World War*, has given critics ample room to roam.[36]

Thus the second explanation is that Operation *Jubilee* capsized because Mountbatten timed the operation extremely badly. Apparently everybody knew about Dieppe, including the Germans. However, there is little if any evidence that the Germans actually knew about the raid's resurrection.

Bad Planning? The operational plan for *Jubilee* was so detailed that it left no room for improvisation once things began to go wrong. Even the Germans made a point out of the Allies' predilection for detailed plans:

The undertaking was prepared most conscientiously. The Operation Order is very detailed (121 typewritten pages) and, therefore difficult to visualize as a whole. The many code words used make it difficult to grasp in its entirety, and even more so to use as a basis for issuing orders in battle. The planning down to the last detail limits the independence of action of the subordinate officer and leaves him no opportunity to make independent decisions in an altered situation.[37]

Another problem was that the planners did not know which assets they actually had access to. Based on the experience with Operation *Rutter*, the following conclusion was drawn:

If the planning and preparation are to run smoothly it is essential that: (A) The planning Staff must know in good time

> *what the Command's capabilities are. (B) The Commander-in-Chief's Staff must know in good time what is required of the Command. Unless these two conditions are fulfilled—and fulfilled continuously—we will get misunderstandings, delays, and sooner or later mistakes which may be disastrous. Neither* [was] *fulfilled in preparation for Rutter.*[38]

The most important asset the planners lost for Operation *Jubilee* was presumably the heavy bombers: "In retrospect, this failure was the most egregious deficiency in the plan for Dieppe."[39]

Thus the third explanation for the Dieppe disaster is that the planning was not good enough. The execution of the operation and the operational art could not have been better than what the rigid plans allowed for.

Bad Rehearsal? If Operation *Jubilee* was the rehearsal for D-Day, we should perhaps expect that the rehearsal for the operation itself was taken good care of. That was not the case. The dress rehearsal, called *Yukon*, was a "complete fiasco."[40] The RN ability to land troops during pitch-dark night was poor. Instead of developing that ability, it was decided to postpone the planned landing to the so-called "civil twilight." The reverse side of that coin was that more light made the assault forces more visible to the Germans in their pillboxes.

Thus the fourth explanation for the Dieppe disaster is that a serious rehearsal, one that would point out what you should practice and prepare for, not just what you should avoid, never occurred.

Bad Command and Control? One of the main challenges in a combined operation is to get the command and control relationship right. Who is actually in charge? The decision to skip the bombers can also be seen in this light: "Compromise on this, compromise on the bombing, compromise on everything. It's no good!"[41] Even during the operation itself, the lack of a supreme commander was, according to Montgomery, crucial:

> *My own feeling about the Dieppe raid is that there were far too many authorities with a hand in it; there was no one single operational commander who was solely responsible for the operation from start to finish, a Task Force Commander in fact.*[42]

For instance, who had the authority to abort the mission after the land forces hit the beaches? Was it the military force commander, Major General John Hamilton Roberts, or the naval force commander, John Hughes-Hallett? Perhaps the chief of combined operations himself, Louis Mountbatten? Even a newspaper article written just a month after the operation stated the point unambiguously:

> *The initial plan of campaign was deficient because it was more in the nature of a combined compromise rather than a combined plan, and that our own Air Force tactic and organisation has not yet the flexibility to enable it to co-operate with the land force in a major modern battle against strongly defended positions.*[43]

Even Churchill struggled to fathom how such a clumsy and hazardous plan actually came about:

> *Although for many reasons everyone was concerned to make this business look as good as possible, the time has now come when I must be informed more precisely about the military plans. Who made them? Who approved them?*[44]

Thus the fifth explanation is that Operation *Jubilee* foundered through "a fatal confusion of command."[45]

Bad Intel? In the 21st century, people have great expectations about "actionable intelligence": The U.S. Intelligence Community officially defines the concept of *actionable intelligence* as "An awareness of information that predicts the location, timing, and intentions of an individual or group." To those of us outside the Intelligence Community, this definition is more appropriately matched with the term *clairvoyance*, and common sense tells us there is no such thing.[46]

What the Allies lacked in August 1942 was not clairvoyance but a somber appreciation of German positions and abilities. As mentioned before, British intelligence expected to find Dieppe lightly held by a single low-category battalion. That was not the case, and "Dieppe [thus] represented a failure of British intelligence."[47]

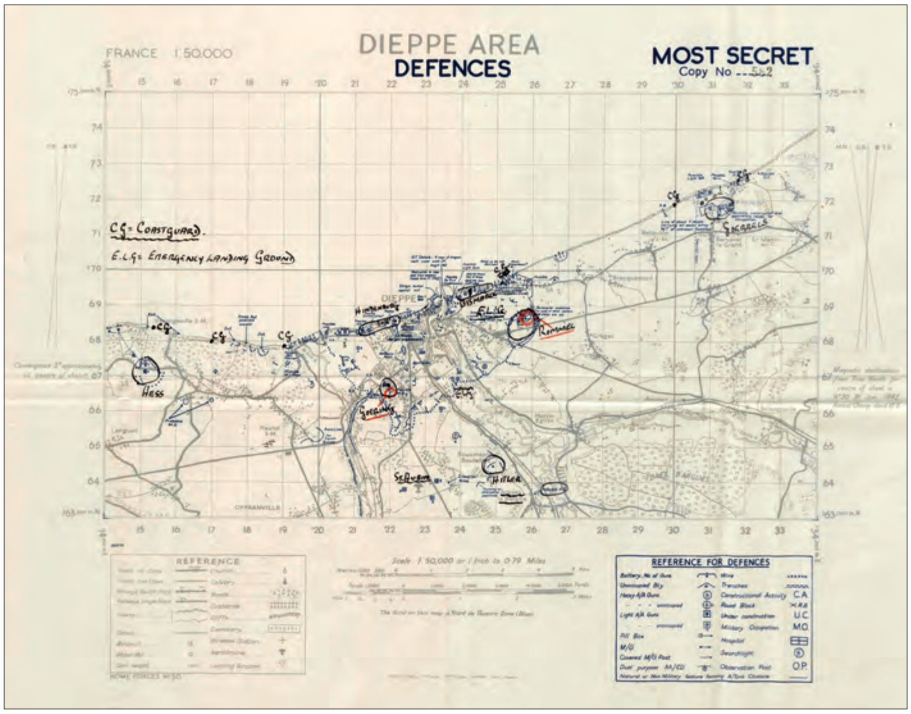
So the sixth explanation for the disaster at Dieppe is that the operation was driven by best-case thinking and hampered by a failure of intelligence.

Bad People? So far we have looked into structural factors, but what about the people involved? Obviously, a number of individuals have been blamed for the calamity.

Combined Operations' head of intelligence, Marquis de Casa Maury, was allegedly "utterly useless."[48] Canadian General J.H. Roberts, who commanded the land forces, had no previous experience and was apparently not up to speed. The naval commander, Hughes-Hallett, was also inexperienced and presumably too eager for action.

The main suspect was Lord Mountbatten himself. Nigel Hamilton describes him as "A master of intrigue, jealously and ineptitude, like a spoilt child he toyed with men's lives with an indifference to casualties that can only be explained by his insatiable, even psychopathic ambition."[49] Andrew Roberts seconds the verdict: "He was also a mendacious, intellectually limited hustler, whose negligence and incompetence resulted in many unnecessary deaths."[50] Indeed, he even pleaded guilty: "Mountbatten finally came clean, boasting that 'It was I, and I alone who took the—and I must say rather bold—decision to attack Dieppe'."[51] However, even here Mountbatten apparently asked for more than he was entitled to: "Mountbatten has taken a strong line, claiming all the responsibility, which surely is more than he need bear."[52]

This is not the place to whitewash Mountbatten or any other, only to point out that history has seen many vainglorious military leaders such as Montgomery, Patton, and MacArthur. In military matters it can be hard to tell where audacity ends and foolhardiness starts, especially in advance.



Map detailing German positions in Dieppe area

Thus the seventh explanation is that the operation miscarried due to sheer madness or other human shortcomings.

Bad Press? Even in 1942 military strategists knew the importance of what we today call "strategic communication":

> *The Effect of a military operation upon public opinion is inseparable from the operation itself: this axiom has proved itself repeatedly in this war. The enemy particularly has employed his own interpretation of military operations so ably, by intelligent anticipatory planning and careful timing, that successful British operations have frequently been made to appear as failures, with detrimental effect upon the morale of our people and that of Occupied Countries. The public relations aspect of Operation "Jubilee," therefore, was approached upon the assumption that a public relations plan is an essential part of any military plan and must be as carefully prepared in advance.*[53]

So the eighth reason for the Dieppe disaster was that its biggest problem apparently was not the failure itself, but the failure to give the failure a positive spin: "The necessity for planning for all eventualities, so that the enemy cannot take a propaganda course which catches us unawares or unprepared, cannot be overemphasized."[54]

Bad Luck? The oldest explanation for military fiascos is bad luck. Operation *Jubilee* had its share:

> *The almost complete achievement of surprise during the channel crossing was marred by one mishap. At 3.30 a.m. the landing craft carrying No. 3 Commando encountered five or six enemy vessels which were acting as escort to a tanker. The presence of this tanker is itself important evidence that the enemy was not expecting an operation on our part.*[55]

Wicked tongues would presumably say there is no such thing as bad luck, only bad (and often too detailed) plans. Others would say that the operation should have been aborted when Hughes-Hallett became aware of the convoy. Nonetheless, the ninth reason the Dieppe Raid failed was bad luck.

Bad History? So far, this article has examined nine generic explanations for military failures and the subsequent placing of blame. The last explanation does not explain the catastrophe itself, but rather the way posterity has dealt with it.

The Dieppe Raid's position in the annals of war is peculiar. Approximately 1,000 men were killed during the operation in a 6-year war that claimed an average of 27,000 lives *a day.*[56] Moreover, Winston Churchill spends less than 3 pages on the operation in his massive six volumes *The Second World War*, which counts almost 5,000 pages. Even the chairman of the chiefs of staff committee, Field Marshal Lord Alanbrooke, gave the Dieppe Raid just fleeting remarks in his diary.

Despite the fact that the number of lives lost was comparatively small and that the main actors gave it comparatively little attention, Operation *Jubilee* is apparently the operation during World War II that has produced the most printed papers-per-killed serviceman. Indeed, "one of the last things the history of the Second World War needs is yet another book about the raid on Dieppe."[57] So where does this overblown attention come from?

First of all, in land warfare the occupation of soil is the only currency. Thus the royal parvenu Mountbatten had nothing to show for himself after the raid. His claim that "the battle of D-Day was won on the beaches of Dieppe" was too subtle and oblique for his many critics to accept.

Moreover, while success has many fathers, failure is—as we all know—an orphan. In this particular case, there were many others to blame. It was a combined joint operation, so the British could blame the Canadians and vice versa, or the military men could blame the airmen and vice versa, and so forth.[58] There are enough pawns on the table to keep this blame game going on forever. On the other side, for those planning for future combined joint operations, Operation *Jubilee* is still "a mine of experience."

Most senior officers in Britain in 1942 had experienced the Great War and they had certainly learned their lesson. This time there should "be no wholesale slaughters."[59] The pertinent question becomes "How is victory possible except by wholesale slaughters?"[60] According to Max Hastings, the Western world was lucky almost beyond comprehension:

> *To defeat Nazi Germany, it was the Western Allies' extreme good fortune that the Russians, and not themselves, paid almost the entire "butcher's bill" for doing this, accepting 95 per cent of the military casualties of the three major powers of the Grand Alliance.*[61]

That our politicians have no taste for attrition warfare is a good thing indeed for all Westerners in uniform. If any servicemember has to risk his life, it should be for a *particular* and, one hopes, *tangible* reason. The main motivation for still remembering Dieppe is that it tells us something important about the West. We value life, even the lives of our military men and women. **JFQ**

The author thanks Colonel Eldar Berli and Lieutenant Colonel Palle Ydstebø for inspiration and support during the writing of this article.

Notes

[1] Andrew Roberts, *Eminent Churchillians* (London: Weidenfeld & Nicolson, 1994), 66.

[2] "Object," *Operation "Jubilee": Combined Plan*, July 31, 1942, AIR 16/746, The National Archives (Kew, United Kingdom).

[3] General Ismay to the Prime Minister, Minute, December 29, 1942, PREM 3/256, The National Archives.

[4] Ken Ford, *Dieppe 1942, Prelude to D-Day* (Oxford: Osprey Publishing, 2003), 91.

[5] Lord Mountbatten, Record of statement, July 1962, CAB 106/6, The National Archives, 4.

[6] Richard K. Betts, "Is Strategy an Illusion?" *International Security* 25, no. 2 (Fall 2000), 11.

[7] Field Marshal Lord Alanbrooke, *War Diaries 1939–1945* (London: Phoenix Press, 2002), xiv.

[8] Robin Neillands, *The Dieppe Raid* (London: Aurum, 2006), 74.

[9] Nigel Hamilton, *The Full Monty: Montgomery of Alamein 1887–1942* (London: Penguin Books, 2002), 465.

[10] Robert Bothwell, *The Penguin History of Canada* (Toronto: Penguin, 2007), 353.

[11] Joint Minute to the Chief of Combined Operations, June 29, 1942, DEFE 2/542, The National Archives.

[12] Brian Loring Villa, *Unauthorized Action, Mountbatten and the Dieppe Raid* (Oxford: Oxford University Press, 1994), 87.

[13] Neillands, 7.

[14] "The Dieppe Raid," address by Vice-Admiral J. Hughes-Hallet, Royal Regimental Association Dinner, January 20, 1962, CAB 106/6, The National Archives.

[15] Ibid.

[16] Ibid.

[17] Minute to The Chiefs of Staff Committee from Chief of Combined Operations, May 9, 1942, DEFE 2/542, The National Archives. Operation *Sledgehammer* was an Allied plan for cross-Channel invasion of Europe in 1942. It was canceled as impracticable in May 1942; see Brooke, 255.

[18] Neillands, 9.

[19] Roberts, 65 and 69.

[20] Brooke, quoted in Hamilton, 455.

[21] Report No. 109, Historical Officer, Canadian Military Headquarters, Operation "JUBILEE," Part III, December 17, 1943, DEFE 2/328, The National Archives, 28.

[22] Winston Churchill, *The Second World War, Vol. IV: The Hinge of Fate* (London: Cassel & Co., 1951), 459.

[23] Hamilton, 427–428.

[24] Neillands, 9.

[25] A.O.C.'s Message to 11 Group, August 18, 1942, Air 16/748, The National Archives.

[26] Air-Marshall T.L. Leigh-Mallory, *The R.A.F. at Dieppe*, AIR 16/748, The National Archives.

[27] Bernard Fergusson, quoted in Villa, 271.

[28] Neillands, ix.

[29] Basil Liddell Hart, "Age-old Truths of War," March 9, 1942, LH 11/1942/70, Liddell Hart Centre for Military Archives, King's College London.

[30] Hamilton, 427.

[31] Ibid., 429.

[32] Mountbatten, undated replies to questions about the Dieppe raid [presumably from 1950], ISMAY 2/3/260/2a, Liddell Hart Centre for Military Archives, King's College London, 1.

[33] Bernard L. Montgomery, *The Memoirs of Field-Marshal Montgomery* (Barnsley: Pen & Sword, 2010, orig. pub. 1958), 76.

[34] Hamilton, 458.

[35] Mountbatten, undated replies, 9.

[36] See especially Villa.

[37] *Intelligence Report on British Landing at Dieppe on 19 Aug 42*, H.Q. LXXXI Army Corps, August 22, 1942, trans. and disseminated by SHAEF, February 26, 1944, WO 219/1867, The National Archives.

[38] Undated Staff Minute Sheet: Remarks put forward as the result of experience gained during the planning and preparation of orders for Operation *Rutter*, ADM 179/220, The National Archives.

[39] Hamilton, 444, 445. There were many reasons for canceling the bombers, but we should not underestimate the human side of this: "Churchill had told Mountbatten he disliked the idea of flattening Dieppe, where he had once picked blackberries with Clemmie."

[40] Ibid., 447.

[41] Ibid., 471.

[42] *The Memoirs of Field-Marshal Montgomery*, 77.

[43] The Military Correspondent, *Evening Standard*, September 19, 1942, AIR 16/764, The National Archives.

[44] Winston Churchill to General Ismay, December 21, 1942, PREM 3/256, The National Archives.

[45] Adrian Smith, *Mountbatten, Apprentice War Lord* (London: I.B. Tauris, 2010), 205.

[46] Pete Blaber, *The Mission, the Men, and Me, Lessons from a Former Delta Force Commander* (New York: Berkley Caliber, 2008), 91.

[47] Philip Ziegler, *Mountbatten, The Official Biography* (London: Book Club Associates, 1985), 193.

[48] Hamilton, 441.

[49] Hamilton quoted in Ziegler, 193.

[50] Roberts, 55.

[51] John Hughes-Wilson, "Review of Robin Neilland's *The Dieppe Raid*," *RUSI Journal*, December 2005, 93.

[52] Minute from Churchill to General Pownall, "The Story of the Dieppe Raid," March 20, 1950, Liddell Hart Centre for Military Archives, ISMAY 2/3/247/2a, King's College London.

[53] C.B. 04244, *Combined Report on The Dieppe Raid*, October 1942, CAB 98/22, The National Archives, 194.

[54] Ibid., 197.

[55] "Dieppe: A Gallant Exploit Re-Told in Detail," *Daily Telegram*, September 19, 1942, WO 106/4197, The National Archives.

[56] Hastings, xv.

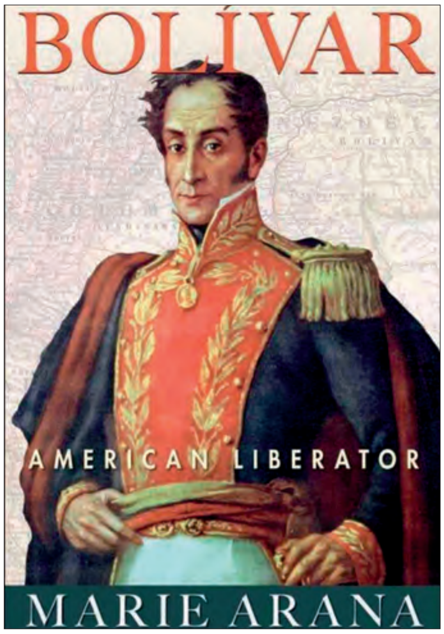
[57] John P. Campbell, *Dieppe Revisited: A Documentary Investigation* (London: Frank Cass, 1993), 1.

[58] That the Germans did their best to thwart the operation is more or less overlooked during this blame game. That is indeed an enduring phenomenon; we usually give little credit to our enemies' skill and proficiency.

[59] Max Hastings, *All Hell Let Loose: The World at War 1939–1945* (London: Harper Press, 2011), 441.

[60] Ibid.

[61] Ibid.



Bolívar: American Liberator

By Marie Arana
Simon & Schuster, 2013
624 pp. $35
ISBN: 978-1439110195

Reviewed by
Alan Gropman

Any U.S. military officer or civil servant yearning to earn the sobriquet "grand strategist" must understand the ethos of the countries of Latin America. While many bodies of water are of great interest to the people of the United States and its government, the Rio Grande River is a *vital* interest. A worthy way to expand one's knowledge of the states south of that long river is to read Marie Arana's sound and solid biography *Bolívar: American Liberator*.

Arana is an exceptionally articulate writer (her Bolívar reads like a novel because she is an outstanding stylist) who has written a brilliantly composed, exceptionally well-researched, scrupulously documented (100 pages of notes), and thorough biography of Simón Bolívar, a hero of the first stripe to South Americans today but at the same time sadly unknown to most North Americans. Bolívar is an idol in South America because he liberated Colombia, Venezuela, Panama, Peru, Ecuador, and Bolivia—almost half the continent—from atrocious Spanish autocracy. Arana takes us from Bolívar's ancestry and birth to his death (and evisceration after burial by those desiring to possess parts of the hero), covering everything from his biological heritage, youth and education, travel, politics, military leadership, and governing capability. She tells the whole story including in nongraphic prose his "unquenchable libido." Many below-the-Rio Grande Americans call him "the George Washington" of South America because of his military exploits.

Arana produces a three-dimensional portrait by delivering the travails, accomplishments, and failures of the South American liberator. Readers who want to understand politics south of the Rio Grande will benefit from this solid account. By learning of Bolívar's many soldierly attributes we can understand why he is revered. Also, however, discovering Bolívar's abundant shortcomings as a politician should leave us wondering why he is esteemed in that regard. Every state he established by conquest disappeared before or soon after his death.

Arana puts the reader inside Bolívar's zeitgeist, explaining that Simón was a child of the 18th-century Enlightenment. He was familiar with the writings of the philosophers undergirding the European and American revolutions and admired America's Founding Fathers.

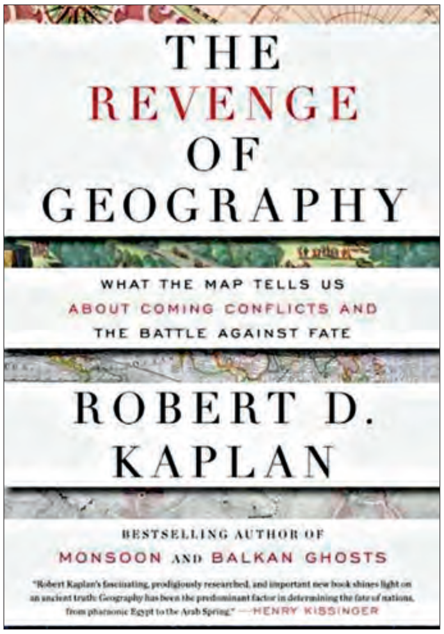
However, he recognized the destructive flaw of slavery in the United States, despised human bondage, and was not a racist. On June 2, 1816, Bolívar affirmed total freedom for slaves in the Spanish colonies, announcing, "I have come to decree, as law full liberty to all slaves who have trembled under the Spanish yoke for three centuries." Bolívar's emancipation proclamation preceded freedom for slaves in the United States by half a century (and real liberty for at least 150 years), and the reasons driving it had some similarities to Abraham Lincoln's motivations. Bolívar needed the manpower former slaves could provide to defeat the Spanish, and he directed the newly freed men to join his revolutionary armies.

Lincoln, similarly, needed blacks to fight for the Union to defeat the Confederacy, and enlisting former slaves was one of his motivations for altering his Proclamation. In the preliminary Emancipation Proclamation issued after the Union "victory" at Antietam in September 1862, using blacks as Union warriors was unmentioned, but in the edict issued on January 1, 1863, it was boldly announced and produced many thousands of highly motivated black soldiers. By the time of Appomattox in April 1865, there were over 120,000 black combatants in the U.S. Army, more than all the soldiers in Robert E. Lee's, Joe Johnston's, and John Bell Hood's armies combined.

With the help of former black slaves, Bolívar defeated the Spanish armies over the next 5 years, but he was a better general than politician. Arana cites his admission of his political shortcomings: "At times, it seems the hardest road of war is that which leads to peace. For Bolívar, it was ever so. 'I am a soldier,' he liked to say even when others begged him to be something more. Despite his well-honed faculties for social justice—despite his gift for imparting democratic ideals—he found the quotidian business of government numbing. He was a man of the sword, not the scepter. But it was the scepter he was handed when he rode triumphantly into Caracas on June 29, 1821, five days after his decisive victory" over the Spanish colonial armies.

Suffice it to say that when Bolívar died at 46, his approval rating was negative and he went largely unmourned. His beatification came when his political inabilities were forgotten and therefore forgiven, his ideas were exalted, and his military victories were elevated. Simón Bolívar is as much an immortal hero today as evidenced by autocrats like the late Hugo Chávez. Arana explains why Chávez retitled his country The Bolivarian Republic of Venezuela. Understanding Bolívar's gravitas and illustriousness in that continent is the beginning of comprehending the character of the United States' closest neighbors. This biography is a must read. JFQ

Colonel Alan Gropman, USAF (Ret.), Ph.D., is the Distinguished Professor of National Security Policy, Emeritus, at National Defense University and an Adjunct Professor at George Mason University.


THE
REVENGE
OF
GEOGRAPHY
WHAT THE MAP TELLS US
ABOUT COMING CONFLICTS AND
THE BATTLE AGAINST FATE
ROBERT D.
KAPLAN
BESTSELLING AUTHOR OF
MONSOON AND BALKAN GHOSTS
"Robert Kaplan's fascinating, prodigiously researched, and important new book shines light on an ancient truth: Geography has been the predominant factor in determining the fate of nations, from pharaonic Egypt to the Arab Spring." —HENRY KISSINGER

The Revenge of Geography: What the Map Tells Us About the Coming Conflicts and the Battle Against Fate

By Robert D. Kaplan
Random House, 2012
403 pp. $28
ISBN 978-1400069835

Reviewed by
Francis P. Sempa

Ever since the rise of Hitler and the Second World War, international events and circumstances have led to periodic revivals of interest in the ideas and concepts of classical geopolitical theorists. As the Wehrmacht surged into the vast expanses of Soviet Russia and Imperial Japan sought to carve out a greater East Asia and Pacific empire, Western strategists and even popular media outlets such as *Time* magazine "discovered" the "Heartland" theory first propounded by British geographer Halford Mackinder in his 1904 address to the Royal Geographical Society entitled "The Geographical Pivot of History," revised and expanded in his 1919 masterpiece *Democratic Ideals and Reality*, and further revised and updated in a 1943 *Foreign Affairs* article, "The Round World and the Winning of the Peace."

Mackinder identified the northern-central core of the Eurasian landmass as the "Heartland" and "pivot" of world politics and the potential seat of a global empire. He viewed Germany's two wars with Russia in the 20th century as struggles for command of the Heartland and preeminence in Eurasia. He also discerned a pattern to international politics that repeatedly pitted insular sea powers against continental-based land powers.

With the onset of the Cold War in the mid-to-late 1940s, some Western strategists perceived that the U.S.-Soviet struggle for the world could best be understood not solely as a conflict between competing ideologies, but more by reference to classical geopolitics. Indeed, George Kennan, Walter Lippmann, James Burnham, and Raymond Aron were among those who viewed the Cold War through Mackinderesque lenses. Containment's intellectual origins can be traced back to "The Geopolitical Pivot of History."

The advent of atomic weapons, however, convinced many in the West that classical geopolitics was outmoded and irrelevant. Nuclear weapons and intercontinental delivery systems, it was argued, made geography less pertinent to international politics. After the U.S. defeat in Southeast Asia and the Soviet offensive in the Third World during the 1970s, Western strategists such as Colin Gray resurrected classical geopolitics to explain the growing threat to the West posed by Soviet expansionism. In the 1970s Gray wrote a monograph entitled *The Geopolitics of the Nuclear Era* that introduced a new generation of scholars and policymakers to the works of Halford Mackinder, Yale professor Nicholas Spykman, and American sea power theorist Alfred Thayer Mahan.

The end of the Cold War, with its promise of a "peace dividend" and a "new world order," once again seemed to consign classical geopolitics to the ash heap of history. Europe, the center of great power struggles for centuries, was at peace. There was no peer competitor to challenge America. Strategist Edward Luttwak argued that "geo-economics" was replacing geopolitics. Francis Fukuyama provocatively proclaimed the "end of history." Thomas Friedman pointed to "globalization" as the key to understanding world politics.

Then, quite suddenly, the United States was fighting two wars in Asia (in Afghanistan and Iraq), conducting a global "war on terror," attempting to prevent two Asian countries (North Korea and Iran) from getting nuclear weapons, and dealing with the rising Asian powers China and India. Geography, it seemed, mattered after all.

That is why the geopolitical writings of Mackinder, Spykman, and Mahan are front and center in Robert D. Kaplan's new book, *The Revenge of Geography*. Kaplan in the recent past has traveled to the world's hot spots to observe up close and write about the difficult and brutal work performed by the U.S. military. With the end of the Cold War and the relative rise of great powers in Asia, Kaplan has taken a broader view of global events. This was first evidenced in his 2010 *Monsoon*, in which he identified the Indian Ocean and its surrounding landmasses as the pivot of world politics in the 21st century. Now, in *The Revenge of Geography*, he uses Mackinder, Spykman, Mahan, and lesser geopolitical thinkers to explain the global politics of today and tomorrow.

Kaplan's is a realist's view of the world that accepts human nature as the "Thucydidean pantheon of fear, self-interest, and honor," resulting in a "world of incessant conflict and coercion" (p. 25) that forces strategists and policymakers to recognize "the most blunt, uncomfortable, and deterministic of truths: those of geography" (p. 28). "[G]eography," he writes, "is the preface to the very track of human events" (p. 28).

Kaplan reviews what he calls "the grand pattern of world history" (p. 37) using the theories and concepts of the great classical geopolitical thinkers to establish a framework to understand the past, contextualize current world events, and foresee the emerging trends in global politics.

That framework—a synthesis of the ideas of Mackinder, Spykman, and Mahan—posits the centrality of the

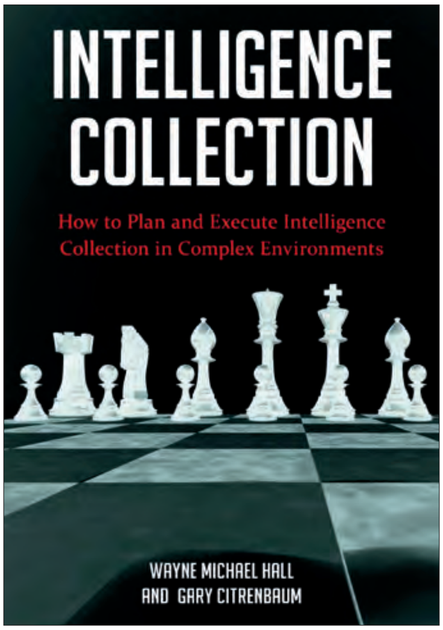
Eurasian landmass to the global balance of power, the distinct and rival geographical power centers of Eurasia, and the historic rivalry between land powers and sea powers for regional and global preeminence.

Kaplan contends that power in Eurasia has shifted from Russia and Western Europe to what Spykman called the Asian "Rimland" and Mahan termed the "Debatable and Debated Ground." This region includes the Middle East, Southwest Asia, Central Asia, and the Far East, the Indian and Pacific Oceans, and the rising powers of China and India, five nuclear powers (China, India, Russia, Pakistan, and Israel), the volatile Korean peninsula, lands with vast reserves of oil and natural gas, and important maritime chokepoints. He reviews in separate chapters the geo-history of the key countries and power centers of Eurasia including Western Europe, Russia, China, India, Iran, and Turkey and explains their relative importance to the geopolitics of the 21st century.

Kaplan writes that although the United States is in relative decline as a world power, it does not have to go the way of previous empires such as Rome, Venice, and Great Britain. He recommends that the United States avoid getting bogged down in small wars, prioritize its sea and air power assets, and become a "balancing power in Eurasia and a unifying power in North America" (p. 346).

While one can quibble with Kaplan's specific recommendations, he deserves much praise for reintroducing and applying classical geopolitical analysis to the 21st-century world. JFQ

Francis P. Sempa is an Assistant U.S. Attorney for the Middle District of Pennsylvania, an Adjunct Professor of Political Science at Wilkes University, and a contributing editor to *American Diplomacy*.


INTELLIGENCE COLLECTION
How to Plan and Execute Intelligence Collection in Complex Environments
WAYNE MICHAEL HALL AND GARY CITRENBAUM

Intelligence Collection: How to Plan and Execute Intelligence Collection in Complex Environments

By Wayne Michael Hall and Gary Citrenbaum
Praeger, 2012
505 pp. $63
ISBN: 978-0313398179

Reviewed by
Todd M. Manyx

In this companion piece to the authors' 2010 work, *Intelligence Analysis: How to Think in Complex Environments*, Wayne Hall and Gary Citrenbaum have brought forth a superior forum by which to consider the challenges associated with intelligence collection in complex environments. Each author brings with him a lengthy résumé of credible service in the intelligence field. Hall is a retired U.S. Army officer with over 30 years of intelligence experience, and he has remained active within the intelligence field by participating in numerous seminars on intelligence training and intelligence transformation. Citrenbaum is actively involved in issues associated with intelligence transformation. Accordingly, both speak with authority on the issues they raise.

The authors' background as educators clearly influenced the organization and prose. On a most positive note, the book is written clearly and in a conversational tone that educates and informs without being didactic. It follows a well-constructed framework that systemically scopes the issues the authors feel are restraints on the current intelligence enterprise's structure and processes. The technical organization of each chapter will be familiar to professional students in that each chapter opens with a brief discussion of the issue followed by a logical and detailed examination. At the end of each chapter, the authors provide a synopsis that specifically details the central points and then explains how it ties into the next chapter. The benefit of this model is that it allows readers to quickly review the salient points with the option of delving into a deeper, more nuanced reading, should they desire.

The book is divided into 15 chapters that comprise the introduction followed by four principal sections in which the authors utilize an inductive reasoning model to organize and present their thesis. The nonintelligence professional will find the introduction and the sections on underpinnings and synthesis to be the most informative. The lengthy sections on operations and specifics can be appreciated by reading the synopsis at the end of each chapter.

The introduction provides a useful discussion of the conceptual framework that should underpin intelligence collection and analysis in complex urban environments representing the dynamic nonlinear conditions that produce the Complex Adaptive Systems that confound the ability of our national-level intelligence collection capabilities to react nimbly when supporting lower-level commanders. It also notes that the enterprise is essentially protecting itself from making the changes required when it resists the calls from experienced junior leaders who understand the changes needed but lack the seniority to effect them.

The introduction also presents the authors' concept of what Advanced Collection should seek to do. At its most elemental level, Advanced Collection serves “a distinct purpose [to] find . . . often fleeting observables . . . at the *right time*, at the *right place*, and in the *right activities*” as they relate to the modern battlefield’s center of gravity, the populace (pp. 2, 5). Later, this basic concept is further refined, with Advanced Collection being “The creative design and use of technical, cyber, human, and open-source collectors in all domains in pursuit of discrete, subtle, nuanced, and often fleeting observables, indicators, and signatures” (p. 292).

In the subsequent chapters, Hall and Citrenbaum discuss the constantly evolving nature of the operating environment and define 11 specific challenges to working in the chaotic and fluid environments that our forces face, particularly in urban areas. They take care to note that by focusing on four kinds of patterns—human/social, technical, functional, and organizations—we can identify anomalies that will help focus the Advanced Collection effort. In detailing the numerous challenges we place on ourselves, the authors also take time to provide specific remedies to each problem.

The most useful chapter provides an in-depth discussion on critical thinking. This chapter makes clear that critical thinking has a deep bench of military theory behind it and is substantively different from the other forms of thinking discussed in other sections. Critical thinking is unique in that, while it is essential for the success of Advanced Collection, it supports every professional regardless of occupation or specific problem.

The intelligence field I work in today is not the same field I joined in the mid-1980s, and that is a good thing. No longer are we focused on the FM-100 series with its attendant foldout sections detailing how the Soviet Motorized Rifle Regiment would array itself on the battlefield with the expectation that collection plans could be derived from such blunt tools. Today the intelligence professional has access to infinitely more information, powerful tools, and, after more than a decade of irregular warfare, a solid understanding of what it will take to continue to improve our intelligence “fighting position” and remain relevant and valuable to commanders at all levels. The thoughts put forth by Hall and Citrenbaum are not a prescription on how we should “fix” intelligence. However, their ideas are provocative and will challenge intelligence professionals to reflect on how they can provide better support. They will challenge everyone else to consider the myriad elements that affect intelligence collection and how the consumer can help focus the intelligence enterprise and use intelligence as yet another arrow in the commander’s 21st-century quiver of weapons systems. **JFQ**

Lieutenant Colonel Todd M. Manyx, USMC, is a career Intelligence Officer assigned as the G-2, Marine Forces Reserve, and Inspector-Instructor for the USMC Reserve Intelligence Battalion.

New from NDU Press

for the Center for Strategic Research

Strategic Forum 286
Targeted Killing of Terrorists
by Nicholas Rostow

INSS

February 2014

STRATEGIC FORUM

National Defense University

About the Author

Key Points

Targeted Killing of Terrorists

By Nicholas Rostow

CENTER FOR STRATEGIC RESEARCH

The battle against terrorism raises important legal and policy concerns for the United States. Efforts to prevent terrorist attacks include the controversial practice of targeted killing, for example—the identification and killing of individuals involved in terrorist operations and organizations. Authority for targeted killing exists in domestic and international law. As a matter of policy even if it is not legally required, the United States should use the Geneva Conventions of 1949 to guide its confrontations with terrorists.

NDU Press

INSS
INSTITUTE FOR NATIONAL STRATEGIC STUDIES

Visit the NDU Press Web site
for more information on publications
at www.ndu.edu/press/index.html

Joint Publications (JPs) Under Revision (to be signed within 6 months)

JP 2-01.3, *Joint Intelligence Preparation of the Operational Environment*

JP 3-02, *Amphibious Operations*

JP 3-02.1, *Amphibious Embarkation and Debarkation*

JP 3-05, *Special Operations*

JP 3-07.2, *Antiterrorism*

JP 3-09.3, *Close Air Support*

JP 3-10, *Joint Security Operations in Theater*

JP 3-13.2, *Military Information Support Operations*

JP 3-26, *Counterterrorism*

JP 3-29, *Foreign Humanitarian Assistance*

JP 3-30, *Command and Control for Joint Air Operations*

JP 3-31, *Command and Control for Joint Land Operations*

JP 3-40, *Countering Weapons of Mass Destruction*

JP 3-52, *Joint Airspace Control*

JP 3-63, *Detainee Operations*

JP 4-05, *Joint Mobilization Planning*

JP 4-09, *Distribution Operations*

JP 4-10, *Operational Contract Support*

JPs Revised (signed within last 6 months)

JP 1-05, *Religious Affairs in Joint Operations* (November 20, 2013)

JP 2-0, *Joint Intelligence* (October 22, 2013)

JP 3-06, *Joint Urban Operations* (November 20, 2013)

JP 3-07.4, *Counterdrug Operations* (August 14, 2013)

JP 3-11, *Operations in Chemical, Biological, Radiological, and Nuclear Environments* (October 4, 2013)

JP 3-16, *Multinational Operations* (July 16, 2013)

JP 3-17, *Air Mobility Operations* (September 30, 2013)

JP 3-24, *Counterinsurgency* (November 22, 2013)

JP 3-27, *Homeland Defense* (July 29, 2013)

JP 3-28, *Defense Support of Civil Authorities* (July 31, 2013)

JP 3-32, *Command and Control for Joint Maritime Operations* (August 7, 2013)

JP 3-57, *Civil-Military Operations* (September 11, 2013)

JP 4-0, *Joint Logistics* (October 16, 2013)

Airman helps Marine load missile at Kunsan Air Base, South Korea (U.S. Air Force/Armando A. Schwier-Morales)

Cross-Domain Synergy

Advancing Jointness

By William O. Odom and Christopher D. Hayes

Today the separate military Services that make up America's Armed Forces work together more often than at any time in the Nation's history. Their success over the last decade of war has cemented the power of "jointness" in accomplishing military objectives. Our ability to integrate land, sea, air, space, and cyberspace military capabilities is unmatched. But despite tremendous progress in achieving jointness, U.S. forces still lack the ability to integrate seamlessly. Moreover, the ability to sustain and build on the considerable gains achieved in the conduct of joint operations is uncertain as our Armed Forces reset from a decade of sustained combat to face a future of complex challenges and constrained resources.

In a recent *Foreign Affairs* article, the Chairman of the Joint Chiefs of Staff explained these challenges to the external audience and highlighted the importance of cooperation among the Armed Forces.[1] Within our ranks, improved cooperation hinges on viewing military problems from a comprehensive cross-domain perspective rather than viewing them through an individual Service lens. To support this shift in focus, the Joint Staff introduced cross-domain synergy as a central idea in recent joint concepts. This article expands on the idea of "cross-domain synergy" by exploring its

Colonel William O. Odom, USA (Ret.), Ph.D., is a Writer/Editor in the Joint Staff J7 Joint Concepts Division. Lieutenant Commander Christopher D. Hayes, USN, is Deputy Director of the Joint Concepts Division.

Marine launches Puma unmanned aircraft system at Patrol Base Boldak (U.S. Marine Corps/Bobby J. Yarbrough)

historical roots, summarizing its usage in recent joint publications, and noting implications for the future joint force.

What Is Cross-Domain Synergy?

The Department of Defense (DOD) recognizes five domains: land, sea, air, space, and cyberspace.[2] Physical space delineates the land, sea, air, and space domains with the physical characteristics of each determining the relative capabilities and vulnerabilities of the actions that occur within them. Cyberspace has different physical characteristics than the geographic domains. It is a crosscutting global domain within the information environment consisting of the interdependent network of information technology infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.[3] Synergy is the interaction or cooperation of two or more organizations, substances, or other agents to produce a combined effect greater than the sum of their separate effects. Cross-domain synergy is achieved when the integrated use of land, sea, air, space, and/or cyberspace capabilities produces a combined effect greater than the sum of the separate effects.[4] In military application, cross-domain synergy is the use of two or more domains to achieve a military advantage. This frequently involves application of capabilities from one domain to another, with the principal aims of improving operational performance and reducing unnecessary joint force redundancies.

Cross-Domain Operations Are Not New

While the term *cross-domain synergy* is new, the underlying concept derives from the age-old military maxim that advises commanders to approach the enemy asymmetrically—to apply strength against an adversary's weakness while protecting one's own vulnerabilities. The history of warfare is rife with use of asymmetry in strategy, operations, tactics, and technology to defeat an enemy. The ability to operate fluidly in more than one domain can afford decisive advantages.

The U.S. military has operated in multiple domains throughout its history. Before it could fly, the United States combined land- and sea-based capabilities to win pivotal victories at Yorktown (1781), Vicksburg (1863), and Santiago (1898). With the advent of flight, the Army, Navy, and Marine Corps added air domain–based capabilities to their growing and rapidly modernizing arsenals. In World War II and Korea, amphibious landings exemplified cross-domain operations. Advances in aviation technology eventually led to the establishment of a separate Service with responsibility for the air domain even as the Army, Marine Corps, and Navy continued to develop their own air capabilities. Most Services have since expanded their organic cross-domain portfolios to include space- and cyberspace-based capabilities.

At first, physical domains largely defined the Services, with the Army focused on land, the Marine Corps and Navy on sea, and the Air Force on air operations.

As each developed cross-domain capabilities to support its activities within a specified geographic domain, it reaped the benefits of cross-domain capabilities without the need for inter-Service coordination.[5] In the last 50 years, technological advances significantly increased the reach of each Service's land, sea, air, space, and cyberspace capabilities and largely erased the geographic distinctions that once delineated the Service's operational domain. As a result, joint operations became increasingly commonplace as each Service took advantage of the additional and often unique capabilities offered by other Services. Today the overlap between Service capabilities is so great that it has shifted the focus of joint operations from coordination along the seams of geographically defined Service boundaries to *integration of Service capabilities within shared domains.* To leverage the Armed Forces' cross-domain capabilities fully, the Services must embrace an evolved understanding of jointness. This has become abundantly clear over the last decade.

Leveraging Cross-Domain Synergy

In recent combat operations, the U.S. military has integrated Service capabilities in ways unlikely to happen in peacetime. Wartime demands have accentuated appreciation of jointness and accelerated the development of joint solutions. A generation of future military leaders has learned through firsthand experiences from Panama through Afghanistan that joint operations offer a greater range of capabilities than single Service operations and that the benefits of combining Service capabilities outweigh the costs. Integration of special operations and general purpose forces along with intelligence, surveillance, and reconnaissance capabilities and the enormous expansion of integrated fires are among the notable examples of improved jointness generating successful multi-Service cross-domain operations.

Recently published concepts, informed by military operations ranging from combat to humanitarian assistance, highlight the synergistic potential of jointness. Four years ago, the *Capstone Concept for Joint Operations V3.0* called for achieving "joint synergy" and noted the importance of thinking in terms of joint functions independent of a specific Service. Last year, the *Joint Operational Access Concept V1.0* (JOAC) expanded the idea of joint synergy by shifting the focus from Service capabilities to domain-based capabilities. The JOAC cited leveraging cross-domain synergy as the central idea of the concept and envisioned a "seamless application of combat power between domains, with greater integration at dramatically lower echelons than joint forces currently achieve." Most recently the *Capstone Concept for Joint Operations: Joint Force 2020* reinforced the idea of cross-domain synergy by specifying that "cross-domain synergy should become a core operating concept in all joint operations" and calling for better integration of joint forces to achieve this effect. These documents reflect the complexity of the changing security environment, embrace the pace of technological advancements, and underline the necessity of combining capabilities within and across domains to optimize our ability to respond to threats. These concepts acknowledge that jointness is the key to conducting operations across domains and this ability gives the U.S. military an asymmetric advantage with the potential to create decisive synergy. They emphasize viewing military problems from a multidomain perspective without regard for Service ownership of the domain or assets. They apply across the spectrum of military activities from combat operations to humanitarian missions and operations other than war.

Implications for the Joint Force

The creation of cross-domain synergy requires approaching military problems from a multidomain perspective. It entails building a comprehensive view of the adversary and the environment, understanding available capabilities, and integrating those capabilities. The key is to advance jointness from integrated Service efforts to a singular multidomain effort.

First and Foremost, the U.S. Military Must Understand Both the Adversary and the Environment. Knowing the enemy is a prerequisite to effective military operations and achieving synergy in operations against it. In addition to assessing an adversary's military capabilities, the defense establishment must better understand the human factors derived from cultural, ideological, and political motivations that shape the enemy's intentions and actions. No less important is understanding the physical environment and the myriad factors that influence the combatant's decisions. Today the United States faces adversaries who are patient, persistent, and elusive—adversaries who have learned to hide from the Nation's overwhelming military capabilities and exploit its weaknesses. This new challenge requires broadening intelligence analysis to include cross-domain perspectives on the enemy's potential weaknesses to identify its motivation, critical vulnerabilities, and ultimately its center of gravity. Integrating the unique perspectives of the 16 separate agencies of the U.S. Intelligence Community as well as those of foreign partners can contribute to developing the strategy, operations, and tactics to defeat the enemy. A comprehensive cross-domain view of the enemy may identify vulnerabilities that might have passed unnoticed when seen through the narrower lens of a single Service or agency, and offer expanded opportunities to strike at weak points from the land, sea, air, space, and cyberspace. The nature of intelligence work makes this inherently difficult, but the benefits of a holistic understanding of the rival system, developed through joint, combined, and interagency intelligence analysis, far outweighs the challenges. In peacetime, intelligence development (collection, analysis, processing, and dissemination) should be the main effort.

The U.S. Military Must Broaden Its Knowledge of Available Capabilities. The scope of American military capabilities is potentially overwhelming, and the list continues to grow and evolve. It takes years to learn how to employ a single Service's capabilities, not to mention staying abreast of new tactics, Marines provide security at landing zone near Boldak, Afghanistan, during Operation *Pegasus II* (U.S. Marine Corps/Austin Long)

techniques, procedures, and technical innovations. Formal education in joint operations usually occurs only after 10 years of immersion in Service-specific programs. However, practical exposure to joint operations is occurring much earlier and more often than in the past. In some specialties, familiarity with relevant joint capabilities is a critical individual skill, especially in the growing number of jobs that routinely employ capabilities from multiple domains. Servicemembers traditionally tended to look to their parent Services first, then elsewhere when seeking solutions to military problems. Achieving cross-domain synergy requires a mindset that expands beyond traditional Service perspectives to embrace all capabilities without undue consideration of the source.

The U.S. Military Must Improve Its Ability to Access and Integrate Service Capabilities. The bumpy transition from Service-centric to joint operations is still incomplete despite 30 years of predominantly joint operations. Make no mistake, American forces have made progress, but the task of accessing and integrating Service capabilities remains complicated even after a decade of war. Observations from joint training events and exercises reveal tendencies to cling to ownership of capabilities rather than accepting assured access to them, and a few holdouts still believe a single Service can do it all without leveraging joint capabilities. This mindset persists in part because the laws that establish and regulate our Armed Forces reinforce Service-centricity. Even those who favor jointness tend to define it from the perspective of enabling their Services. As a result, "joint" is still shaped by the personality and experiences of the senior joint commander rather than by common standards.

Evolving Our Thinking on Jointness

The watershed Goldwater-Nichols Act provided a tremendous external stimulus driving the imperative to achieve Service integration across DOD. The next evolution in jointness must be internally driven and center on the ability to achieve cross-domain synergy by shifting the focus to employing capabilities without regard for Service origin. This shift hinges on building trust and shared understanding by educating leaders earlier and routinely participating in joint training throughout careers—by expanding the scope of the profession of arms to include employing the full range of capabilities. It also requires development of streamlined means to access and integrate capabilities. Despite efforts to function as an interoperable joint force, the military still lacks the authorities, relationships, procedures, and technology to do it without effort. Again, the U.S. military does this better than at any time in its history, but it still cannot reach across Service boundaries and employ cross-domain capabilities with the speed and dexterity it seeks. The JOAC acknowledges many risks associated with integrating cross-domain capabilities, most notably that cross-domain operations could become too complex to be practical. While this is an important consideration, it does not preclude pursuing the concept and moving toward an interoperable joint force capable of creating battlespace synergy through seamless cross-domain operations. The impetus to achieve cross-domain synergy, however, should never supplant the imperative to select the simplest, most efficient solution.

A domain-based view of capabilities not only bridges the Services, but also reaches across combatant command boundaries. The global nature of current military operations often requires the ability to act across two or more combatant command areas of responsibility. In fact, "globally integrated operations" *is* the capstone concept for *Joint Force 2020*. Conducting cross-domain operations within a single area of responsibility is difficult, but it is even harder when

the operation involves multiple combatant commands. Combatant commands remain relatively independent multi-Service organizations, each tailoring joint and combined operating procedures to match theater needs. At the same time, the blurring of simultaneous supporting-supported relationships demands reexamining what interoperability truly requires. Globally integrated operations—and the implied requirement to access and integrate capabilities from multiple combatant commands—necessitate greater commonality in materiel, procedures, and policies to achieve cross-domain synergy.

Another well-known, persistent challenge to achieving cross-domain synergy is accessing and integrating U.S. Government agencies and foreign partners. Put simply, DOD lacks the authority to direct changes that would permanently solve the problem because they are external organizations or they serve other nations. Clearly defined relationships and authorities will advance the military's ability to leverage the unique capabilities these partners bring to operations. Leaders must remain sensitive to the challenges of partnering even as they continue to focus on achieving cross-domain synergy within the "unity of effort" framework.

Conclusion

The employment of cross-domain capabilities to exploit enemy weaknesses and achieve decisive victory is not a new idea, but much has changed in recent years. Cross-domain operations have expanded beyond the combination of land and sea operations to include capabilities delivered from the air, space, and cyberspace. Modern technology has vastly increased available capabilities and these capabilities are rarely controlled exclusively by any single Service. Nor are they the exclusive tools of superpowers and nation-states. Technology, proliferation, and global integration of networks have eroded much of the U.S. advantage in military power and technology. At the same time, other government organizations and foreign partners offer unique capabilities that can dramatically affect the outcome of military operations. The problems the U.S. military faces are more complex, but it has a greater quantity, quality, and variety of tools with which to solve them because the joint force's ability to achieve cross-domain synergy is at an all-time high. However, two postwar trends risk undermining the tremendous gains the Armed Forces have made in their ability to execute joint operations and achieve cross-domain synergy. First, the end of combat operations in Iraq and Afghanistan will remove a powerful impetus for inter-Service cooperation. Second, defense budget reductions could result in prioritization of unique Service requirements over joint requirements.

Soldier inspects static line before jumping from C-17 Globemaster III during mission in support of Joint Operations Access Exercise 12-2 (DOD/Eric Harris)

Ultimately, achieving cross-domain synergy is about evolving the understanding of jointness. Cross-domain perspectives on military problems advance jointness. Improved jointness enables more effective combination of the capabilities of the Armed Forces and the achievement of cross-domain synergy in joint operations. To improve jointness the military needs to shift from Service-centric approaches to a mindset that holistically views the military problem and considers the full range of available capabilities. It also requires changes in the way the military accesses and integrates capabilities, essentially transcending Service and combatant command ownership of capabilities and assuming a global perspective on military operations to achieve globally integrated operations.

Historically, the end of combat operations removes the impetus for Service cooperation, and budget reductions result in prioritization of Service requirements over joint requirements. It is certain that any future military operation will involve joint forces exercising cross-domain capabilities. Therefore it is vital that the military forge the next joint force based on the lessons of recent combat experiences. Those experiences not only validate the effectiveness of jointness as the key to achieving cross-domain synergy, but also highlight persistent challenges in joint operations. Expanding the military mindset to encompass cross-domain perspectives builds the trust and shared understanding the military needs to address the challenges of joint operations within a larger interagency and multinational context. **JFQ**

Notes

[1] Martin E. Dempsey, "The Future of Joint Operations: Real Cooperation for Real Threats," *Foreign Affairs*, June 20, 2013, available at <www.foreignaffairs.com/articles/139524/martin-e-dempsey/the-future-of-joint-operations>.

[2] This categorization pertains to places from which we apply military capabilities and is not to be confused with other models that explore warfare in terms of cognitive, moral, and human "domains." In a recent article titled "Joint Force 2020 and the Human Domain: Time for a New Conceptual Framework?" in *Small Wars Journal*, the authors make a valid case for the centrality of human interaction in all military actions.

[3] Joint Publication 1-02, *Department of Defense Dictionary of Military and Associated Terms* (Washington, DC: The Joint Staff, November 8, 2010, as amended through December 15, 2012), 74.

[4] The JOAC elaborates by stating that *cross-domain synergy* is "The complementary vice merely additive employment of capabilities in different domains such that each enhances the effectiveness and compensates for the vulnerabilities of the others—to establish superiority in some combination of domains that will provide the freedom of action required by the mission."

[5] Not all cross-domain operations are inherently "joint," such as when one Service provides all the land, sea, or air forces. For example, an all-Marine Air-Ground Task Force operation is not joint, yet it typically operates in three domains. On the other hand, not all joint activities are necessarily cross-domain, as when the Air Force and Navy team up to execute air superiority missions or Army and Marine Corps units share ground security missions.

CALL FOR ENTRIES

for the

2014 Secretary of Defense and 2014 Chairman of the Joint Chiefs of Staff

Essay Competitions

Are you a professional military education (PME) student? Imagine your winning essay published in a future issue of *Joint Force Quarterly*, catching the eye of the Secretary and Chairman as well as contributing to the debate on an important national security issue. These rewards, along with a monetary prize, await the winners.

Who's Eligible? Students, including international students, at U.S. PME colleges, schools, and other programs, and Service research fellows.

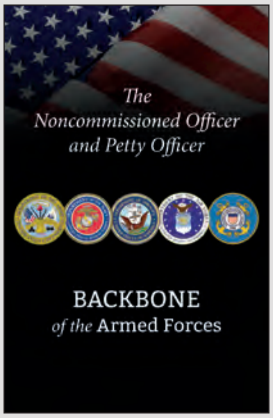
What's Required? Research and write an original, unclassified essay on some aspect of U.S. national, defense, or military strategy. The essay may be written in conjunction with a course writing requirement. Important: Please note that entries must be selected by and submitted through your college.

When? Anytime during the 2013–2014 academic year. Students are encouraged to begin early and avoid the spring rush. Colleges set their own internal deadlines, but must submit their official entries to NDU Press by April 23, 2014, for the first round of judging. Final judging and selection of winners take place May 15–16, 2014, at NDU Press, Fort McNair, Washington, DC.

National Defense University Press conducts the competition with the generous support of the NDU Foundation. For further information, see your college's essay coordinator or go to:

https://ndupress.dod.afpims.mil/EssayCompetitions.aspx

General Martin E. Dempsey, USA, Chairman of the Joint Chiefs of Staff, presents award certificate to Gina M. Bennett. While a student at the Marine Corps War College, Ms. Bennett won First Place in the 2013 CJCS Strategy Article Competition with her paper entitled "The Elusive Defeat of al Qaeda."



The
Noncommissioned Officer
and Petty Officer

BACKBONE
of the Armed Forces

The Noncommissioned Officer and Petty Officer: Backbone of the Armed Forces

NDU Press, 2013 • 176 pp.

A first of its kind, this book—of, by, and for noncommissioned officers and petty officers—is a comprehensive explanation of enlisted leaders across the United States Armed Forces. It balances with the Services' NCO/PO leadership manuals and complements *The Armed Forces Officer*, the latest edition of which was published by NDU Press in 2007. Written by a team of Active, Reserve, and retired enlisted leaders from the five Service branches, this book describes how NCOs/POs fit into an organization, centers them in the Profession of Arms, defines their dual roles of complementing the officer and enabling the force, and exposes their international engagement. As Chairman of the Joint Chiefs of Staff General Martin E. Dempsey writes in his foreword to the book, "We know noncommissioned officers and petty officers to have exceptional competence, professional character, and soldierly grit—they are exemplars of our Profession of Arms."

Aspirational and fulfilling, this book helps prepare young men and women who strive to become NCOs/POs, re-inspires currently serving enlisted leaders, and stimulates reflection by those who no longer wear the uniform. It also gives those who have never served a comprehensive understanding of who these exceptional men and women are, and why they are known as the "Backbone of the Armed Forces."

JFQ

JOINT FORCE QUARTERLY
Published for the Chairman of the Joint Chiefs of Staff by National Defense University Press
National Defense University, Washington, DC

NDU Press