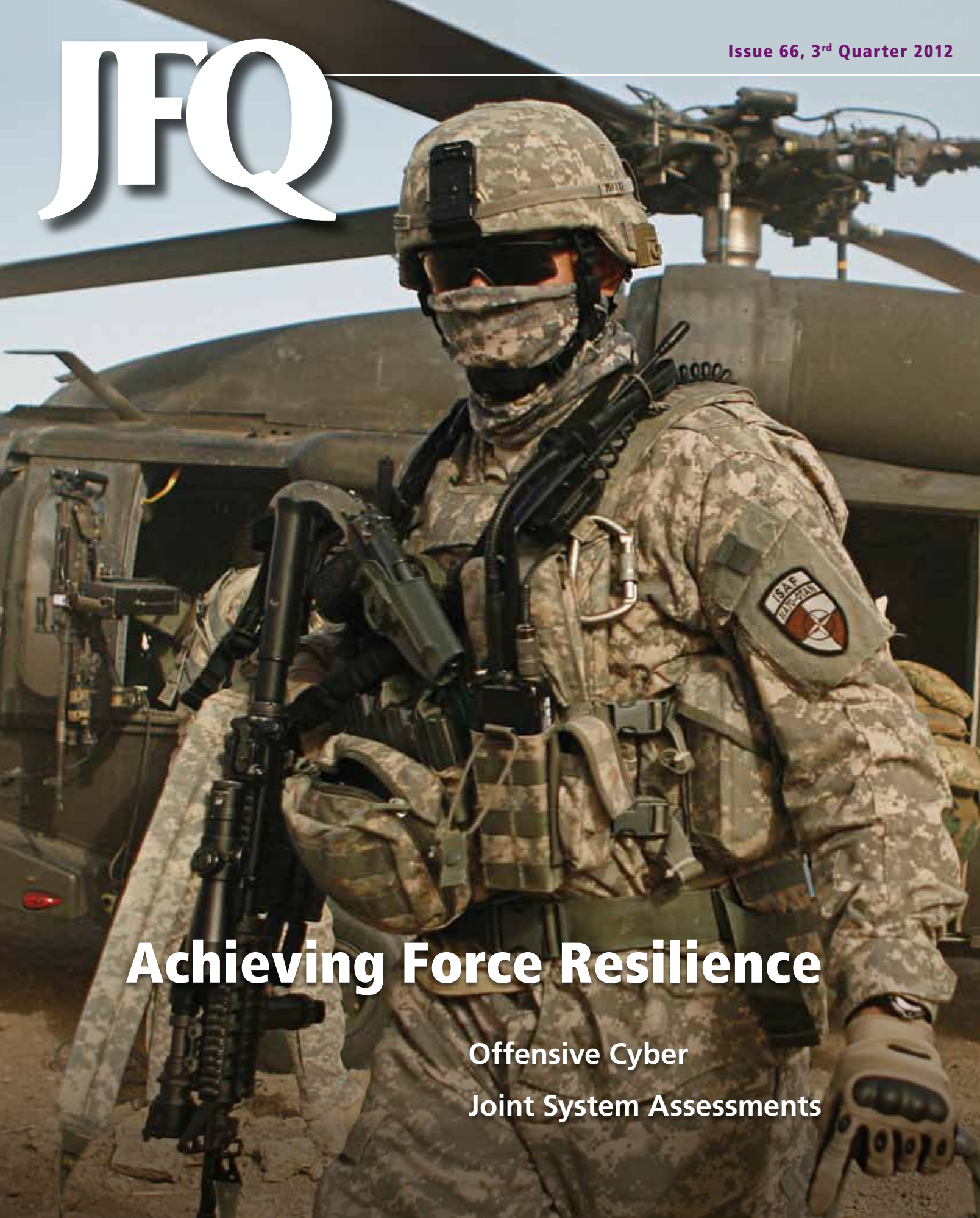
JFQ

Issue 66, 3rd Quarter 2012



Achieving Force Resilience

Offensive Cyber

Joint System Assessments

JOINT FORCE QUARTERLY

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
2012		**00-00-2012 to 00-00-2012**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Joint Force Quarterly. Issue 66, 3rd Quarter 2012	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **National Defense University,260 Fifth Avenue, S.W. (Building 64, Room 2505),Fort Lesley J. McNair,Washington,DC,20319**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**104**	

Inside

Issue 66, 3rd Quarter 2012

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

COMMUNICATIONS

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

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

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

3rd Quarter, July 2012
ISSN 1070-0692

JFQ Dialogue

Forum

Special Feature

Commentary

JFQ

Features

Book Reviews

Joint Doctrine

ABOUT THE COVERS

Front cover: Soldier exits UH-60 Blackhawk in village of Darrah-I-Bum, Badghis Province, Afghanistan (U.S. Marine Corps/Brian Kester). Table of contents shows (left to right) Soldiers in M2 Bradley Fighting Vehicles approach firing line at Nightmare Range, Camp Casey, Republic of Korea (U.S. Army/Ryan Elliott); Navy chaplain prays with Marines before security patrol in Sangin, Afghanistan (British Royal Army/James Elmer); Navy SEALs hoisted onto Air Force Special Operations CV-22 Osprey at Hurlburt Field (U.S. Air Force/Andy M. Kin); and Seaman stands watch in combat information center aboard USS *Monterey* (U.S. Navy/Daniel Viramontes).

CONTRIBUTIONS

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

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

ndupress.ndu.edu

From the Chairman

Making Strategy Work

Earlier this year, the President and Secretary of Defense released new strategic defense guidance, *Sustaining U.S. Global Leadership: Priorities for 21st Century Defense*. Six months on, I would like to share some of my insights about making the strategy and about making the strategy work.

Strategy is essentially about choices—choices about how to achieve our aims with the resources available to us. A sound strategy reconciles ends, ways, and means. Strategic coherence, however, does not just happen. Rather, it results from dialogue and debate. Our new defense strategy emerged from just such a collaborative process. The Service chiefs, who are charged with developing the force for the strategy, were heard early and often. The combatant commanders, charged with executing the strategy, all weighed in. And we were all afforded extraordinary access to our civilian leaders. Since the strategy was released, the Vice Chairman and I have gathered with the Service chiefs and combatant commanders for three full-day strategy seminars in Quantico, Virginia. We used these unprecedented forums to stress-test the strategy against some of the most challenging security scenarios we may face as a nation. This is exactly how it is supposed to work.

Strategic choices are not made in isolation. Instead, they are informed by a context. Once made, choices have consequences that create new context. It is an iterative process—that never ends. In this respect, strategy is as much emergent as it is deliberate.

The context we confront today can best be described as a security paradox. True, geopolitical trends are ushering in greater levels of peace and stability worldwide. But destructive technologies are also available to a wider array of adversaries. Destructive—and disruptive—technologies are proliferating down and out. They are proliferating vertically, down to violent nonstate actors, and they are proliferating horizontally, across advanced militaries in the world. As a result, more people have the ability to harm us than at any point in many decades.

Another compelling feature of our time is a new fiscal reality. Cost has reemerged as an independent variable in the U.S. national security equation. We have often defined our desired endstates before fully considering the cost. The money was there for us. As we advance on the joint force that we will need in 2020, we must consider cost sooner in our decisionmaking. We need to be more affordable in every possible way.

Within this context, the strategy makes choices that are already being put to work. I will highlight three, but there are more. First, we are mainlining capabilities that have really come into their own over the last decade. Among these are cyber, special operations, and intelligence, surveillance, and recon-

DOD (Erin A. Kirk-Cuomo)

Chairman receives update from commanding general, U.S. Forces–Afghanistan, at new Kabul compound

DOD (Glenn Fawcett)

Chairman speaking at the Law of the Sea Convention forum in Washington, DC

naissance. We are not just sustaining our investments in them; we are exploring new ways to organize and employ them. Each is potent in its own right, but when integrated into a global networked joint force, they create options that simply did not exist before.

Second, we are rebalancing toward the Asia-Pacific region. Of course, we never left. But security and socioeconomic trends speak to the region's growing consequence. For now, this shift in focus is more about thinking than it is doing. That said, we are doing some important things. The reintroduction of our Marines to Australia is just one example. We are also looking at our overall presence with an eye toward diversifying our relationships and activities. At the same time, we are affirming the value of several longstanding alliances throughout the region.

Third, we are expanding the envelope of cooperation. When we network within and beyond government, we add capacity and capability, and we gain credibility. In the future, we need to complement standing institutions and alliances with startup, purpose-driven communities of interest. Innovative partnering means working with old allies in new ways, boosting regional security architectures, and building on public-private efforts. It also means getting out of our own way. Security assistance reform is past due. Our export control and intelligence-sharing policies hinder our ability to build trust and make new friends. Effective partnering can be achieved with a modest investment. For that investment, we can expect an exponential return in cooperation.

The real test of this strategy is not in the choices we made, but in putting the choices to work. I am confident that we will pass this test for one simple reason—leadership. The young men and women charged to carry out the lion's share of this strategy are among the best leaders in the history of the U.S. Armed Forces. They prove daily that they have the minds, mettle, and muscle necessary for its success. For that reason, above all others, I am absolutely convinced that this strategy will meet the Nation's needs for the future, sustaining the trust put in us by the American people to defend them and our country. JFQ

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

Developing Joint Force Officer-Enlisted Leadership Capacity for the 21st Century

By CURTIS L. BROWNHILL

As a part of my efforts to assist the Chairman in moving the joint force toward where we need to be in 2020, I have seen the need to improve the quality of joint training and education for our enlisted leaders as they increasingly find themselves confronting the problem of operating in joint formations and staffs around the globe. While their Service training and education have prepared these leaders for their tactical missions, their training and education in joint operations have yet to meet the same standard. Chief Brownhill expresses many of the concerns I have heard from enlisted leaders in my travels as the Senior Enlisted Advisor to the Chairman (SEAC). I am certain that the Chairman and I will continue to seek the best possible joint training and education opportunities for the entire enlisted force as we adapt the entire joint force to meet the challenges ahead.

—Sergeant Major Brian B. Battaglia, USMC, SEAC

Across the globe, our all-volunteer joint force remains fully engaged in operations to keep our homeland secure, defeat global enemies, set conditions for global stability, and establish and maintain long-term multinational security partnerships. This remarkable joint force, led by a professional officer and senior enlisted leader corps, continues a legacy of greatness.

Our military is a learning organization, and advancements in joint capability have matured over the 26 years since passage of the Goldwater-Nichols Department of Defense Reorganization Act of 1986. However, the U.S. Government has yet to realize the act's *full* potential due to an institutional underinvestment in the joint development of its professional enlisted corps. "Just in time" training is both operationally shortsighted and professionally inadequate. To reach full capacity, the Department of Defense (DOD) must institute a comprehensive joint enlisted development concept that is commensurate with what our enlisted force is already doing (validated throughout a decade of war). It needs to begin early in a military career and be proportionate to predetermined levels.

Chief Master Sergeant Curtis L. Brownhill, USAF (Ret.), is the former Command Senior Enlisted Advisor, U.S. Central Command (2003–2007). He retired on August 1, 2007, after 34 years of service.

Why Joint Enlisted Education Is Needed

The 21st-century joint operating environment (JOE) is complex and can be generally characterized as a globalized, demographically emergent world with interdependent economies; shared and competing interests of developed and developing states; unpredictable failed states, rogue states, and nonstate actors; and ideologically based international terrorist networks fueled by dangerous historical animosities enhanced by technology.

The dynamic nature of the JOE is the new normal. For the U.S. Government and the Armed Forces, the scope and duration of current and future operations and missions will require tremendous flexibility and the ability to adjust to meet global threats. Clearly, given the magnitude of our strategic objectives, our enlisted leaders, alongside our officers, will be called upon to meet these challenges. We should anticipate more responsibilities to be placed on the shoulders of our noncommissioned officers (NCOs) and petty officers. This new and enduring environment will demand adequate educational preparation for all military leaders.

The JOE will shape our military doctrine and resultant Service force structures based on the strategic ways, means, and ends as determined by each combatant commander. Additionally, an interdependent joint force will require a well-trained joint battle staff in which NCOs and petty officers can and should play an increasing role. In any given operational area, our military leaders are immersed with U.S. interagency partners and allies in building long-term security cooperation partnerships (Phase 0 shaping). The JOE also demands the ability to integrate the efforts of DOD civilians, contractors, and international nongovernmental organizations.

Command Team Relationship

The cornerstone of the Armed Forces professional military model and the emulation of many a nation is our commitment to the strong and proven officer-enlisted leadership relationship resident within each Service. This unique capacity is a direct result of a lineage of honor and service, as well as nearly four decades of collective and determined professionalization of the all-volunteer force. Furthermore, the evolution of the NCO and petty officer from the traditional support leadership (what to do) role to one of empowerment and responsibility (how to think) role is matched only by the unquestioned trust and confidence placed in them by the officers of their respective Services. Today, NCOs and petty officers, regardless of Service, not only enhance the chain of command but are also responsible for a strong chain of communication in a far more complex environment than in the past.

At the root of the U.S. military officer-enlisted leadership relationship is the foundational concept of unity of command based on trust and confidence and grounded in mission accomplishment. This critical reality ensures continuity of mission and authority as an essential element of U.S. military doctrine and is intrinsic to each Service's core competencies and creeds. In essence, the battle will continue in the absence of the officer. For U.S. military NCOs and petty officers, this is a well-defined concept that ensures unit integrity, discipline, and overall effectiveness. Our NCOs are professionally developed to reach this standard. Difficulties arise, however, when proven officer-enlisted leadership relationships, time-tested unity of command, and communication qualities, seemingly easy to execute within their respective Services, must expand (often rather quickly) for leadership in joint and coalition organizations.

Goldwater-Nichols—The Next Step

Goldwater-Nichols was not an endstate in itself but an important first step in the direction of a fully integrated joint force. As a first step, it was not focused on expanding the joint aspect of the enlisted corps. Rather, it was principally focused on defining the combatant command lines of authority, improving joint operations and planning, and developing

officers capable of leading joint forces in the future. The drafters of the law may well have included a joint enlisted development focus had they been able to predict the second- and third-order effects of a quarter-century of collective joint development of our officers (by law) and over three decades applied to the professional evolution of the enlisted corps.

Goldwater-Nichols redirected a Service-centric military to become joint in planning and execution of operations, as well as developing officers from each Service educated in the reality of joint operations. As a result, the majority of our nation's military officers are steeped in joint doctrine and well prepared to lead in a joint-combined operational environment. However, while our officers (company grade, field grade, and senior) continue to depend heavily on their enlisted leaders to complement and enable them to be comprehensively effective, their enlisted leaders have not been adequately prepared for the same environment.

The operational analysis of the past 10 years reveals that the joint professional enlisted corps, specifically midgrade and senior enlisted leaders, complements the officer joint competencies of strategic-mindedness, critical thinking, skilled joint warfighting, process development, and planning in the tactical and operational battlespace and on joint force staffs. And they do that with little-to-no formal joint development opportunities. Complementing is fine, but enabling should be the goal.

A recognized term—the *strategic corporal*—is a means of illustrating that the tactical decisions made by Soldiers, Sailors, Marines, Airmen, and Coastguardsmen may indeed have strategic impacts. It is a realistic term that can be applied to all grades and levels, but it fails to acknowledge two key issues:

- If a corporal's actions could have either a positive or negative strategic effect, then how was the corporal developed for the task he was given?
- When a corporal looks up from a difficult or complex task for guidance, purpose, and strength, it is the NCO or petty officer he sees first.

These are important considerations. The NCO or petty officer could reasonably be termed the *operational staff sergeant*. Thus, our critical focus really must be on the operational staff sergeant who leads the strategic corporal and is a component of the officer-enlisted leadership team.

Unfortunately, for too many enlisted leaders regardless of Service, especially senior enlisted leaders, the leap from Service-centric tactical-level focus to joint/combined/interagency operational focus and mission exposure is immense. Many simply cannot adapt and overcome the unknown and can only find comfort in their Service-laden foxhole. They are not incapable of adapting—far from it; they simply have not been provided available joint education and preparation that provides confidence in leading forces other than their own. They, like commissioned officers, must have education, training, and seasoning to a level appropriate and proportionate to the environment in which they will operate and lead.

The Way Ahead

Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 1805.01, Enlisted Professional Military Education Policy, is limited as a forcing function to achieve full potential for a comprehensive joint development process for the enlisted corps. However, as a policy, it may be considered "directive enough" to accommodate the joint development of our junior and midlevel enlisted members with a proper focus. On the other hand, CJCSI 1805.01 falls well short as a policy (as opposed to a law) when addressing compelling joint development requirements of senior enlisted leaders and staff NCOs performing duties at operational and strategic level organizations.

As we work toward the necessary endstate of joint enlisted leaders, we must understand that any strategy to accomplish that should be pursued in a diligent manner that recognizes that it is essential to achieve joint capacity appropriate to the joint operational environment. We must remain aware that the strength of the joint team lies in the uniqueness of the ability of the Services to apply their capabilities at the decisive point to promote synergy of effort and accomplishment of the Nation's objectives. Furthermore, no strategy should dilute the distinction between the status of officers and enlisted members; it must instead complement it. This strategy cannot negatively affect command structure or degrade a Service's Title 10 responsibilities to organize, train, and equip forces.

Any strategy should be proportionate to the scope of each enlisted grade, keeping in mind that our young warriors, enablers, and rebuilders must remain focused on their primary military specialties. Most importantly, any strategy must strike a necessary and desirable balance between traditional Service culture and identity and the unique leadership demands resident within the joint force. The endstate of the strategy is to build upon what gives us our known strengths and capacities in order to make us even more effective for the future.

DOD should establish and adapt joint courses of study at the E-6 to E-9 grades at both Service and joint educational institutions, which provide the opportunities to grow student intellectual capacity at all levels. Such education should be accredited by civilian educational institutions and linked to advancement and consideration for selected joint duties. As an institution, DOD should feel comfortable in affording opportunities for selected enlisted leaders to attend appropriate levels of existing joint professional military education institutions traditionally reserved for junior and field-grade officers. Joint curriculum within the enlisted professional military education institutions of each Service should also be redefined and developed in ways that encourage "cross-pollination" of students on a large scale.

At a joint-minded level, we need to rethink our Service personnel systems, which could enhance the ability to ensure that our joint force commanders have the best possible considerations for critical joint-enlisted leadership and staff NCO positions in the future. While a policy would work for junior and midlevel enlisted grades, legislation might be required to ensure that our senior enlisted leaders are afforded the necessary advanced joint professional military education.

The U.S. officer-enlisted leader relationship and unity of command ethos is a cornerstone of our strength and success as a military. However, by simply sustaining it as it currently is, as opposed to advancing it to where it needs to go, we are setting the conditions for failure in meeting the leadership demands of the 21st-century joint operating environment. We require a new national vision and a broadened military culture that is consistent with this century and for this all-volunteer joint force. We need to be confident in taking the necessary bold steps in providing appropriate levels of joint development for the enlisted force to complement our joint officers and to advance the capabilities of the total joint force. **JFQ**

Executive Summary

A colleague of mine who teaches at the National War College recently returned from his annual visit to Afghanistan. This trip was different however as he was traveling with his seminar students. Before they departed, I wondered just what would become of them given the fluid situation there, at least from what we read in the press. Of course, given my own brief but instructive tour in Kabul in 2008, I knew that often the facts on the ground are hidden here at home because the lenses of the media are never able to capture the full scope of events anywhere.

While there is no doubt that danger of different kinds exists both in Afghanistan and here at home, nothing replaces the value of seeing the situation with one's own eyes. Many question the expense of sending professional military education (PME) students on foreign or even domestic travel. Given the chance to see more with one's classmates than what one experienced in the past—even if it means covering the same ground as before—is without doubt an invaluable experience for which no other means can substitute. Even with a combined number of over a dozen tours in Iraq and Afghanistan among this seminar, there were some who had experienced neither. The value of this new and shared experience was, as the commercial says, priceless. I have encouraged my colleague to urge these students to write about their experiences so that others may benefit, even if only to debate the issues of where we go next in Afghanistan or the world of 2020, which the Chairman is now seeking to understand. Experiences not evaluated and shared are lost. Many of those in PME classrooms today will soon be in positions to guide civilian leadership to achieve successful decisionmaking on strategy, policy, and even crisis management. Whether in the War College classroom or elsewhere, we continue to receive many insightful submissions that continue both to inform and discuss the ever-changing nature of jointness, the joint force, and the global challenges we face.

I was also recently reminded of how far we have traveled in the past few decades and how far we have to go as I attended an event where one of my Academy classmates—the first female graduate of any U.S. military academy to reach the rank of general—was promoted. In the summer of 1976, just 150 women entered the Air Force Academy with 10 times that many men. More than half of these women went on to graduate, with one achieving the highest rank possible some 32 years later. The U.S. military has two such women academy graduates at that rank, and as far as I am aware, we are the only nation that does. These women represent the best in all of us as Americans, confident in manner and able to achieve a path to success regardless of the challenges they face. The sniper in the photograph in this column is a person of similar character and achievement. As of this writing, the media are reporting on a lawsuit to remove the remaining restrictions on women in combat, and the Marines are evaluating women's fitness for combat duty. I suspect we will all learn that our national defense is based on capability to get the mission done regardless of other concerns.

In his From the Chairman column, General Martin Dempsey discusses the process and outcome of our national leaders' development of the new strategic defense guidance, *Sustaining U.S. Global Leadership: Priorities for 21st Century Defense*. The Chairman offers a valuable set of insights into the changing nature of strategy at the national level and what it will take to effectively execute it. Continuing to speak for the enlisted force within the joint force, Sergeant Major Brian Battaglia presents the commentary of Chief Master Sergeant Curtis L. Brownhill, the former Command Senior Enlisted Advisor, U.S. Central Command, on the need to provide better joint education for our enlisted leaders.

This edition's Forum brings us the thoughts of an experienced National Defense University researcher, a brand new officer, and a joint professional military education team, all focused on the growing area of cyber. From the Center for Strategic Research in the Institute for National Strategic Studies at the National Defense University, Vincent Manzo suggests that the U.S. Government needs to focus on an integrated effort to seek strategies to better defend and use the similar domains of space and cyber. Recent Air Force Academy graduate Second Lieutenant Soren Olson suggests our cyber defense efforts to protect our national infrastructure need substantial review and attention to prevent what he believes will be a likely massive attack in the near future. Rosemary Carter, Brent Feick, and Roy Undersander outline the requirement and suggest specific ways to integrate cyber operations below the joint force commander level, building on the argument offered by Brett Williams in *JFQ* in 2011. Cyber and space discussions continue to be among the most active topic areas based on *JFQ* submissions and reader feedback.

With the increasingly important and needed focus on the overall health of military members, veterans, and their families, especially those affected by our recent conflicts, the Special Feature section provides two substantial articles that reinforce the Chairman's efforts to effectively address this issue. While a specific Service program, the approach on resilience discussed by the USA Comprehensive Soldier Fitness leadership team of Rhonda Cornum, Thomas Vail, and Paul Lester offers extensively researched findings and commonsense recommendations for how senior leaders can dramatically improve the lives of the people they lead. Discussing a specific component of individual fitness, Patrick Sweeney, Jeffrey Rhodes, and Bruce Boling offer insights on the role religion plays in the overall health of military personnel.

In the Commentary section, we welcome back four *JFQ* veterans with their insights on several important and continuing themes in joint warfare that will likely be catalysts for others to respond with their views. First, from Australia, Carlo Kopp provides a guide to developing effective strategies during the era of exponential growth of new systems that characterizes the current information age. Next, Benjamin Lambeth provides an in-depth analysis of recent Israeli combined arms campaigns with enduring lessons for students of jointness. As the discussion over budgets and the Services continues to heat up, Lee Wright

U.S. Air Force (Daniel Hughes)

Staff Sergeant Alyssa Gomez, the ninth female sniper in the Air Force, demonstrates how a camouflaged ghillie suit blends into surroundings at Nevada Test and Training Range

compares the relative costs of recent conflicts and suggests airpower has not always been given its appropriate due. Finally, adding to his already rich offerings to the journal on strategy, operational planning, and thinking about doctrine, Milan Vego discusses the ancient but constant tension between science and art in the profession of war.

Having received a number of excellent submissions on specific technology, our Features section brings them together for review and comment. Now beginning to appear in significant numbers in combat and stability environments, nonlethal weapons still have a long way to go to convince many of their utility. Tracy Tafolla, David Trachtenberg, and John Aho discuss the background and current state of development and employment of this growing family of options for joint operations. After a turbulent and controversial development period, the current state of play with the CV-22 Osprey tilt-rotor aircraft is discussed by Eric Braganca. As with many defense acquisition programs, only when fielded will the true value of a capability be known. Another system still experiencing similar rough air, the Joint Strike Fighter F-35 aircraft is now beginning to be received by operational squadrons. Robbin Laird and Edward Timperlake discuss the operational and tactical significance this system will have for the future battlespace. As several states continue to field ballistic missile systems with the potential to attack other nations, the ability of missile defense systems to counter these emerging threats has been a major focus of U.S. national military strategy.

As always, we have our regular joint doctrine update, which in this issue completes the three-part series on multinational command by George Katsos; and to close out the issueof *JFQ*, we present three insightful book reviews.

We have just completed the annual Secretary of Defense and Chairman of the Joint Chiefs of Staff Strategy Essay Competitions, and the winning essays will appear in the October edition. The judges, many of whom are longtime veterans of this contest, believed as a group that this year's submissions from PME students were among the best they have seen. The key to these students' success is the fact that they wanted to compete. In the end, everyone who reads *JFQ* benefits from their efforts. These future senior leaders took the time and effort to write about issues they thought were important. I firmly believe there are even more authors interested in topics related to jointness waiting for their moment to do the same.

As an editor of a military journal, I frequently have the opportunity to work with both experienced and novice authors who want to get their ideas and experiences to our audience. I am always asked, "What should I write about for *JFQ*? What issues do you want to publish?" My answer is always the same: Write about what you know and what you think you need to have others understand. Ask questions and offer answers. Talk about your experiences and what you have learned directly as well as what you have learned from others. Frequently, when I am in the classroom, I ask students what our military world would be like if someone other than Carl von Clausewitz had taken the time and effort to write about war. Suddenly, writing a short essay for a military journal doesn't seem too difficult a task by comparison. **JFQ**

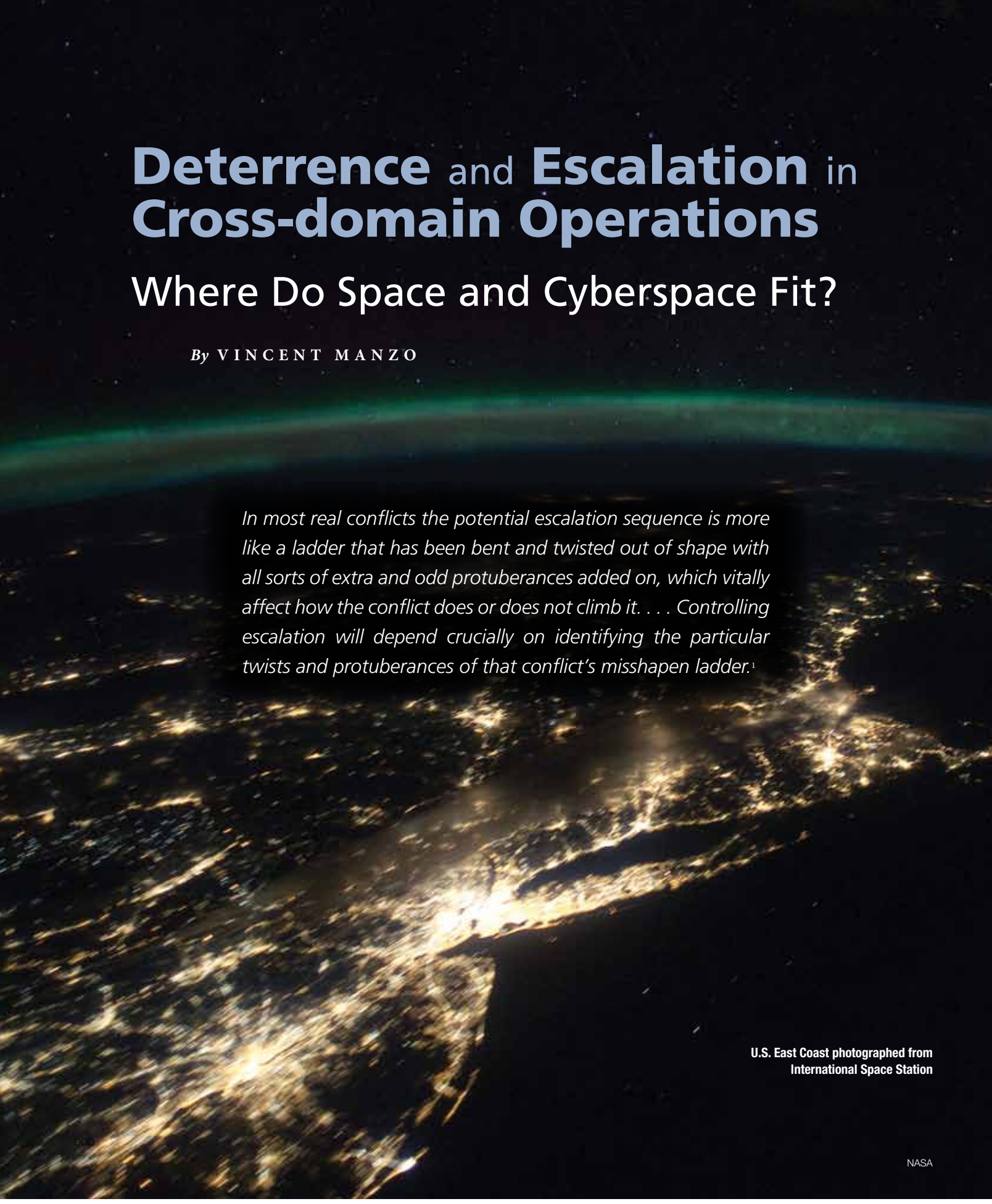
—William T. Eliason, Editor

Deterrence and Escalation in Cross-domain Operations

Where Do Space and Cyberspace Fit?

By VINCENT MANZO

In most real conflicts the potential escalation sequence is more like a ladder that has been bent and twisted out of shape with all sorts of extra and odd protuberances added on, which vitally affect how the conflict does or does not climb it. . . . Controlling escalation will depend crucially on identifying the particular twists and protuberances of that conflict's misshapen ladder.[1]



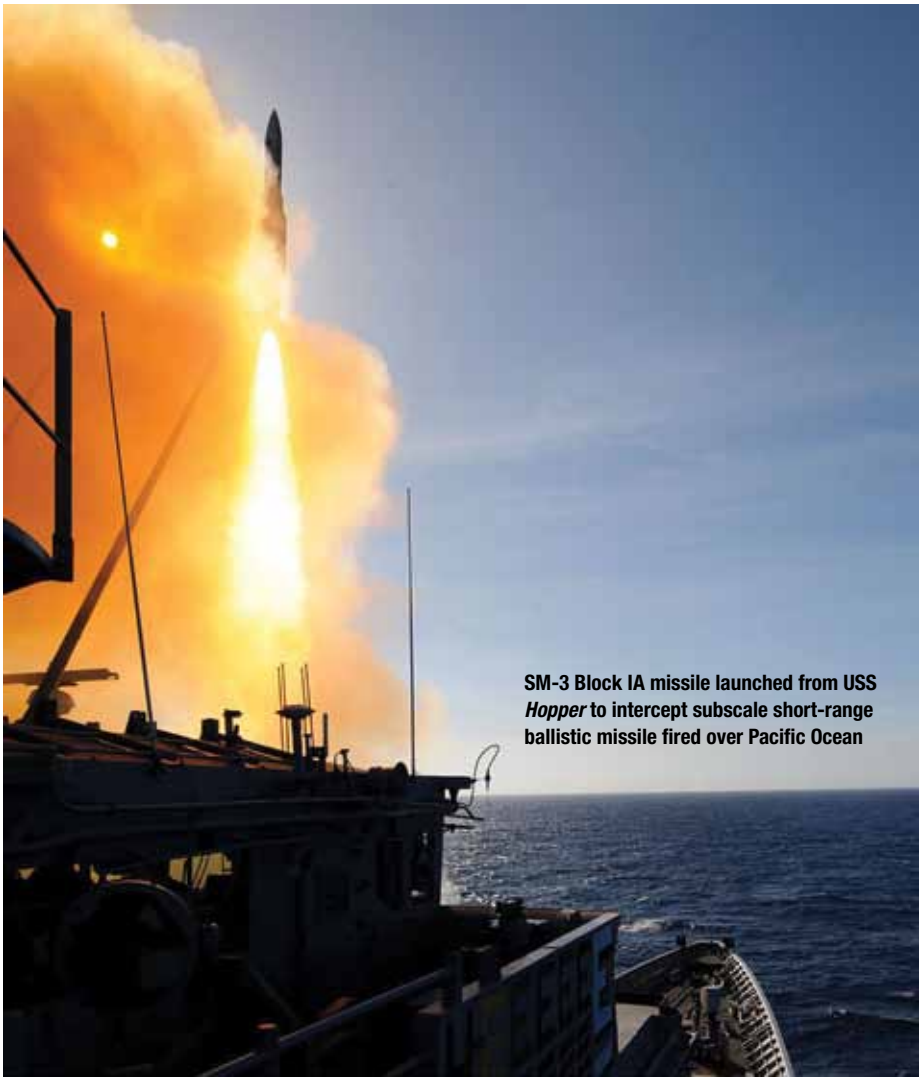
U.S. East Coast photographed from International Space Station

DOD

NASA

Warfare has become even more complicated since Richard Smoke wrote this description of escalation in 1977. The *National Security Space Strategy* describes space as "congested, contested, and competitive," yet satellites underpin U.S. military and economic power. Activity in cyberspace has permeated every facet of human activity, including U.S. military operations, yet the prospects for effective cyber defenses are bleak. Many other actors depend on continued access to these domains, but not nearly as much as the United States.

For this reason, some analysts argue that China's opening salvo in a conflict with the United States would unfold in space and cyberspace. Worst-case scenario assessments conclude that such an attack might render the United States blind, deaf, and dumb almost exclusively through nonkinetic means, although it is unclear how effective attacks in the space and cyber domains would be in an actual military conflict. How do concepts such as escalation, deterrence, and proportionality apply in such a context? What "odd protuberances" would counterspace and cyber attacks create in an escalation ladder? What are the salient thresholds for cross-domain attacks? And what exactly does *cross-domain* mean? This article explores these questions using the illustrative example of a hypothetical U.S.-China conflict because both countries possess diverse strategic capabilities that span air, land, sea, space, and cyberspace.



U.S. Navy

SM-3 Block IA missile launched from USS *Hopper* to intercept subscale short-range ballistic missile fired over Pacific Ocean

Defining Cross-domain: Platforms or Effects?

Cross-domain is an ambiguous term. U.S. doctrine identifies land, air, and sea as domains. Recent U.S. national security policy and strategy documents recognize space and cyberspace as distinct domains as well.[2] Assuming that all five are strategic domains, there are at least two different ways an action could cross domains.

Cross-domain could be defined according to the platform from which an actor launches an attack and the platform on which the target resides. Destroying a satellite with a ground-launched antisatellite (ASAT) missile is a cross-domain attack, whereas destroying one with a co-orbital ASAT (for example, a maneuverable satellite) is not. Striking a surface ship with a conventional air-launched cruise missile is a cross-domain attack, whereas an attack on the same target with a sea-launched cruise missile (SLCM) is not. Defining *cross-domain* by platforms demonstrates that cross-domain operations are not new. Air attacks on naval forces, naval attacks on air forces, and attacks from both domains on ground forces are common in modern warfare. Indeed, in many instances, a cross-domain operation might simply be the most expedient option. As an example, a nation under attack by SLCMs might, for a variety of reasons, be able to attack the adversary's naval assets more quickly with aircraft than with submarines and surface ships.

This definition might be too simplistic. Most U.S. military forces on land, in the air, and at sea make use of cyber and space assets, and most complex missions integrate contributions from multiple domains. One could even argue that a precision conventional strike is a cross-domain attack, regardless of whether the attacking platform and target are in the same domain, if it utilizes satellites and computer networks. By the same reasoning, characterizing a cyber attack—as opposed to cyber exploitation—against U.S. military computer networks as single-domain is misleading. If successful, such an attack would have important cross-domain effects: it would undermine the air, ground, or naval forces that depend on the degraded computer networks. These indirect effects in other domains are often the primary purpose of cyber attacks.[3] The same logic applies to attacks with co-orbital ASATs; even if the platforms are in the same domain, the effects are cross-domain.

Thus, *cross-domain* can also be defined according to the effects of an operation. Under this approach, an attack is cross-domain if its intended consequences unfold in a different

Vincent Manzo is a Research Analyst in the Center for Strategic Research, Institute for National Strategic Studies, at the National Defense University.

U.S. Air Force (Michael R. Holzworth)

Pilot conducts preflight check of F-16CJ

domain than its target. This definition illuminates that inter-domain relationships (our own and our adversary's) create strategic vulnerabilities.[4] For example, U.S. precision conventional strike operations depend on access to multiple domains. A potential adversary might be incapable of destroying U.S. aircraft or nuclear-powered cruise missile submarines, but it might be able to attack the space and cyber assets that enable these platforms to destroy targets. This appears to be the logic underlying China's interest in counterspace and cyber attacks: such attacks shift the conflict to domains where China's offensive forces have an advantage over U.S. defenses, thereby altering U.S. capabilities in domains (air and sea, for example) where China would otherwise be at a disadvantage.[5] This cross-domain approach would be ineffective if U.S. air, sea, and ground forces did not depend heavily upon space and cyber assets. Without this link, China would be unable to translate U.S. vulnerability in space and cyberspace into an operational impact in other domains. Cross-domain attacks thus enable an actor to best utilize its strengths and exploit an adversary's vulnerabilities in some instances. Reports that the United States considered launching a cyber attack at the start of North Atlantic Treaty Organization operations in Libya suggest that the U.S. military also perceives cross-domain attacks as useful for exploiting adversary vulnerabilities.[6]

Cross-domain Operations and Deterrence

These definitions highlight the fact that military actors frequently cross domains. Indeed, U.S. military posture is inherently cross-domain: U.S. offensive and defensive weapons are distributed across air-, sea-, and ground-based platforms; space and cyber assets are ubiquitous in U.S. military operations and engender advantages in other domains; and it is highly unlikely that future U.S. conflicts will unfold exclusively within one domain. From this perspective, U.S. deterrence is inherently cross-domain too: when the United States threatens to respond to actions that endanger U.S. and allied interests, it threatens, albeit implicitly in most cases, cross-domain responses. The platforms the United States employs, the targets it attacks, and the effect of the attack might be in different domains and might differ from the domains utilized in and affected by the adversary's initial attack.

By the same logic, the United States traditionally deters attacks in general, without distinguishing between attacks that cross domains and those that do not. Naval attacks on naval forces are not inherently more or less dangerous than air attacks on naval forces. The United States attempts to deter both, and the means, target, and scale of the U.S. response to either would depend on the effects of the attack and U.S. objectives rather than the domains involved.

Thus, the United States deters attacks, regardless of whether the attacks cross domains, by threatening responses that will likely cross domains and differ from the initial attack. Given that cross-domain deterrence is neither new nor rare, the real question underlying recent interest in the topic is: How can the United States mitigate vulnerabilities that stem from its dependence on space and cyberspace? Both are offense-dominant domains where U.S. defenses are inadequate and policymakers are uncertain about how to credibly threaten to impose costs on aggressors and deny benefits of attacks. Although potential adversaries depend on space and cyberspace less than the United States does, this does not explain why threats to respond to counterspace and cyber attacks in other domains are considered less credible than cross-domain responses to air, land, or sea attacks.

Shared Framework for Assessing Proportionality and Escalation in Space and Cyberspace

A concept Thomas Schelling explored in *Arms and Influence* is a useful starting point for answering these questions. Schelling argued that deterrence threats are more comprehensible to potential adversaries, and thus more credible, if they are proportionate with and connected to the actions they are intended to deter:

There is an idiom in this interaction, a tendency to keeps things in the same currency, to respond in the same language, to make the punishment fit the character of the crime. . . . It helps an opponent in understanding one's motive, and provides him a basis for judging what to expect as the consequences of his own actions . . . the direct connection between action and response helps to eliminate the possibility of sheer coincidence and makes one appear the consequence of the other.[7]

Of course, such communication requires that countries interpret military actions and reprisals similarly—in other words, that they communicate through a shared idiom of action.

Schelling also acknowledged that breaking a pattern of behavior (that is, escalation) might be necessary in some circumstances "to catch an adversary off balance, to display unreliability and dare the adversary to

respond in kind." Even then, however, a shared understanding of limits, norms, and expected responses creates a necessary frame of reference by which actors distinguish between proportionate and escalatory behavior: "Breaking the rules is more dramatic, and communicates more about one's intent, precisely because it can be seen as a refusal to abide by rules."[8]

The idiom of military action was never as coherent, communicable, and universally recognized in reality as it is in Schelling's prose. Nevertheless, during the Cold War, there was a generally accepted escalation ladder from conventional to chemical and biological to nuclear weapons. Within a conventional conflict, there has been an understanding that escalation can occur by broadening the geographical area of fighting, expanding the targets attacked (for example, shifting from narrow military to broader societal targets), and increasing the intensity of violence (for example, using more bombs per sortie or shifting to more destructive conventional weapons). The salient thresholds differ in every conventional conflict.

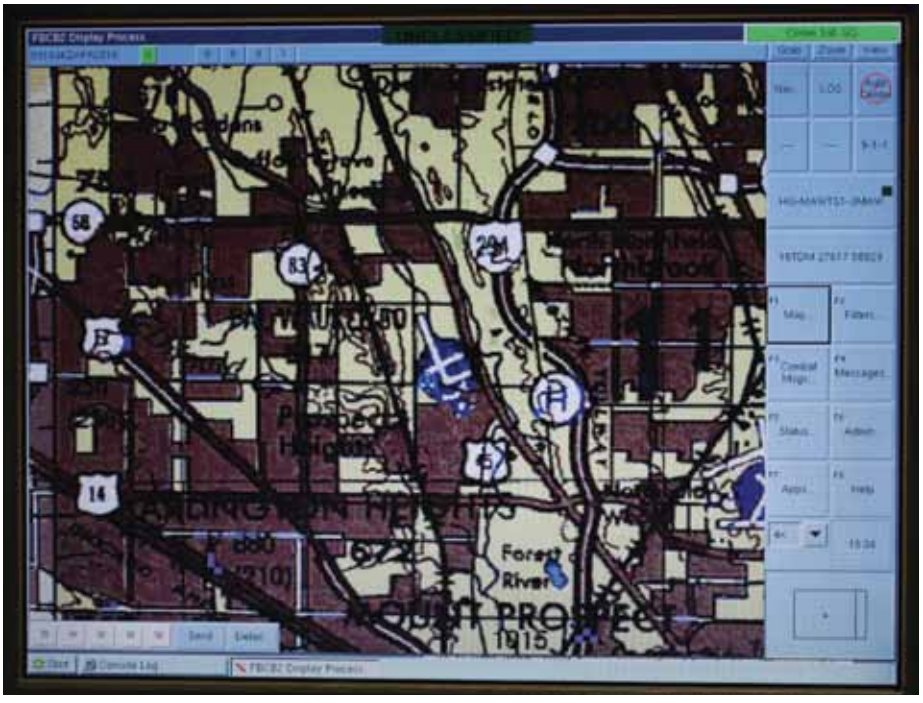
Unfortunately, countries lack a shared framework for interpreting how counterspace and cyber attacks fit into an escalation ladder. Competition and vulnerability in space and cyberspace are new relative to land, air, and sea. Countries have less experience fighting wars in which space and cyberspace are part of the battlefield. Unlike conventional and nuclear weapons, experts are less certain about the precise effects of attacks in these domains.[9] For these reasons, a widely shared framework for judging how counterspace and cyber attacks correspond with interactions in other domains and, more broadly, with political relations between potential adversaries during peacetime, in crises, and in wars does not yet exist. Without one, decisionmakers will have difficulty distinguishing between proportional and escalatory attacks and reprisals that cross from traditional strategic domains into these newer ones and vice versa.

The absence of a shared framework within the U.S. strategic community complicates effective cross-domain contingency planning. Developing coherent, effective, and usable options for responding to attacks in space and cyberspace requires that military planners in the different Services and combatant commands possess similar assumptions about cross-domain proportionality and escalation. For example, Principal Deputy Under Secretary of Defense for Policy James Miller testified that U.S. responses to counterspace attacks "could include necessary and proportional responses outside of the space domain."[10] Yet there are a variety of types of counterspace attacks and even more potential nonspace targets for U.S. reprisals. A common framework would help planners determine which "nonspace" responses best correspond with counterspace attacks of varying scope and severity.

The absence of a shared framework between the United States, allies, and potential adversaries undermines deterrence and increases the potential for miscalculation. Effective deterrence requires that U.S. officials influence potential adversaries' perceptions of the likely consequences of the actions the United States wishes to deter. The United States might threaten to respond to a particular type of attack in space or cyberspace by employing different capabilities against different targets in other domains. Such threats, however, are less likely to resonate as credible with potential adversaries if they do not understand U.S. assumptions about how domains are linked and why a particular response is a logical and proportional reaction to the initial attack.

As an example, imagine the United States threatened to respond to ASAT attacks on U.S. intelligence, surveillance, and reconnaissance (ISR) satellites with attacks against the adversary's air defense network. The logic underlying this policy is that the United States might employ ISR aircraft over the adversary's territory to compensate for the lost satellites. Attacks on the air defense network would be necessary to ensure that the aircraft could effectively penetrate the country's airspace. This policy is proportional because the United States is restoring its lost ISR capability, thereby denying the benefits of the ASAT attack. However, the U.S. response would be different from the adversary's attack. Instead of responding in space, the United States would attack targets on or around the adversary's homeland. To further complicate the situation, the United States might use conventional weapons to destroy the air defense network even if the initial ASAT attack was nonkinetic. Without a shared framework, potential adversaries might consider this deterrence threat illogical and therefore not credible. If deterrence failed, they might perceive such a U.S. response as arbitrary and escalatory. Even with a shared framework, they may still consider this response as escalatory, but they would also understand it to be a likely consequence of employing ASATs against the United States before authorizing an attack.

To be clear, a shared framework would not and could not prescribe set actions for every imaginable scenario. Rather, it would define a generic escalation ladder, a tacit or



U.S. Marine Corps (Benjamin R. Reynolds)

GPS-enabled Blue Force Tracker tactical operations center kit allows commanders to track forces in field

loosely defined code of conduct that would give decisionmakers a better sense of which actions and responses are expected and accepted in real-world scenarios and which would cross thresholds that escalate the situation. This would pave the way for more coherent cross-domain contingency planning within the U.S. Government and U.S. deterrence threats that potential adversaries perceive as clearer and more comprehensible and credible. The United States would also have a better understanding of the calculus of potential adversaries in their efforts to deter U.S. actions. Cultivating such a shared framework is a constructive goal for the future because deterrence, crisis management, and escalation control would be easier if different countries interpreted proportionality, connectedness, and escalation similarly. Engaging the U.S. strategic community in a thorough dialogue on these issues is the first step toward achieving this goal. Forming a deterrence working group of regionalists, functionalists, and legal experts might be a fruitful approach to starting this conversation.

What would be the basis for assessing counterspace and cyber attacks in a shared framework? Must responses to kinetic attacks also be kinetic to be proportional? Is a kinetic response to a nonkinetic attack always escalatory? Can a cyber attack be proportional to a cruise missile strike? How do officials compare attacks that strike targets in some domains and affect capabilities and events in other domains? Counterspace and cyber attacks can vary widely in intensity, from the equivalent of a tap on the shoulder to a fist in the face. Clearly, the mere act of extending the conflict into these domains is an insufficient metric for evaluating attacks and calibrating responses. Rather, the real-world effects of such attacks, both within the domain of the attack and in other domains, should determine whether they are escalatory and which responses would be appropriate.

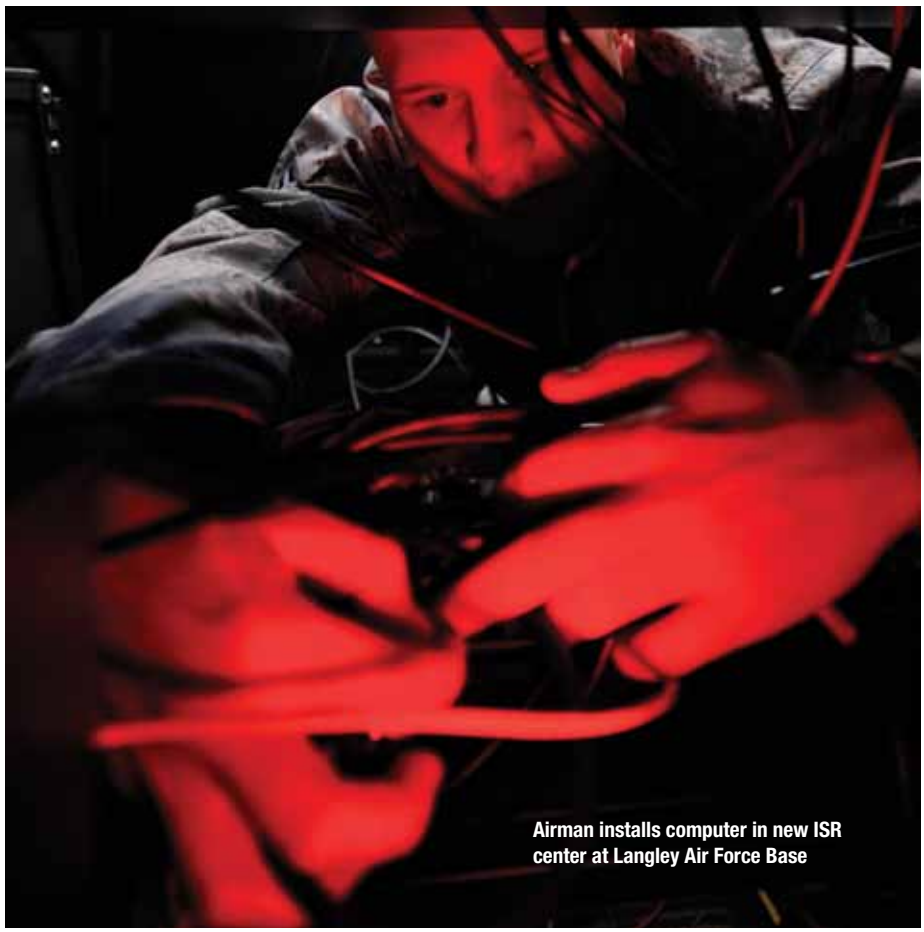
Variables in a Shared Framework

Cultivating a shared framework between potential adversaries for assessing effects and formulating appropriate responses is difficult regardless of how many domains are involved. U.S. and foreign officials interpret events through different prisms. Cultural differences, contrasting strategic objectives, differences in force structure and doctrine, and differing strengths and vulnerabilities can cause decisionmakers in the United States and other countries to reach different conclusions about proportionality and escalation.[11] This challenge is not new, but the uncertainties in emerging strategic domains discussed in the previous paragraphs might exacerbate it.

Imagine that China interferes with U.S. satellites via nonkinetic means (laser-dazzling or jamming) during a military crisis that has yet to escalate into an armed conflict. The United States might attempt to undermine China's ability to attack U.S. satellites, perhaps by scrambling its space-tracking data through a cyber attack. One could argue that this response is proportional because it is limited to systems that China is already employing against the United States and does not cross the kinetic threshold. On the other hand, one could argue that attacking in a new domain is escalatory, opening the door to reprisals and counterreprisals in cyberspace and other domains. Would Chinese officials distinguish between attacks on military computer networks and computer networks that support the regime's domestic security operations? If not, they might interpret this "proportional" response as an existential assault, especially if they believe that U.S. cyber attacks will cause collateral damage to computer networks other than the one targeted.

What if the initial Chinese ASAT attack is kinetic? Would U.S., allied, and Chinese officials perceive a nonkinetic response against China's space tracking capability as weak even if it succeeded in protecting U.S. satellites? On the other hand, would kinetic attacks on the ASAT weapons China is employing be proportional? Or would crossing the geographic threshold (assuming the targets are on mainland China) make this response escalatory? One could argue that a symmetrical response—a kinetic attack on a Chinese satellite—is proportional. However, if satellites play a smaller role in Chinese military operations, one could also argue that such a response is less than proportionate because it does not impose comparable operational costs on China.[12]

The balance between offense and defense in these domains will also influence perceptions of effects, escalation and proportionality, and optimal deterrence strategies. For example, if offense continues



U.S. Air Force (Dana Hill)

Airman installs computer in new ISR center at Langley Air Force Base

to dominate in space and cyberspace and potential adversaries want to attack U.S. assets in these domains precisely because they are the U.S. military's "soft underbelly," U.S. stakes in any conflict would grow exponentially after such attacks occur because the effects in other domains would be profound. As a result, U.S. officials might feel pressure to take preemptive action prior to such an attack, or they might take risks to quickly terminate a conflict and punish the adversary in its aftermath. The linkage between vulnerabilities in space and cyberspace and the effectiveness of U.S. capabilities in other domains that makes U.S. satellites and computer networks high-value targets also makes the threat of a strong reprisal more credible: it would be proportionate to the effects of the attack. Conveying this to potential adversaries would be a central component of a deterrence strategy. Emphasizing this link might even enhance the credibility of the U.S. commitment to retaliate.

Alternatively, the United States might become capable of denying adversaries the benefits of attacks in these domains through cyber defenses and substituting terrestrial assets for satellites. In this case, U.S. deterrence strategy would strive to convince potential adversaries that they cannot affect U.S. ground, air, naval, and nuclear forces by attacking satellites and computer networks. Such a message might make U.S. threats to respond offensively appear disproportionate and less credible, but this would be a worthwhile tradeoff if the United States developed a defensive advantage in space and cyberspace.

Decisionmakers will also perceive attacks in space and cyberspace differently depending on the context. Attacks on military satellites and computer networks might be expected and accepted once a conventional war has started. But similar attacks might trigger a conventional conflict if they occur prior to hostilities, when both countries want to prevent a crisis from escalating into a war but are concerned about being left blind, deaf, and dumb by a first strike in space and cyberspace. Proportionality and escalation are relative concepts: actions that are escalatory during crises might be proportionate in limited wars and underwhelming responses as the scope and intensity of a conflict increase.

U.S. Army (Sean P. Casey)

Soldier documents lay of the land with GPS camera in Afghanistan

A related issue is whether U.S. reactions to cyber exploitation during peacetime would affect deterrence in crises. Though the technology and operations of cyber exploitation and cyber attacks are similar, the goals and effects are different: exploitation extracts information from computers and networks without authorization; attacks destroy, degrade, or alter them to achieve effects in other domains.[13] But news outlets frequently describe incidents of cyber exploitation against the U.S. Government as cyber attacks and evidence of an ongoing war in cyberspace.[14] Conflating these operations contributes to the impression that U.S. deterrence has already failed. Potential adversaries might conclude that U.S. threats to respond to cyber attacks in other domains lack credibility based on how the United States reacted to previous exploitation operations. This perception might affect how they calculate risks and benefits of cyber attacks in crises. How can U.S. officials publicly convey that cyber exploitation and attacks pose different threats and require different responses, especially given the overlap between the two? Emphasizing that the real-world effects of attacks and exploitation differ might be a first step toward establishing a threshold between the two. This message would reinforce that deterrence has not failed because the effects of exploitation in cyberspace have not yet warranted U.S. military responses in other domains. It clarifies the types of actions that the United States is attempting to deter.

Some strategists may conclude that proportionate counterspace and cyber responses are impossible because escalation control in these domains is too difficult. There is an "infinite number of scenarios that are neither indicative of a minor harassing incident of jamming nor strategic attack" in space and cyberspace.[15] Assessing the effects of such attacks and choosing appropriate responses amid the stress and confusion of a military crisis might be difficult. U.S. and foreign officials likely will have differing views about the severity of nonkinetic disruptions that defy easy categorization, and the obstacles to developing a common framework might be too formidable. Furthermore, the effects of sophisticated attacks on satellites and computer networks might be indiscriminate and too difficult to predict. In this case, a

deterrence strategy could emphasize that limited counterspace and cyber attacks carry an intolerable risk of misperception, miscalculation, and unintended escalation. Evoking "threats that leave something to chance," U.S. officials could credibly argue that they are uncertain about what they would do because such attacks would involve "a process that is not entirely foreseen . . . reactions that are not fully predictable . . . decisions that are not wholly deliberate . . . events that are not fully under control."[16] Of course, expressing trepidation about unintended escalation could backfire. Adversaries may conclude that threatening such attacks would yield U.S. concessions.

actions that are escalatory during crises might be proportionate in limited wars and underwhelming responses as the scope and intensity of a conflict increase

Conclusion

Many weapons systems and most military operations require access to multiple domains (land, air, sea, space, and cyberspace). These linkages create vulnerabilities that actors can exploit by launching cross-domain attacks; the United States may seek to deter such attacks by threatening cross-domain responses. Yet both the U.S. Government and potential adversaries lack a shared framework for analyzing how concepts such as proportionality, escalation, credibility, and deterrence apply when capabilities in space and cyberspace not only enable operations in other domains but also are part of the battlefield. The real-world effects of attacks that strike targets in space and cyberspace and affect capabilities and events in other domains should be the basis for assessing their implications and determining whether responses in different domains are proportionate or escalatory.

Integrating actions in the emerging strategic domains of space and cyberspace with actions in traditional domains in a clear escalation ladder would be a first step toward more coherent cross-domain contingency planning within the U.S. Government. Communicating this framework to potential adversaries would contribute to more effective deterrence and crisis management. **JFQ**

NOTES

[1] Richard Smoke, *War: Controlling Escalation* (Cambridge: Harvard University Press, 1977), 252.

[2] See Department of Defense (DOD), *Quadrennial Defense Review Report* (Washington, DC: DOD, February 2010), 33–34, 37–39; The White House, *National Security Strategy* (Washington, DC: The White House, May 2010), 22; DOD, *National Security Space Strategy* (Washington, DC: DOD, January 2011); The White House, *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World* (Washington, DC: The White House, May 2011); DOD, *Department of Defense Strategy for Operating in Cyberspace* (Washington, DC: DOD, July 2011).

[3] A 2009 National Research Council report defined *cyber attacks* as deliberate actions that "alter, disrupt, degrade, or destroy adversary computer systems or networks or the information and/or programs resident in or transiting these systems or networks," whereas cyber exploitation is extracting information from computer systems or networks without authorization. The report demonstrates that the intended effects of cyber attacks occur in other domains: "Direct or immediate effects are effects on the computer system or network attacked. Indirect or follow-on effects are effects on the systems and/or devices that the attacked computer system or network controls or interacts with, or on the people that use or rely on the attacked computer system or network . . . the indirect effect is often the primary purpose of the attack." National Research Council, *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities* (Washington, DC: National Academies Press, 2009), 80.

[4] For more on interdomain relationships and vulnerability, see Mark E. Redden and Michael P. Hughes, *Global Commons and Domain Interrelationships: Time for a New Conceptual Framework?* INSS Strategic Forum 259 (Washington, DC: National Defense University Press, October 2010).

[5] For a discussion of the role of space, counterspace, and cyber capabilities in China's military strategy, see David C. Gompert and Phillip C. Saunders, *The Paradox of Power: Sino-American Strategic Restraint in an Age of Vulnerability* (Washington, DC: National Defense University Press, 2011), chapter 3; James Dobbins, David C. Gompert, David A. Shlapak, and Andrew Scobell, *Conflict with China: Prospects, Consequences, and Strategies for Deterrence* (Santa Monica, CA: RAND, 2011), 5–7; Office of the Secretary of Defense, *Annual Report to Congress, Military and Security Developments Involving the People's Republic of China 2010* (Washington, DC: DOD, August 2010), 22–37; Jan Van Tol with Mark Gunzinger, Andrew Krepinevich, and Jim Thomas, *AIRSEA Battle: A Point-of-Departure Operational Concept* (Washington, DC: Center for Strategic and Budgetary Assessments, 2010), 17–47; Roger Cliff et al., *Entering the Dragon's Lair: Chinese Anti-Access Strategies and their Implications for the United States* (Santa Monica, CA: RAND, 2007), 51–60.

[6] For reports of U.S. debates about launching a cyber attack against Libya, see Eric Schmitt and Thomas Shanker, "U.S. Debated Cyberwarfare in Attack Plan on Libya," *The New York Times*, October 18, 2011, and Ellen Nakashima, "Pentagon Officials Had Weighed Cyberattack on Gaddafi's Air Defenses," *The Washington Post*, October 18, 2011.

[7] Thomas C. Schelling, *Arms and Influence* (New Haven: Yale University Press, 1966), 146–149.

[8] Ibid., 150–151.

[9] For a discussion of expert uncertainty surrounding intended and cascading effects of cyber attacks, see National Research Council, 121–128.

[10] James N. Miller, testimony for the House Armed Services Committee, Subcommittee on Strategic Forces, March 2, 2011.

[11] For a theoretical/historical study of the causes and implications of doctrinal differences in U.S.-China relations, see Christopher P. Twomey, *The Military Lens: Doctrinal Differences and Deterrence Failure in Sino-American Relations* (Ithaca: Cornell University Press, 2010).

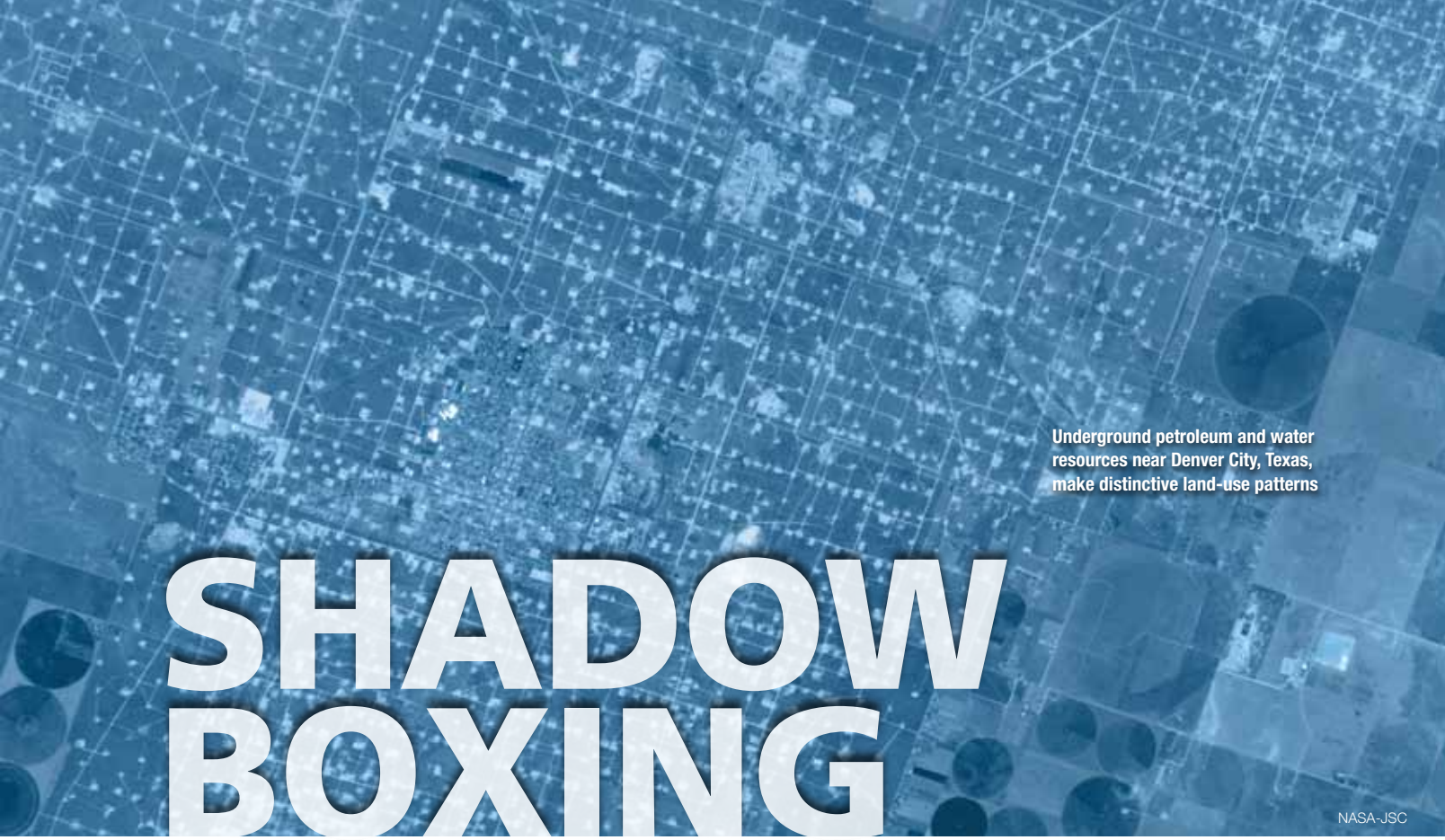
[12] This example demonstrates that symmetrical and asymmetrical responses to attacks in space and cyberspace are not synonymous with proportionate and escalatory responses; however, since symmetrical responses attack the same type of target with the same type of weapon in the same domain as the initial attack, it likely would be easier for different countries to reach similar assessments about whether such responses are proportionate or escalatory. Assessing asymmetric responses against targets in the same domain as the initial attack—which might attack the same type of target with different types of weapons, different types of targets with the same type of weapon, or different types of targets with different types of weapons—might be more difficult. Assessing asymmetric responses against targets in different domains than the attack would likely be the most difficult because it requires a shared standard for determining equivalencies across domains.

[13] National Research Council, 149–152.

[14] For example, Michael Riley and Ashlee Vance, "Cyber Weapons: The New Arms Race," *Bloomberg Businessweek*, July 20, 2011.

[15] Susan J. Helms, "Schriever Wargame 2010: Thoughts on Deterrence in the Non-Kinetic Domain," *Air Force Space Command High Frontier* 7, no. 1 (November 2010), 14.

[16] Schelling, 95.



Underground petroleum and water resources near Denver City, Texas, make distinctive land-use patterns

NASA-JSC

SHADOW BOXING

Cyber Warfare and Strategic Economic Attack

By SOREN OLSON

First attack the enemy's strategy, then his alliance, next his army, and last his cities.

—Sun Tzu, *The Art of War*

U.S. critical infrastructure and resources are open to assault by "clever and persistent" cyber attacks. Such attacks could dramatically affect the supply chain of our most strategic resource, petroleum. Two decades of warnings concerning cyber vulnerabilities inherent in U.S. infrastructure have effectively gone unheeded. Bureaucratic constructions such as U.S. Cyber Command (USCYBERCOM) create the illusion of security but do not address the true problem. As we focus on creating effects in the enemy, we largely ignore the effects the enemy can create in us. Our culture of strategic fads (for example, hybrid war, fourth-generation warfare, irregular war, counterinsurgency, and counterterrorism) and our force-centric threat assessment indicate that changes in the character of war and corresponding implications may be missed. The character of war now undeniably involves attacks against economic and domestic infrastructure and cyber methods will be the weapons of choice.

Lacking the flashy nature of weapons systems, protection of domestic infrastructure and economic systems does not command a sufficiently high priority in strategic planning. While the Department of Defense (DOD), Department of Homeland Security, and other parts of the U.S. strategic community have begun to respond to the threat posed by cyber warfare, more needs to be done. Action must be taken despite domestic infrastructure and economic systems being run by civilians and outside traditional DOD jurisdiction.

Further complicating the issue of jurisdiction is the Stuxnet program. Stuxnet demonstrated conclusively that nationally developed cyber weapons are being directed at civilian targets in order to achieve strategic effects. Moreover, with two of the three major exploits in the Siemens software that Stuxnet attacked remaining unpatched several years later, the willingness of private companies to protect critical infrastructure systems is called into question.[1] These two observations combine to suggest that cyber warfare will not respect traditional institutional responsibilities. Indeed, one must wonder if it might be unwise to leave defense against strategic-type attacks—by foreign nations and others—to private companies and the domestic security apparatus.

Many authors use pre- and post-9/11 to characterize a shift in a how terrorism was viewed. Prior to September 2001, terrorism was largely seen as a criminal behavior.[2] After the impact of terrorism was demonstrated, it became a matter of national defense. Similarly, cyber security must be thought of in terms of before and after Stuxnet; the tendency to view the use of cyber weapons as criminal must be replaced with a view that sees their use against any U.S. interest as a hostile act.

Second Lieutenant Soren Olson, USAF, is a graduate of the Department of Military and Strategic Studies at the United States Air Force Academy. He is currently undergoing pilot training at Columbus Air Force Base.

DOD (Cherie Cullen)

Commander, U.S. Strategic Command, General C. Robert Kehler

Evolution of a Weapon

Of the challenges facing U.S. strategists, the tendency to dismiss vulnerabilities inherent in domestic infrastructure is likely the most insidious. The hubris with which cyber vulnerabilities are viewed is well illustrated by the following:

Cyber attacks have a potentially important role to play against unprepared and unlucky adversaries that have enough sophistication to acquire and grow dependent upon information systems but not enough to defend them against a clever and persistent attack.[3]

U.S. domestic infrastructure is dependent on cyber technologies,[4] and dismissing or limiting the cyber threat to existing concepts of warfare will ensure we are unprepared and unlucky.

Many assert that advances in technology fundamentally change our world. Similarly, when new technologies, weapons, and tactics are observed, many strategists call them revolutions in military affairs (RMA). These RMAs are asserted to change how warfare is conducted.[5] Regardless of RMA's utility as a concept, some developments in warfare such as technology, weapons, or methods have altered the character of war. Cyber warfare is one of these.

Change in the character of war is always noticeable after the fact, but the development of the technologies and methods that are the basis of the change is not. The roots of shifts in warfare are often present and undergoing development for years prior to their first decisive employment. Use of railroads, telegraphic communications, and headlong assaults into fortified positions during the Civil War foreshadowed operations in World War I.[6] The Germans tested coordination of ground and air elements in the Spanish Civil War, years before it was employed on a large scale against the Polish and French in World War II.[7] Similarly, the Yom Kippur War in 1973 used airpower to pin and hammer ground formations—a technique that would be used nearly 20 years later in Operation *Desert Storm*.[8] In each example, the years between initial development and large-scale implementation served only to increase the lethality of the final product. Cyber warfare has been developed and tested in a similar manner to these examples, and reports have consistently warned of the danger such warfare poses.

In 1991, the National Research Council stated, "Many disasters may result from intentional attacks on systems, which can be prevented, detected, or recovered from through better security."[9] The report called for a coherent strategy. Six years later, a Presidential committee noted that there was still no coordinating agency as had been previously recommended. Oddly, it asserted that contrary to the 1991 report, the nature of cyber threats was still poorly understood.[10] In 2001, arguments about the relative strengths of defense and offense in this new domain[11] were so indecisive that a congressional subcommittee recommended the cyber security of critical U.S. infrastructure and networks be left to the private sector.[12]

Advocates for relying on private industry to defend critical infrastructure should recall that businesses cannot always be relied on to serve national interests. Private companies are unquestionably patriotic and responsible, yet strategists must not forget the names of projects, companies, and people synonymous with short-term focus: the Ford Pinto, Enron, Fannie Mae/Freddie Mac, and Bernie Madoff. Nor can strategists discount the possibility of a private company intentionally leaving cyber vulnerabilities for its own

exploitation or at the direction of another national power. In light of these concerns, it would seem unwise to place the mandate of national defense on private industry, particularly when the stakes are high and the ability or willingness of companies to defend against cyber weapons, such as Siemens in the case of Stuxnet, is questionable.

Despite past errors, there is no question that U.S. cyber capabilities are increasing, particularly with the recent creation of USCYBERCOM. However, apologists for current cyber defense efforts should consider this recent assessment of U.S. cyber defense efforts by the Government Accountability Office:

U.S. Strategic Command has identified that DOD's cyber workforce is undersized and unprepared to meet the current threat. . . . It remains unclear whether these gaps will be addressed since DOD has not conducted a more comprehensive department wide assessment of cyber-related capability gaps or established an implementation plan or funding strategy to resolve any gaps that may be identified.[13]

Twenty years of disaster, investigation, and policy change have repeatedly led to the same regrettable outcomes.

Refinement of cyber warfare continued even as this dark comedy of concern and inaction played out. By 1999, one defense official stated the Federal Bureau of Investigation (FBI) was investigating some 6,080 daily attacks that were recorded on DOD computer systems.[14] In 2001, researchers at Dartmouth University predicted that cyber attacks would be the asymmetric weapon of choice for hostile groups and countries well into the future.[15] In 2003, the *Guardian* commented that U.S. Federal organizations were experiencing such a staggering number of cyber attacks on critical networks that the attacks were code-named "Titan Rain."[16] At this point, the Federal Government began pondering whether commercial cyber networks should be considered critical infrastructure and thus protected, but it took little significant action. A 2005 Presidential committee found that the "computers that manage critical U.S. facilities, infrastructures, and essential services can be targeted to set off system-wide failures, and these computers frequently are accessible from virtually anywhere in the world via the Internet."[17]

In March 2009, *Forbes* described a cyber espionage ring known as "GhostNet." GhostNet is thought to have infiltrated the government networks of 117 nations.[18] Such intrusions demonstrate the capability of foreign attackers to penetrate critical defended networks over long periods. Finally, the Stuxnet worm was discovered in July 2010 and is an example of cyber warfare coming of age. In a situation where traditional military attack was politically impractical, this complex series of 1s and 0s is asserted to have seriously damaged or even delayed the Iranian nuclear program.[19]

Despite its demonstrated capability to produce kinetic effects, the true significance of cyber warfare lies in its strategic application. Cyber warfare is ideally suited to Sun Tzu's definitive order of attack when engaging an enemy: "First attack the enemy's strategy, then his alliance, next his army, and last his cities."[20]

An adversary looking to attack the strategy of the United States should first determine what it seeks to protect. Security of energy supplies is the driving priority of current U.S. foreign policy, and trillions of defense dollars have been spent on maintaining access to Middle East oil supplies.[21] It is a cruel irony that in spite of this investment, persistent vulnerabilities in the oil supply chain demonstrate that the U.S. commitment to critical resource defense remains lacking.[22]

the anonymity of cyber warfare allows coordinated "submarine"-like attacks against the physical and cyber aspects of the U.S. petroleum supply chain

Crude Threat

As the world's largest consumer of petroleum, the United States is unable to supply its demand from domestic sources. Accordingly, some 36 percent of imports come from concentrated overseas routes and another 27 percent is transported into the continental United States via overland pipelines.[23] Even domestic petroleum depends on the domestic pipeline system. The ability to attack or defend this global and domestic petroleum supply network rests on computer systems.[24] Commercial guardians of critical resources, such as petroleum infrastructure, have been unable to even keep abreast with revealed vulnerabilities of supervisory control and data acquisition systems (SCADA).[25] They are not prepared for the onslaught that history dictates will be orders of magnitude greater than any cyber attack previously employed.

Historically, nations that import energy from sources prone to invisible attacks do not fare well. In World War II, U.S. submarines intentionally targeted Japanese petroleum imports.[26] After 2 years of invisible battering, less than 28 percent of oil shipped reached Japan.[27] Furthermore, the "loss of raw materials and petroleum and inability to transport items to the front lines lay at the heart of Japan's weakening ability to maintain effective military strength."[28] In the face of a sustained and coordinated attack, it is nearly impossible to completely defend an expansive network against an invisible enemy.

With cyber warfare, the true danger lies in the ability of an enemy to coordinate disparate actors and launch them against global interests while simultaneously attacking U.S. domestic petroleum infrastructure. In the late 1500s, England used privateers to attack the Spanish economy by raiding the gold-laden vessels sailing out of Central America. More recent examples are the American use of the Contras and mujahideen during the Cold War, as well as the Soviet support of Central American guerrillas. Among pawn employments, the Russian use of "patriotic" hackers against the Georgian banking and communication systems in 2008 is most applicable.[29] Each example points to the malleability of independent groups by a greater power.

The value of pawns in cyber warfare is that they further complicate attribution. A power can find and map vulnerabilities and then coordinate strikes using intermediaries. Past mapping of network and infrastructure vulnerabilities has not been treated as an act of war. Thus, while the source of information enabling the attacks may be known, so long as the originating hostile power uses pawns, there would be little direct action the United States could undertake.

Today, the spread of al Qaeda affiliates and other armed groups results in more pawns willing to attack American interests. This is the opportunity that a coordinating nation-state would offer such groups:

It should be clear that the energy infrastructure of the United States is its lifeblood, and as such,

it is one of the most critical of all infrastructures. The assets of the oil and gas industry are thus clear targets for economic jihad.[30]

Somali pirates are already using information from within shipping companies to seize vessels off the Horn of Africa.[31] These pirate groups have demonstrated a willingness to act on information received concerning the vulnerabilities of Western shipping companies. Modern pirates, armed with inside information, do token amounts of damage compared to the havoc an anonymous, malicious state actor could generate with a coordinated campaign. However, direct physical attacks augmented by information procured from cyber warfare are only one part of the threat: "The reliance on cyber technologies creates the opportunity for interrupted communications, false or misleading transactions, fraud, or breach of contracts, and can result in loss of service, loss of stakeholder confidence, or the failure of the business itself."[32]

Similarly, the anonymity of cyber warfare[33] allows coordinated "submarine"-like attacks against the physical and cyber aspects of the U.S. petroleum supply chain. The proliferation of armed groups along global shipping routes could allow an anonymous actor to coordinate an equivalent submarine campaign against the physical links of the global oil supply chain. This campaign of resource disruption would be aided by direct cyber attacks against the SCADA systems that run petroleum logistic hubs in the United States.

Logistics hubs serve as gateways for regional supply. They are characterized by interconnections among many pipelines and, often, other modes of transportation—such as tankers and barges, sometimes rail, and usually trucks, especially those used for local transport—that allow supply to move from system to system across counties, states, and regions in a hub-to-hub progression.[34]

When examining the layout of the U.S. petroleum infrastructure, concentration of pipelines run by SCADA systems at logistics hubs are clear domestic chokepoints. There are six primary hubs in the United States. These hubs are vulnerable to cyber sabotage directed either at the SCADA systems or the power grid supporting the hubs, as was demonstrated in 2007 when "an ice storm knocked out power to the hub in Cushing, Oklahoma, shutting down four crude oil pipelines [and] halting transport of roughly 770,000 barrels of oil per day."[35]

Though little known now, the 1982 U.S. cyber attack on the Trans-Siberian oil pipeline used a Trojan program that caused an explosion within the pipeline equivalent to a 3-kiloton weapon: "The U.S. managed to disrupt supplies of gas and consequential foreign currency earnings of the Soviet Union

U.S. Air Force (Lou Hernandez)

Anacortes Oil Refinery at base of Mount Baker, Washington

for over a year."[36] Though this example shows that cyber warfare's kinetic effects can be fearsome, such are not necessary to cause catastrophic economic damage.

Fear of Fear?

Deliberate attacks by a nation-state, using a combination of cyber weapons and traditional arms, have already been directed at economic targets. The addition of cyber means and economic targeting to the character of war was first demonstrated by the Russians:

When Russia invaded Georgia, a large portion of its military operations focused not on securing the areas inhabited by ethnic Russians but on Georgian ports and facilities for handling oil and gas. Unstable ground conditions, augmented by cyber attacks, soon made all of the Georgian pipelines seem unreliable. Meanwhile, 2 days after the invasion began, the Turkish section of the Baku-Tbilisi-Ceyhan pipeline was attacked by local militants, supposedly on their own initiative. One result of these developments was that BP Azerbaijan shifted its oil transport to the Russian Baku-Novorossiisk pipeline, even though the costs were double those of the Georgian pipelines.[37]

Cyber warfare was employed to leverage a target that was purely economic. BP shifted its oil contracts based on perception; physical compromise of the Georgian pipeline was not necessary. Due to the influence of perception, Georgia experienced serious economic damage with no physical destruction of infrastructure.

Given the ease with which economic damage can be inflicted on a single economic target, in this case a pipeline, one can see how the global system the United States relies on is at risk. Furthermore, proliferation of pawns would make it easy for a power to use them to coordinate attacks against the maritime routes and land-based logistic hubs used for transport of petroleum. Only a few of these attacks would need to succeed to undermine the foundation of the international energy system and reliable transport:

In 2007, total world oil production amounted to approximately 85 million barrels per day (bbl/d), and around half, or over 43 million bbl/d of oil, was moved by tankers on fixed maritime routes. The international energy market is dependent on reliable transport. The blockage of a chokepoint, even temporarily, can lead to substantial increases in total energy costs. In addition, chokepoints leave oil tankers vulnerable to theft from pirates, terrorist attacks, and political unrest in the form of wars or hostilities as well as shipping accidents.[38]

One commentator asserts that cyber attacks also look for "digital chokepoints," such as the electrical grid. As he explains, "Cyberspace is complex terrain, but the same idea obtains: squeeze a vulnerable throat."[39] Cyber warfare, like submarine warfare, is ideally suited to closing chokepoints. This approach was successfully employed by the United States against the Japanese; planners must anticipate a similar attack against the U.S. oil supply chain if only because of the potential for catastrophic damage. An incident that closed the Strait of Malacca even temporarily would reroute 50 percent of the world's shipping and cause further doubts about the reliability of energy transport. The potential economic damage from a coordinated cyber campaign executed on global oil chokepoints by a major power—or on domestic chokepoints—is inestimable.[40]

active defense for infrastructure systems would take years of development before they could be trusted to match modern offensive weapons

Shadow Puppets

Cyber weapons, potential proxies, and supply chain vulnerabilities all exist. What remains to be examined is what might motivate an actor to coordinate such a campaign. Sun Tzu and Carl von Clausewitz suggest what might cause such a campaign against U.S. petroleum supplies. First, consider Clausewitz's assertion that "Strong fortifications force the enemy elsewhere." Even in economic decline, the U.S. military has demonstrated its ability to fight in three conflicts on the opposite side of the world.[41] This military strength forces potential opponents to find a more effective angle of attack, such as a vulnerable supply line that provides a vital strategic resource. Second, the use of cyber against strategic resources is in accordance with Sun Tzu's maxim "to defeat the enemy without fighting and, when necessary, to win first, and then fight." These two concepts support the idea of removing a strategic resource via asymmetric and anonymous means. The example of submarine warfare in World War II, interdicting strategic resources, though not anonymous, demonstrates the ability of economic targeting by an invisible opponent to bring a great power to its knees.

However, the cyber warfare foreshadowed by Stuxnet and envisioned here would require resources in numbers that are available only to state actors.[42] Furthermore, such an indirect approach is distinctly contrary to typical Western strategy.[43] Whose hand should the United States expect to wield cyber warfare against its interests? It stands to reason that the nation with the clearest motive and intent is the most likely to challenge the reigning superpower.

The idea of using cyber warfare to strike at an unanticipated target, such as strategic resources, is perfectly in line with the Chinese concept of warfare known as *shashoujian*:[44] "Once strengths and weaknesses have been identified and assessed, the strengths can be avoided, and the weaknesses can be targeted for attack using *shashoujian*."[45]

Since 2004, China has conducted at least 14 major cyber attacks, including Titan Rain and GhostNet, on targets ranging from ExxonMobile and the German chancellor to Indian and DOD military networks.[46] The signs of weapon development have been noted, and the call for economic weaponization by Chinese experts has gone out: "It is only necessary to break with our mental habit of treating the weapons' generations, users, and combinations as being fixed to be able to turn something that is rotten into something miraculous."[47] The authors later give an example of what might be accomplished with such an approach:

On October 19, 1987, U.S. Navy ships attacked an Iranian oil drilling platform in the Persian Gulf. News of this reached the New York Stock Exchange and immediately set off the worst stock market crash in the history of Wall Street. This event, which came to be known as Black Monday, caused the loss of $560 billion in book value to the American stock market.[48]

Though this is an inaccurate claim, the validity of the statement is irrelevant insofar as the Chinese believe it is true.

Admittedly an attack by the Chinese against the international links of the U.S. petroleum supply chain would injure their own economy.[49] For this reason it seems unlikely they would attack international links except as a prelude to full-scale war with the United States.[50] However, the theory of economic interdependence should not be used as a shield to dismiss the possibility of economic cyber attack. Prior to World War I, the theory circulated that nations would not go to war as the economic devastation would be too great, yet it proved wrong.

Shadows' War

The destructive potential of cyber warfare in the economic, social, and physical realms demands that it be accorded the same level of respect and study strategists afford nuclear weapons. Defending against cyber attacks is like defending against nuclear weapons: attacks can take nearly any form and come from anywhere, and static defenses can be overwhelmed through mass or unconventional delivery. Unlike nuclear weapons, the anonymous and diffuse nature of cyber war may make deterrence impossible.

Further complicating successful defense is the proliferation of potential pawns that could be invisibly manipulated via cyber means. When this combines with the success of repeated enemy infiltration (Titan Rain), the global scope of infiltrations (GhostNet), and the kinetic effects (Stuxnet), no defense should be expected to withstand a coordinated cyber assault. Cyber warfare is well developed, and active defense for infrastructure systems would take years of development before they could be trusted to match modern offensive weapons. Active defense must not be the first focus. Instead, engaging in passive defense, evaluating vulnerabilities, creating backup systems, determining opponent cyber capabilities, and solving the attribution problem must take priority.

The problem of jurisdiction over cyber defense and the conundrum that DOD faces in the form of a mandate for national defense and a prohibition against domestic operations are not issues that can be solved by strategists. As the complications were created by national law, they can only be solved by national law. However, this inability to immediately fix a problem should not deter strategists from considering the uncomfortable implications of an infrastructure that is indefensible against modern cyber weapons and might not be reliable in case of limited or full-spectrum conflict.

We must recognize that while there are significant vulnerabilities among the links in the U.S. oil supply chain, they are but symptoms of a larger problem. Warnings about cyber warfare have been present for years, but reminiscent of another prominent defense failure prior to 9/11, actions taken remain insufficient. In light of these facts, we face the uncomfortable truth that China, as well as other nations, possesses a weapon, and our best defense against it amounts to boxing with its shadow. **JFQ**

NOTES

[1] Paul Roberts, "Many Stuxnet Vulnerabilities Still Unpatched," *Threatpost.com*, Kaspersky Lab Security News Service, June 8, 2011.

[2] Stephen D. Biddle, *American Grand Strategy after 9/11: An Assessment* (Carlisle, PA: U.S. Army War College Strategic Studies Institute, 2003), 25.

[3] Martin C. Libicki, "Cyberwar as a Confidence Game," *Strategic Studies Quarterly* 5, no. 1 (Spring 2011), 134.

[4] *Cyberspace Policy Review* (Washington, DC: The White House, May 2009), 3, available at <www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf>.

[5] Andrew F. Krepinevich, Jr., *The Military-Technical Revolution: A Preliminary Assessment* (Washington, DC: Center for Strategic and Budgetary Assessments, 2002, from Office of Net Assessment, 1992), 3, available at <www.csbaonline.org/wp-content/uploads/2011/03/2002.10.02-Military-Technical-Revolution.pdf>.

[6] Paddy Griffith, *Battle Tactics of the Civil War* (New Haven, CT: Yale University Press, 1989), 20.

[7] Rainer Waelde, *The Experience of the Japanese-Chinese War and of the Spanish Civil War for the Development of the German "Blitzkrieg Doctrine" and Its Lessons for the Transformation Process* (Fort Leavenworth, KS: U.S. Army Command and General Staff College, 2003), 25, available at <www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA419865&Location=U2&doc=GetTRDoc.pdf>.

[8] Steven Baxter, "Arab-Israeli War October 1973: Lessons Remembered, Lessons Forgotten" (Master's thesis, Naval War College, 1994), available at <www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA279557&Location=U2&doc=GetTRDoc.pdf >.

[9] National Research Council, *Computers at Risk: Safe Computing in the Information Age* (Washington, DC: National Academies Press, 1991), 2–3.

[10] President's Commission on Critical Infrastructure Protection, *Critical Foundations: Protecting America's Infrastructures* (Washington, DC: The White House, October 1997), 78, available at <www.fas.org/sgp/library/pccip.pdf>.

[11] Professionals for Cyber Defense, letter to President George W. Bush, February 27, 2002, available at <www.uspcd.org/letter.html>.

[12] General Accounting Office, *Critical Infrastructure Protection: Significant Challenges for Developing National Capabilities,* report to the Subcommittee on Technology, Terrorism, and Government Information, Committee on the Judiciary, U.S. Senate, April 2001, available at <www.gao.gov/new.items/d01323.pdf>.

[13] Government Accountability Office, *Defense Department Cyber Efforts: DOD Faces Challenges in Its Cyber Activities*, report to Congressional Requesters, July 2011, available at <www.gao.gov/new.items/d1175.pdf>.

[14] "Guarding Cyber Pentagon," *CNN.com*, available at <http://articles.cnn.com/1999-03-05/tech/9903_05_pentagon.hackers_1_pentagon-computers-computer-attacks-computer-hackers?_s=PM:TECH>.

[15] Michael Vatis, *Cyber Attacks During the War on Terrorism: A Predictive Analysis* (Dartmouth, NH: Institute for Security Technology Studies, September 24, 2001), available at <www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA395300>.

[16] Richard Norton-Taylor, "Titan Rain: How Chinese Hackers Targeted Whitehall," *The Guardian*, September 4, 2007, available at <www.guardian.co.uk/technology/2007/sep/04/news.internet>.

[17] President's Information Technology Advisory Committee, *Cyber Security: A Crisis of Prioritization* (Arlington, VA: National Coordination Office for Information Technology Research and Development, February 2005), 17, available at <www.nitrd.gov/pitac/reports/20050301_cybersecurity/cybersecurity.pdf.>

[18] Paul Maidment, "GhostNet in the Machine," *Forbes.com*, March 29, 2009, available at <www.forbes.com/2009/03/29/ghostnet-computer-security-internet-technology-ghostnet.html>.

[19] William J. Broad, John Markoff, and David E. Sanger, "Israeli Test on Worm Called Crucial in Iran Nuclear Delay," *The New York Times*, January 15, 2011.

[20] Sun Tzu, *The Art of War*, trans. Samuel B. Griffith (Oxford: Oxford University Press, 1973), 77–78.

[21] Daniel Yergin, "Ensuring Energy Security," *Foreign Affairs* 85, no. 2 (March–April 2006), 82.

[22] Walter Russell Mead, "The Serpent and the Dove," in *Special Providence: American Foreign*

Policy and How It Changed the World (New York: Routledge, 2002), 110.

[23] U.S. Energy Information Administration, "How Dependent Are We on Foreign Oil?" *Energy in Brief* (Washington, DC: Department of Energy, June 24, 2011), available at <www.eia.doe.gov/energy_in_brief/foreign_oil_dependence.cfm>.

[24] Ulf Lindqvist, "Securing Control Systems in the Oil and Gas Infrastructure," *Oil & Gas Processing Review* (London: Touch Briefings, 2005), available at <www.touchbriefings.com/pdf/1713/ACF1A57.pdf>.

[25] Roberts.

[26] Navy Department, *Section III: Japanese Anti-Submarine Warfare and Weapons*, War Damage Report, no. 58 (Washington, DC: U.S. Hydrographic Office, January 1, 1949), 8, available at <www.ibiblio.org/hyperwar/USN/rep/WDR/WDR58/WDR58-3.html>.

[27] W.J. Holmes. *Undersea Victory: The Influence of Submarine Operations on the War in the Pacific* (Garden City, NY: Doubleday, 1966), 425.

[28] Michel T. Poirier, "Results of the American Pacific Submarine Campaign of World War II," U.S. Navy, December 30, 1999, available at <www.navy.mil/navydata/cno/n87/history/pac-campaign.html#N_19>.

[29] David Hollis, "Cyberwar Case Study: Georgia 2008," *Small Wars Journal*, January 6, 2011, 2, available at <http://smallwarsjournal.com/blog/journal/docs-temp/639-hollis.pdf>.

[30] James J.F. Forest, *Homeland Security: Protecting America's Targets, Vol. III: Critical Infrastructure* (Westport, CT: Greenwood Publishing Group, 2006), 136.

[31] Giles Tremlett, "This Is London—The Capital of Somali Pirates' Secret Intelligence Operation," *The Guardian*, May 11, 2009, available at <www.guardian.co.uk/world/2009/may/11/somalia-pirates-network>.

[32] National Petroleum Council, *Securing Oil and Natural Gas Infrastructures in the New Economy* (Washington, DC: Department of Energy, June 2001).

[33] U.S. Naval Institute and CACI International, Inc., "Cyber Threats to National Security: Symposium I—Countering Challenges to the Global Supply Chain," March 2, 2010, available at <http://asymmetricthreat.net/docs/asymmetric_threat_4_paper.pdf>.

[34] Allegro Energy Group, "How Pipelines Make the Oil Market Work: Their Networks, Operation and Regulation," a memorandum for the Association of Oil Pipelines and American Petroleum Institute's Pipeline Committee, December 1, 2001, 7.

[35] "Ice Storm Trips Power, Paralyzes Key U.S. Oil Hub," Reuters, December 11, 2007, available at <www.cnbc.com/id/22200736/Ice_Storm_Trips_Power_Paralyzes_Key_US_Oil_Hub>.

[36] Eric J. Byres, "Cyber Security and the Pipeline Control System," *Pipeline & Gas Journal* 236, no. 2 (February 2009), available at <http://pipelineandgasjournal.com/cyber-security-and-pipeline-control-system>.

[37] U.S. Cyber Consequences Unit (US-CCU), special report, *Overview by the US-CCU of the Cyber Campaign Against Georgia in August of 2008*, available at <www.registan.net/wp-content/uploads/2009/08/US-CCU-Georgia-Cyber-Campaign-Overview.pdf>.

[38] Energy Information Agency, *World Oil Transit Chokepoints* (January 1, 2008), 1, available at <www.eia.gov/cabs/world_oil_transit_chokepoints/Full.html>.

[39] Austin Bay, "Grab the Planet By the Throat," *RealClearPolitics* (April 22, 2009), 8, available at <www.realclearpolitics.com/articles/2009/04/22/grab_the_planet_by_the_throat_96106.html>.

[40] Energy Information Agency, 4.

[41] Referring to Iraq, Afghanistan, and Libya.

[42] Holger Stark, "Mossad's Miracle Weapon: Stuxnet Virus Opens New Era of Cyber War," *Der Spiegel Online*, August 8, 2011, available at <www.spiegel.de/international/world/0,1518,778912-2,00.html>.

[43] Laurent Murawiec, "China's Grand Strategy Is to Make War While Avoiding a Battle," *Armed Forces Journal* 143 (November 2005), available at <www.armedforcesjournal.com/2005/11/1164221/>.

[44] Most commonly translated as "Assassin's Mace," it refers to the Chinese search for weapons that are undetectable prior to use and cause such damage as to make retaliation by the victim impossible.

[45] Jason E. Bruzdzinski, "Demystifying Shashoujian," in *Civil-Military Change in China: Elites, Institutes, and Ideas after the 16th Party Congress*, ed. Larry Wortzel and Andrew Scobell (Carlisle, PA: U.S. Army War College, Strategic Studies Institute, 2004), available at <www.mitre.org/work/best_papers/04/bruzdzinski_demystify/bruzdzinski_demystify.pdf>.

[46] Richard Stiennon, "A Brief History of Chinese Cyberspying," *Forbes.com*, February 2, 2011, available at <www.forbes.com/sites/firewall/2011/02/11/a-brief-history-of-chinese-cyberspying/>.

[47] Qiao Liang and Wang Xiangsui, *Unrestricted Warfare: China's Master Plan to Destroy America* (Beijing: PLA Literature and Arts Publishing House, February 1999), 20.

[48] Ibid., 190.

[49] Unless the attack affected only the domestic U.S. petroleum distribution network.

[50] Nations that export oil or have little stake in the international system (Iran, Venezuela, Russia, and North Korea) could execute campaigns against all links of the supply chain with little self-damage; indeed, the resulting petroleum market instability might be economically advantageous to these actors.

Offensive Cyber *for the* Joint Force Commander

NASA Defense Meteorological Satellite Program

It's Not That Different

By ROSEMARY M. CARTER, BRENT FEICK, *and* ROY C. UNDERSANDER

Satellite view of power distribution

The instruments of battle are valuable only if one knows how to use them.

—Charles Ardant du Picq[1]

In 2008, as part of the campaign against the Republic of Georgia, Russia conducted a series of widely publicized cyber attacks. The attacks were not against purely military target sets. For 19 days, cyber warriors conducted distributed denial-of-service attacks against Georgia's Internet infrastructure and defaced public and private Web sites.[2] The initial impact was a virtual cyber-blockade against the government of Georgia that reduced the country's ability to lead internally and stifled its ability to gain international sympathy. A second-order effect was that the National Bank of Georgia shut down its Internet connections for 10 days, stopping all electronic financial transactions. The strike is one of the first publicized employments of offensive cyber as an integrated part of a military operation and demonstrates the powerful impact of these types of attacks on private sector business.[3]

The cyber domain consists of four operating areas: providing capability, protecting that capacity, exploiting within the domain, and conducting offensive operations that are also referred to as computer network attack. The areas of "provide" and "protect" are the most mature because our day-to-day information technology operations require a secure and functioning cyber domain. This article focuses instead on *offensive cyber capability*, which is the newest segment of the domain but is rapidly maturing. Unlike airpower, where development was limited to nations with significant industrial and financial resources, the cyber warfare arena is inexpensive and characterized by state and nonstate actors limited only by creativity and the Internet. Therefore, to maintain strategic capability for cyber superiority,[4] the cyber domain must be rapidly synchronized with the other warfighting domains. A full understanding of the features, capabilities, limitations, and impacts of the cyber domain may be years away, but actionable knowledge of this domain at the operational level will not be achieved as long as cyber operations remain segregated from the other warfare mission areas.

The assertion that cyber operations are different is the most common argument for

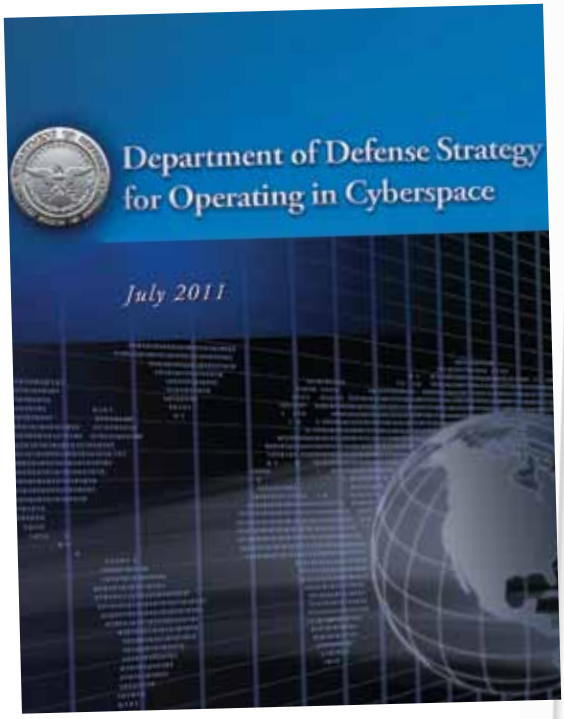
Colonel Rosemary M. Carter, USA, is a Communications Officer on the Army Staff. Colonel Brent Feick, USAF, is a Senior Policy Advisor for the Office of the Deputy Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs, Integration, and Defense Support of Civil Authorities. Captain Roy C. Undersander, USN, is the Executive Officer of Naval Air Station Jacksonville, Florida. The authors collaborated on this article while attending the Joint and Combined Warfighting School at the Joint Forces Staff College.

segregating cyber from the other domains. Cyber is different just as the solid terrain of the land domain differs from the physical structures of air and space domains. Speed of action is also different in cyber. Events occur and situations develop faster than the human mind can observe, orient, decide, and act.[5] But this is not the first time in the history of warfare that the speed of conflict has changed. The introduction of fighter aircraft and space capabilities changed the military decision calculus, yet these capabilities were not in themselves sufficient justification to segregate the domain. In fact, initial efforts to isolate space from the other domains were overcome as our understanding of the domain matured. The purpose of this article is to analyze the challenges of cyber policy, targeting, and the planning process to argue that offensive cyber is not so different from other capabilities, and that it must be fully integrated at the joint force command level to ensure unity of effort and maximize effectiveness.

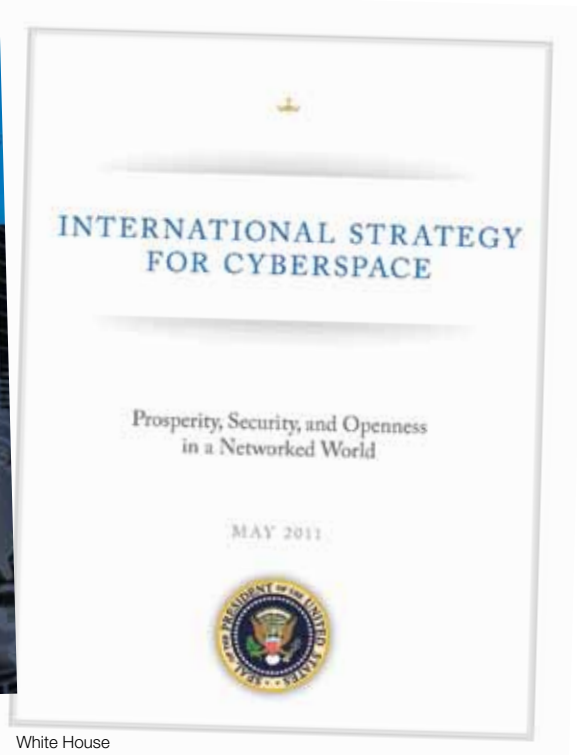
The Need for Rules

U.S. policy, authorities, and doctrine for military operations in the cyber domain are not mature. The *International Strategy for Cyberspace*[6] (May 2011) and the *Department of Defense* (DOD) *Strategy for Operating in Cyberspace*[7] (July 2011) are a start, but both documents focus almost entirely on cyber defense. While this is an important aspect, it leaves the Armed Forces in a state of flux with regard to integrating offensive capability. As is to be expected, conduct of cyber attacks is a sensitive issue. International organizations such as North Atlantic Treaty Organization (NATO) Watch advocate for a ban on offensive cyber operations altogether because the domain is so pervasive that offensive operations could quickly escalate beyond the intended virtual boundaries with devastating global impact.[8] Cyber activity is also being addressed through international anticrime channels,[9] but care must be given to provide separate and distinct definitions for acts of crime as opposed to acts of war. Without international rules, some countries have started to set precedent by their actions, demonstrating ethics that differ from ours. Standards of conduct for cyber warfare similar to those for other aspects of war are required. The United States should draft a declaratory policy that establishes lines we do not intend to cross in the cyber domain and that we expect an adversary to adhere to as well.

The U.S. Code is another source of guidance for DOD. The authorities of Title 10, The Armed Forces, and Title 50, War and National Defense, were established prior to the existence of the concept of cyberspace, so translating them to the cyber domain is extremely complex and not yet fully deconflicted. For example, under Title 10, a joint force commander is authorized to collect intelligence on an adversary for operational preparation of the environment (OPE). In the cyber domain, this task becomes mired in law because the same capability used to exploit is also used to attack, and there is no way to demonstrate intent within the effects of the task.[10] Because of the legal concerns, collection to date is done under Title 50 authorities, which severely limit military capacity and compel a centralized approach to these types of intelligence. If Service cyber components were allowed to conduct OPE on behalf of the joint force command for targeting, offensive cyber options could be much more integrated and timely. As it is, joint force planning staffs routinely lose national-level support due to higher priority tasking from the National Intelligence Priority Framework. Agencies supporting national tasking are highly skilled but have limited resources; hence, they do not have excess capacity to meet DOD requirements. Section 954 of the National Defense Authorization Act for Fiscal Year 2012[11] starts to address DOD authorities for offensive cyber operations, but it is vague enough that debates over Titles 10 and 50 will still occur. Its lack of clarity indicates that the thinking of policymakers and lawmakers is still too traditional for this newest domain.



DOD



White House

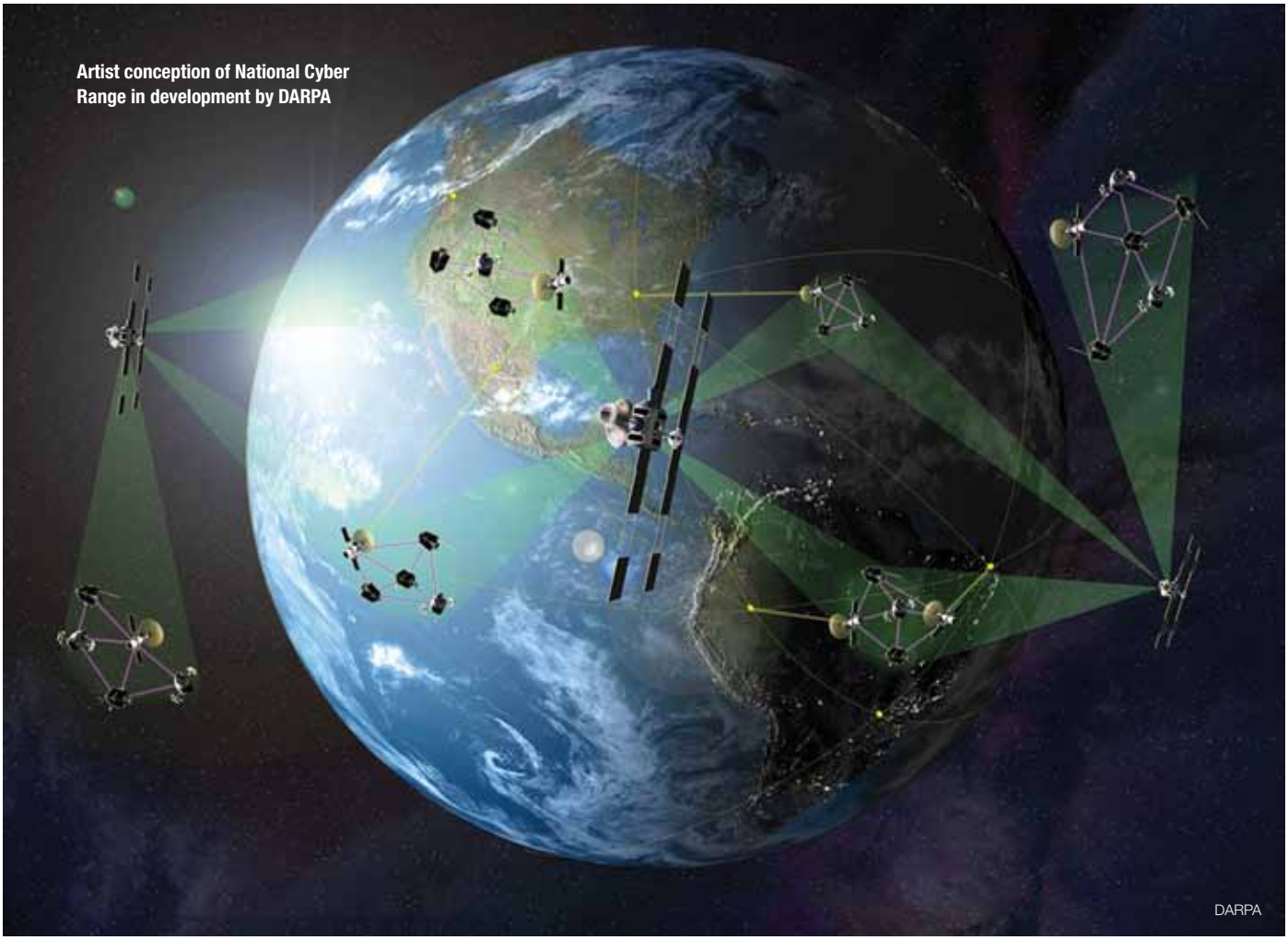
General Keith Alexander, USA, commander of U.S. Cyber Command (USCYBERCOM) and director of the National Security Agency (NSA), announced in October 2011 that DOD is currently staffing rules of engagement for the cyber domain from which his command will provide guidance to the DOD cyber force.[12] These rules of engagement are an important step, but they are not sufficient without training and rehearsals to validate and inculcate them into operational ethos.

Per DOD Directive 5100.01, the Services and combatant commands have authority to man, train, and equip cyberspace forces to enable joint force commanders to perform decisive operations.[13] Tactics, techniques, and procedures for computer network attack are maturing. What are needed now are plans to inform defense leadership and other policymakers how these capabilities integrate to achieve military and national endstates. Planning will drive understanding of current authorities and help inform recommended changes prior to a military crisis.

The Targeting Process

Military operations require effective targeting to identify objects or entities for engagement or action. To be effective, these targets must be linked to the commander's intent. In accordance with Joint Publication 3-60, *Joint Targeting*, the principles for joint targeting are focused, effects-based, interdisciplinary, and systematic.[14] The joint targeting process is cyclic and relies on target system analysis and assessments to establish functional relationships among the adversary's political, military, economic, social, informational, and infrastructural systems. The process includes both target system elements and target system components to be inclusive of all elements of the adversary's power. It is dependent on staff judge advocates to ensure that targets are in compliance with the laws of armed conflict and the rules of engagement. The targeting process is an essential component of mass and unity of effort, bringing integrated capabilities to bear during all phases of operations—shaping, deterring, seizing the initiative, dominating, stabilizing, and enabling civilian authorities.

The targeting process is as critical for the cyber domain as it is for the domains of land, sea, air, and space because we expect our adversaries to have as complex a military cyber capability as our own integrated with civilian networks. Additionally, other targets, to include manufacturing plants, logistics systems, and power generation facilities, are dependent on the cyber domain to function properly and effectively.[15] The characteristics and sophisticated intricacies of cyber make it tempting to isolate cyber targeting from the larger effort. There are some compelling arguments for this approach. First, the domain requires specialists, some of whom will never wear the uniforms of our Armed Forces. There are few cyber specialists, so the vision of a consolidated cohort of cyber targeteers ready to converge on a designated



Artist conception of National Cyber Range in development by DARPA

threat is appealing. Consolidating resources also facilitates centralized training, which is attractive in a resource-constrained environment. Finally, the shared connectivity between adversary and civilian or commercial cyber space argues for keeping cyber targeting inside of a compartmented community with a small number of personnel knowledgeable on the efforts. However, none of these arguments is sufficient to overcome the risks associated with lack of integrated targeting at the operational level. This integration is fundamental and cannot be achieved during the execution phase.

The commander and his staff must fully understand both the friendly and adversary cyber domains to the same degree they understand the other domains. As with any limited resource, the global force management system should prioritize and allocate the cyber force based on priorities and risk. Training for specialized forces will always be a challenge. However, training difficulties should not drive operational capabilities. Leaders should demand flexibility and creativity from the force providers in their training programs, not from a warfighting commander with limited access to the domain until operations are imminent. Efforts now to decentralize and optimize cyber training will also reap benefits for the operational force by establishing virtual environments that can test training, exercises, scenarios, and contingency plans.

Risk is associated with the negative second- and third-order effects of targeting an adversary's cyber space with civilian and commercial cyber activities operating in the same space. This risk is the strongest argument for integrating cyber targeting within the commander's larger targeting effort. The Georgia case study provides an example of these risks. Whether or not the cyber attackers intended for the Georgian National Bank to cease electronic transactions, the impact was the same. Unintended consequences of a limited cyber attack may impact the financial instrument of power in waves of effects generated by actual damage, perceived damages, or, as in Georgia, loss of confidence. Commanders must understand the most dangerous and most likely effects of cyber operations within their areas of responsibility. These effects must synchronize with the entire operation to protect friendly forces and the civilian population.

Joint force commanders must integrate information from the cyber domain into their joint targeting process to synchronize capabilities. This should be a two-way street, benefiting other warfare operators and, just as important for cyber operators, opening avenues of approach in other domains that otherwise would be closed in the cyber domain. While cyber information can fit into the targeting process, there are some manual manipulations that need to take place until the targeting community catches up with new policies and the supporting technology.

First, the military targeting process is geographically focused to the point that the Modernized Integrated Database, a database for all military targeting, only references targets by geographic position. This poses problems for a cyber operator who may have a virtual network as a target. The Intelligence Community is aware of this shortfall and working to make the database more flexible. Second, access to signals intelligence (SIGINT) data is too constrained. Joint planners must have access to these reports in a timely manner if they are to have a full understanding of the operational environment. SIGINT data should be pushed from NSA, not pulled. Once targets are identified, raw SIGINT may even need to be shared in order to maintain a target on the joint target list.

our country is currently more willing to drop a bomb on an adversary than break his computer

Finally, a tiered approach to identifying targets in the cyber domain must be adopted. There is an authorities question nested in this as well, but a joint force commander, with the help of all-source intelligence and a military cyber component, may produce Internet-facing targets to hold at risk. These are targets that are accessible directly from the Internet (as opposed to a closed network) and would constitute the first tier. OPE on tier one targets would not involve national intelligence assets, but would help refine questions that can focus national assets on the harder problems for the military, and thus would be the second tier. Many agencies are skeptical of the utility of Internet-facing targets, but the Georgia attack, where the known cyber targets were Internet-facing, is an example of their utility. The target list was even posted on the Internet. This discussion demonstrates that there are some differences in dealing with cyber targeting information, but in general it fits into the Joint Publication 3-60 construct.

It is incumbent upon USCYBERCOM to enable joint force staffs to fully contribute in this environment and understand the positive and negative effects of cyber operations on friendly forces, on the adversary, and on noncombatants in their area of responsibility during all aspects of targeting.

Operational Planning

Larger than the targeting process is overall planning for an operation. Today, a limited understanding of the cyber domain artificially constrains military planners. Many planners perceive that DOD does not have authority to do offensive operations in the cyber domain. However, the real issue is that the authorities are not understood or delegated down. Joint force commanders need to develop integrated plans with offensive cyber operations to help shape policy and build a norm of authorities and rules of engagement for military cyber attack, but their planners do not know the domain well enough to develop these plans. The discussion becomes circular. Civilian policymakers want to know exactly what DOD intends to do and commanders perceive that they cannot do anything because they do not have the authority.

With this, the value of the J5 Planning Directorate and deliberate plans come into play. The more fidelity joint force commanders can put into offensive cyber planning, the easier it will be to articulate potential new authorities with sufficient time to integrate them into the plan. Often, intelligence agencies will not be supportive of specific targets, citing a concern over loss of intelligence. However, this is a moot point at the planning stage, and planners should not let this, or the lack of authorities, defer their planning if the target will help meet an objective. It is better to have a plan available in times of crisis from which to have the intelligence gain/loss and legal discussions than to be caught with no options when the government is prepared to take action.

Unique features of the cyber domain have encumbered deliberate cyber planning in the past. The following generic scenario demonstrates the methodology and the unique features. A planner determines that Effect A can be met either by dropping a joint

direct attack munition on Target 1, a building, or by conducting a cyber attack on Target 2, a router. In both cases, the planner uses intelligence to link the target to the effect, determine access, pick the appropriate capability, and maintain the target in the joint target list. However, it typically takes much more intelligence preparation to develop Target 2 because our culture is so focused on geographic targets that it takes an extra level of intellectual energy to broaden the aperture. If the planner can obtain imagery of Target 1, then it is simply easier for a weaponeer to plan for a kinetic solution and hold that target at risk.

In determining access, we see the second difference. Access to Target 1 may constitute a bomber flying through or avoiding a surface-to-air missile threat. This is a well-understood problem and is addressed by the tactical force. In the case of Target 2, access must be established through the cyber domain by cyber operators, who are limited. To do this, the command requires cyber OPE or exploitation authorities as discussed. This is often where targeting in the cyber domain stops due to limited NSA resources and competition with national priorities. If Service cyber components were conducting cyber preparation of the environment under Title 10 at the joint force commander's direction, many of these issues would be resolved. As it is, these differences add up to a longer timeline to develop the target.

The third difference is the capability itself. The United States has a finite number of types of kinetic weapons to attack physical targets. Using the right combination and number of weapons, and based on experience, it is easy to quantify the level of damage that these weapons inflict, which aids in the decisionmaking process. By contrast, cyber weapons are customized for each target, which makes it difficult for decisionmakers to use experience to visualize the mode of attack and its effects. Many cyber weapons are also based on specific software versions, so if the version changes, the weapon may no longer be effective.

The fourth and most significant difference is maintaining the target, the process in which the intelligence and planning teams routinely review the intelligence and endstates to ensure that the target still meets the desired effects and nothing has changed that requires new weaponeering. This is a common task for any target on the joint target list; the difference is the volatility of the cyber target. In the case of Target 1, a planner may go 1 or 2 years between conducting maintenance. The structure of the building rarely changes and it will not move. However, Target 2 may receive a software upgrade 3 months after identification that makes the weapon developed for it obsolete. As a result, if the planner is serious about holding this target at risk, the maintenance cycle must speed up significantly.

In a *Joint Force Quarterly* article, Major General Brett Williams, USAF, stated that "our understanding of nonkinetic effects in cyberspace is immature."[16] This is a fair statement and frankly one of the biggest barriers for decisionmakers who grew up waging kinetic war. Our country is currently more willing to drop a bomb on an adversary than break his computer, which stems from two issues. First, as discussed earlier, the Nation is concerned about escalation without set standards. Second, decisionmakers are not likely to experiment with a cyber attack when lives are on the line and collateral damage is not well known. Until DOD makes the cyber attack option as tangible for a decisionmaker as dropping munitions, and can prove it will meet or exceed the effect of a kinetic option without catastrophic collateral effects, the decisionmaker will choose the kinetic option every time. To remedy this, planners must develop high-fidelity cyber attack options that are part of an integrated solution and can be tested on ranges prior to execution. This will allow the cyber community to establish a historical database to provide the confidence and statistical data required for decisionmakers to choose the nonkinetic options.

To summarize deliberate planning, the primary reason that some organizations push back on cyber planning to this level of detail is the increased level of effort to develop the target and the volatility of the target. However, if joint force commanders want to normalize cyber attack and have a reasonable expectation of successfully executing it as a part of combined fires, deliberate planning is a must. Likewise, cyber operators need to embrace this concept as well lest they become irrelevant, especially when effects cannot be brought to bear where and when they are needed for the commander.[17]

Finally, if a computer network attack is not planned for standalone delivery, the capabilities must be synchronized with the other capabilities brought to bear by the joint force commander. U.S. Strategic Command (USSTRATCOM) is responsible for or is assigned many of the nonkinetic capabilities in DOD, and its planners must work alongside joint force planners to provide the commander the most successful attack options and courses of action. This effort must include USCYBERCOM, a subunified command under USSTRATCOM that is assigned DOD cyber forces. During the integration process, joint force planners must develop an appreciation for the synergies between USCYBERCOM and the other components of USSTRATCOM. Additionally, because cyber attacks may have global implications as well as the intended regional effects, it is imperative that these options also be vetted collectively through the DOD and interagency communities. This is a coordinating task that must be completed by U.S. Strategic Command. USSTRATCOM's Joint Functional Component Command–Global Strike started a model for this, but it is immature and requires refinement and expansion. As military professionals, we have recognized the need to work closely with interagency partners to fully achieve desired endstates and ultimately the national strategy. Cyber warfare is no different and may be one of the most compelling reasons for interagency cooperation because agencies outside of DOD have authorities in the cyber domain and may have interest or even cyber attack options developed for a particular target. These tasks must be normalized into the joint interagency coordination group process to become a force multiplier for DOD.

with new fiscal constraints on the horizon, our ability to make the best use of cyber capabilities is even more important

Recommendations

This article makes the case for integrating offensive cyber at the joint force command level. The list of recommendations below is designed to generate the discussion necessary to fully develop these details. Lead agencies identified are based on the authors' understanding of current roles and responsibilities.

1. DOD must delegate proper authorities to USCYBERCOM and its components to shorten the development time of targets,

streamline cyber operational preparation of the environment, and increase throughput of the Intelligence Community.

2. USSTRATCOM/USCYBERCOM must ensure that organizational and information-sharing policies are optimized to support and include joint force planners. This includes devising methods to share raw SIGINT for timely maintenance of targets on a joint target list.

3. The Intelligence Community must update applications and procedures associated with the Modernized Integrated Database to accommodate nongeographic targets.

4. Joint force planners must incorporate high-fidelity offensive cyber plans into their deliberate plans. USCYBERCOM must facilitate this in order to train, educate, and empower joint planners. The objective is to have planners with knowledge of cyber capabilities, limitations, and basic concepts for employment.

5. DOD must establish policy that allows joint force planners to take advantage of nontraditional cyber information sources. Commercial companies are assessing many of the same problems and could be leveraged to provide critical information.

6. DOD must resource joint force commands to test offensive cyber attacks on virtual cyber ranges. The targeting community should use the test results to develop the cyber equivalent to the kinetic Joint Munitions Effects Manual, which provides a probability of damage based on target/weapon pairing.

7. DOD, in conjunction with the U.S. Government, must develop a declaratory policy for cyber warfare. It is time for the United States to lead an international dialogue on cyber warfare, perhaps modeled on the Council of Europe Convention on Cybercrime in 2001.

8. USSTRATCOM must devise a method to track nonkinetic options for global impact and incorporate these nonkinetic attack options and associated targets into the synchronizing efforts of the joint force commander's plan.

9. USCYBERCOM must standardize the interface between joint force planners and interagency partners for targeting. This may be a logical function for the Joint Inter-Agency Coordination Group, but a separate technical interagency team may be warranted. The team should be responsive to the joint force commander.

All future U.S. military operations will include the cyber domain. Cyber is where we coordinate joint functions and control weapons systems. We must operate securely across the cyber domain and commanders must protect it. Of equal importance is our ability to operate offensively within this domain to ensure dominance, restrict the offensive cyber capabilities of the adversary, and leverage cyber as a force multiplier. With new fiscal constraints on the horizon, our ability to adapt and make the best use of these cyber capabilities is even more important. Offensive cyber operations must be integrated into the joint force commander's plan, and his planning and executing staffs must understand the desired effects. As cyber domain doctrine matures, there is an opportunity to correct current deficiencies in an integrated approach through deliberate planning and the targeting cycle. This will inform U.S. policymakers and allow for new language in key policies, laws, and treaties. The United States must act quickly because the clock is ticking and the adversary is learning. Offensive cyber—it's not that different. **JFQ**

NOTES

[1] Charles Ardant du Picq, *Battle Studies: Ancient and Modern Battle*, 8th ed. (French), trans. John Greely and Robert C. Cotton (New York: Macmillan, 1920).

[2] Eneken Tikk et al., *Cyber Attacks Against Georgia: Legal Lessons Identified* (Tallin, Estonia: Cooperative Cyber Defence Centre of Excellence, November 2008), 4–5.

[3] Scott Borg and John Bumgardner, *Overview By the US-CCC of the Cyber Campaign Against Georgia in August of 2008*, A US-CCC Cyber Special Report, August 2009, available at <www.registan.net/wp-content/uploads/2009/08/US-CCU-Georgia-Cyber-Campaign-Overview.pdf>.

[4] Cyber superiority is comparable to air superiority, which is defined in Joint Publication 1-02, *Dictionary of Military and Associated Terms* (Washington, DC: The Joint Staff, as amended through November 15, 2011), as "that degree of dominance in the air battle of one force over another which permits the conduct of operations by the former and its related land, sea and air forces at a given time and place without prohibitive interference by the opposing force" (16). In the cyber domain, superiority provides the degree of dominance in cyber that permits the conduct of operations by land, sea, air, and cyber forces without prohibitive cyber interference.

[5] Colonel John Boyd, USAF, "Destruction and Creation," September 3, 1976. Boyd's concept of the OODA loop (observe, orient, decide, act) was developed and presented through a series of briefings and lectures. His paper, "Destruction and Creation," provides scientific justification for decisionmaking without describing the OODA process in detail. Several books on the life of Boyd provide additional detail on the concept and a five-slide set titled "The Essence of Winning and Losing" dated June 28, 1995, that defines the OODA loop is attributed to Boyd.

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

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

[8] Ian Davis, NATO Watch, "Ban on offensive cyber operations needed," available at <www.natowatch.org/node/463>.

[9] Convention on Cyber Crime, ETS 185, Council of Europe, November 23, 2001, available at <http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CL=ENG>.

[10] Robert Chesney, "Military-Intelligence Convergence and the Law of the Title 10/Title 50 Debate," *Journal of National Security Law and Policy*, October 17, 2011; and University of Texas Law School, Public Law Research Paper, available at Social Science Research Network, available at <http://ssrn.com/abstract=1945392>.

[11] The National Defense Authorization Act for Fiscal Year 2012 was signed by President Obama on December 31, 2011. The bill is available at <http://armedservices.house.gov/index.cfm/ndaa-home>.

[12] Donna Miles, "Doctrine to Establish Rules of Engagement Against Cyber Attack," American Forces Press Service, October 20, 2011, available at <www.defense.gov/news/newsarticle.aspx?id=65739>.

[13] Department of Defense (DOD) Directive 5100.01, *Functions of the Department of Defense and Its Major Components* (Washington, DC: DOD, December 21, 2010).

[14] Joint Publication 3-60, *Joint Targeting* (Washington, DC: The Joint Staff, April 13, 2007), I-4.

[15] Benjamin Lambeth, "Airspace, Spacepower, and Cyberpower," *Joint Force Quarterly* 60 (1st Quarter 2011), 46–53.

[16] Brett Williams, "Ten Propositions regarding Cyberspace Operations," *Joint Force Quarterly* 61 (2nd Quarter 2011), 11–17.

[17] Eric Schmitt and Thom Shanker, "U.S. Debated Cyberwarfare in Attack Plan on Libya," *The New York Times*, October 7, 2011, available at <www.nytimes.com/2011/10/18/world/africa/cyber-warfare-against-libya-was-debated-by-us.html_r=1&emc=etal>.

BG Rhonda Cornum, USA, speaks at first Master Resilience Training course, Fort Meade, Maryland

U.S. Army (C. Todd Lopez)

Resilience

The Result of a Totally Fit Force

By RHONDA CORNUM, THOMAS D. VAIL, *and* PAUL B. LESTER

As the Nation's war against terror has unfolded over the last decade, each Service has shown evidence of higher levels of stress. Increased operational tempo has been a ubiquitous part of military service thus far in the 21st century. Repeated deployments have required junior Servicemembers to represent the Nation's interests with foreign populations while performing dangerous tasks that extend beyond their training. This has contributed to "stress on the force." Personnel who have not deployed face different stressors, as do family members and civilians remaining in the United States. It is not surprising that all Services have experienced increased negative behavioral outcomes attributable to stress and poor coping. Active surveillance has documented increased rates of obesity; tobacco, drug, and alcohol abuse; family violence; sexual assaults and other felonies; psychological diagnoses; and suicide, especially among junior members of the force.

In response, the Department of Defense (DOD) and Department of Veterans Affairs have dramatically increased assets dedicated to helping Servicemembers who are experiencing negative behavioral health outcomes. These departments will continue this effort as long as there is a need. But as it became clear that the current war was a long-term struggle, DOD increasingly recognized that building and maintaining psychological strength is critical to maintaining the Nation's ability to wage sustained combat and contingency operations. While fully recognizing that treatment of personnel suffering physical and psychological injuries and disease is vital, DOD has also recognized it is at least as important to prevent injury and disease.

Brigadier General Rhonda Cornum, USA (Ret.), is the former Director of Comprehensive Soldier Fitness. Colonel Thomas D. Vail, USA (Ret.), is the former Deputy Director of Comprehensive Soldier Fitness. Major Paul B. Lester, USA, is the former Director of Research, Development, and Program Evaluation for Comprehensive Soldier Fitness.

Use of body armor, malarial prophylaxis, and immunizations are all accepted measures to prevent physical illness and injury. Daily physical training (PT) has long been accepted as important to building physical assets including speed, endurance, strength, and flexibility. These physical assets allow better performance on the battlefield. But only in the past few years has DOD recognized that enhancing baseline psychological strength and fitness could improve performance on the battlefield as well, and that it thus might reduce the incidence of negative psychological and behavioral outcomes.

There has been a fortunate collision between the *need* to increase the psychological strength of the force with the *science* allowing that to occur. A significant amount of research has been completed in the past two decades that outlines how to enhance the psychological fitness of a healthy population—that is, personnel without any diagnosis or symptom complex. The discipline of *positive psychology*, defined as "scientific study of the strengths and virtues that enable individuals and communities to thrive," became recognized as a legitimate degree-producing branch of psychology in 2004. This is quite different from traditional clinical psychology, much of which focuses on abnormal behavior and mental illness. At least for the military, whether the issue is physical or psychological health, a mere absence of disease or infirmity is a necessary but insufficient condition; success, as we see it, is making sure that everyone has the education, training, and opportunity to develop and maintain *optimum* health.

In 2009, former Chairman of the Joint Chiefs of Staff Admiral Mike Mullen tasked the Uniformed Services University and Samueli Institute to develop a framework for a more holistic view of "fitness." The concept of Total Force Fitness (TFF, pronounced *tough*)[1] is the result of this work, as shown in figure 1. On September 1, 2011, Admiral Mullen signed Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 3405.01, "Chairman's Total Force Fitness Framework," requiring each Service to use the TFF framework to enhance and/or refine its current fitness program. This instruction tasks each Service to provide appropriate medical support, training, equipment, and supplies for implementing the Chairman's policy, allowing the uniformed Services complete flexibility on how these measures are accomplished.

This instruction was not written in a vacuum. Over the same time period, the Services had individually recognized the same need. They were at various stages of designing or implementing fitness plans when the letter of instruction was published. The Army had devoted much of 2008 and 2009 to designing a strategy to improve the psychological fitness of the entire Service. Designated Comprehensive Soldier Fitness (CSF), this strategy was not directed at individuals with behavioral health problems. Rather, the CSF mission was to improve the baseline psychological strength of the force by synchronously developing and deploying psychological skills training and education along three lines of effort: institutional, leader-led, and individual. Simultaneously, CSF was to develop and implement an assessment tool to give individual Soldiers a confidential azimuth check on their own psychological fitness. Moreover, the Army leadership, after removing individual Soldier identification, could use the aggregate results longitudinally to determine the effect of education, training, deployments, and other policy decisions on the psychological health of the force. Army-wide deployment of CSF was launched October 1, 2009.

Figure 1. The Shield of Health: Eight Domains of Fitness

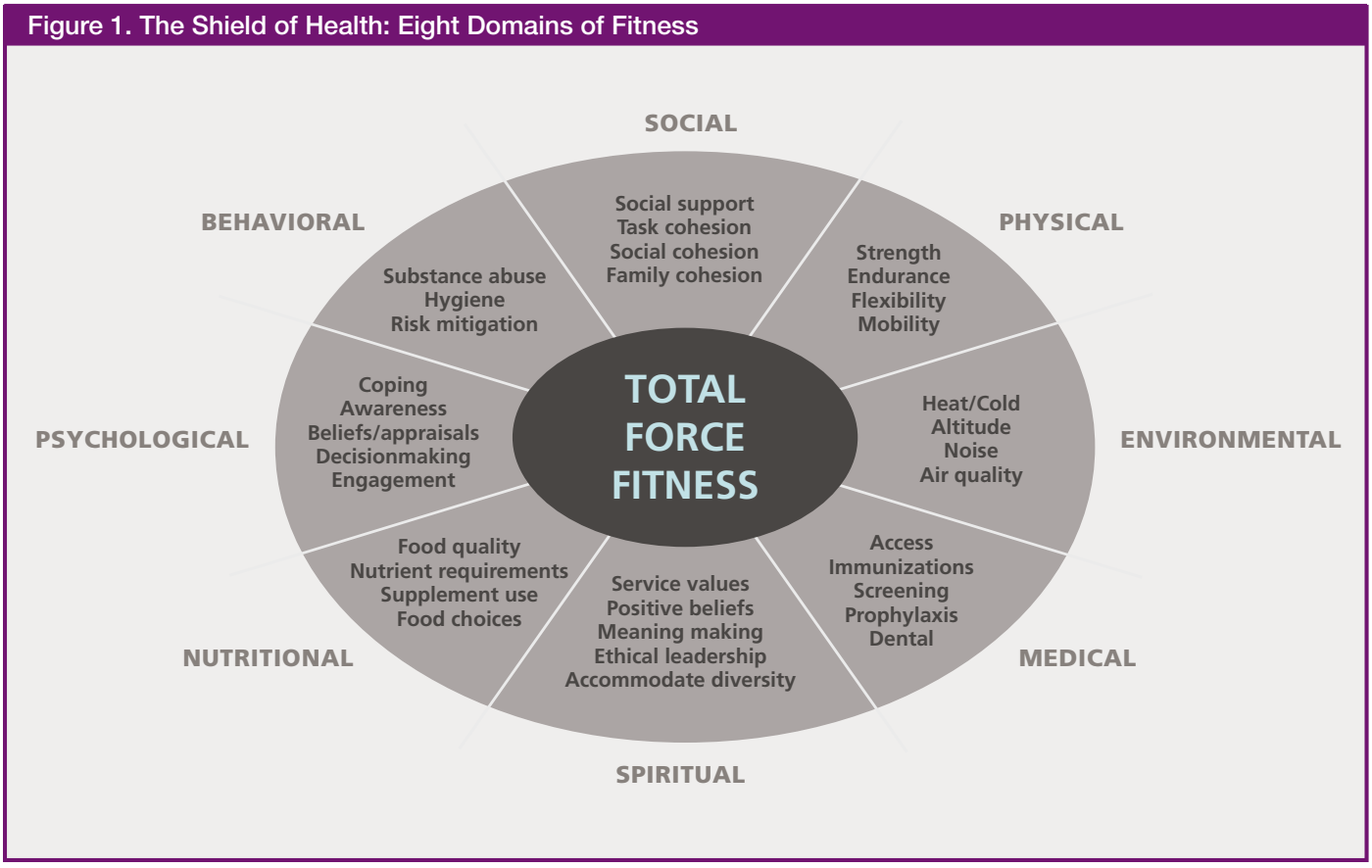
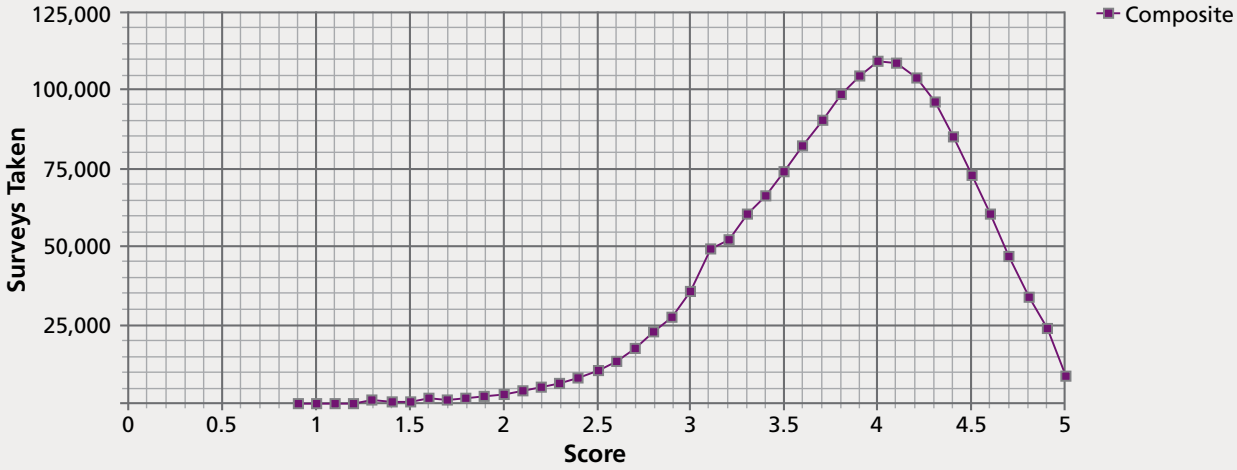


Figure 2. Actual Distribution of Global Assessment Tool Scores for Army Population



Development of the assessment tool, content of the material to be taught, and the method of delivery was informed by many of the leading psychological experts in the Nation. A special issue of *American Psychologist* in January 2011 was devoted to the science behind the development of the entire CSF initiative.[2] The present article is in no way intended to repeat that scholarly work. Instead, it discusses the results after 2 years of CSF implementation, what has been learned about the fitness of Army personnel, and the effectiveness of education and training to enhance psychological fitness. Lastly, the potential for further application of psychological assessment and strength training in the Army and in the rest of DOD is discussed.

Major Components of CSF

First, a self-assessment devise known as the Global Assessment Tool (GAT) was developed and tested. Comprising 105 questions, it takes 15 minutes to complete. At this time, the GAT has been completed more than 2.1 million times by over 1.5 million users, and over 700,000 Soldiers have taken it more than once. The GAT measures psychological assets (rather than psychological symptoms or deficiencies) in four important domains: emotional, social, family, and spiritual. The results have an expected distribution; that is, few people score low, making it a fairly typical bell-shaped curve with the greatest number of those surveyed achieving about 75 percent of the maximum possible score (figure 2). We know that most Soldiers (86 percent) take it seriously (that is, no "left or right justified" response patterns). Furthermore, there are few differences across demographics (for example, rank, gender, and education). Additionally, GAT scores across the Army Components (Active, National Guard, and Reserve) are also similar. In short, there is a normal distribution of resilience and psychological health across the Army when the entire population is analyzed.

However, the distribution of scores changes when we look at special populations. Using data culled from a hypermassive database known as the Person-Event Data Environment (PDE), which connects data together from across DOD, we found that GAT results are strongly related to both positive and negative behavioral outcomes of interest to the military. For example, we learned that Soldiers who are caught using illicit drugs, committing violent crimes, or committing suicide are—not surprisingly—concentrated at the bottom of the psychological fitness curve.

Conversely, personnel selected for below-the-zone promotions, command sergeant major, and command are overrepresented in the upper 25 percent of psychological health. Moreover, we used the PDE to learn that attrition from basic training is 3 times higher for Soldiers who enter the Army in the bottom 10 percent of psychological fitness compared to the top 90 percent. We also found that Soldiers in the upper 90 percent of psychological health have approximately one-third the rate of post-traumatic stress disorder (PTSD) symptoms as Soldiers in the bottom 10 percent when they return from deployment. This clearly underscores the importance of entering combat with a strong baseline of psychological health; not doing so will have an effect on Soldiers when they return from deployment. When taken together, we now know the GAT is in fact measuring psychological assets that relate to success or failure in the military.

In parallel with releasing the GAT for Army-wide usage, CSF also launched the Master Resilience Trainer (MRT) course. This 10-day in-residence course gives first-line supervisors, primarily noncommissioned officers (NCOs), the opportunity to both learn and learn to teach proven resilient thinking skills that are validated by social scientists as being effective. The MRT course employs a train-the-trainer format. Here, our master resilience trainers learn the resilience skills and then fan back out across the Army to teach them to the Soldiers they lead. This train-the-trainer methodology is important for two reasons. First, a train-the-trainer format is cost-effective given that it does not add to the Army's total force structure (that is, the Army does not have to hire 5,000 new trainers). Second, this format embeds the training within the backbone of our Army—the NCO corps—the very leaders who understand Soldiers best and are responsible for training them.

Our MRTs learn 13 critical resilience skills. One of the first lessons taught is the "ATC" model. This model teaches that behavior is based on a sequence of events: there is an *A*ctivating event, which leads to a *T*hought, which then leads to *C*onsequences. Consequences can be emotions or behaviors,

which can be managed. This model, which is based on extensive experimental and clinical work, explains how two individuals can experience the exact same event but manifest different emotions and behaviors. Once they understand the sequence, people can learn to reframe how they think using more accurate assumptions and beliefs.

As a real world example, imagine a combat medic giving aid to a badly wounded Soldier, yet the Soldier ultimately dies. The activating event is the Soldier dying of wounds whose severity the medic had no control over. Yet if the medic's thought is "It's my fault he died—I don't know what I'm doing—I cost that guy his life," then the likely consequence of his thinking is guilt, shame, and perhaps, depression. The medic may then "self-medicate" with drugs or alcohol to assuage these negative emotions, leading to a downward spiral of thoughts with negative consequences. If, on the other hand, the medic thinks "I did everything I knew to do, and sometimes an injury is so severe I cannot save the guy," the consequence is likely to be sorrow, but not guilt or shame.

Moreover, while the short-term behavioral consequence of sorrow may be tears, the long-term consequence will be the understanding that he did his best and that he can continue to do "good" by getting back out and using his skills. The event itself was the same: there was a severely wounded patient, a medic rendered aid, and the patient died. But the consequences were different. Of course, this same scenario is played out at every level of care. But physicians, especially surgeons, typically spend a decade in training before they are faced with the absolute responsibility of a seriously wounded Soldier's life. Asking a 20-year-old medic within 2 years of graduating from high school to have the same level of objectivity and maturity as a 30-year-old surgeon is perhaps an unrealistic expectation—but it is an expectation that is inherent in combat. It is therefore our responsibility to teach these skills deliberately and preventively before Soldiers are faced with these challenges.

It is important to recognize that the value of competence with these skills is in no way unique to the military context; they apply equally whether the person is a secretary or a sniper, and whether the challenge is professional or personal. One colonel at Fort Bragg told us, "As a father with a 20-year-old son and 19-year-old stepson, I think the program would be valuable for all teenagers." In reality, the basis for the thinking skills taught by MRTs is the same as the basis of Cognitive Behavioral Therapy, a well-recognized technique for combating depression, anxiety, and PTSD. That basis is simple: it is "the idea that our *thoughts* cause our feelings and behaviors, not external things, like people, situations, and events."[3] The guiding principle at CSF is that the time to learn something new is not in the midst of a crisis. The Army now understands that the time to learn these skills is beforehand, and therefore Soldiers should learn and practice these "thinking skills" during their normal lives and while facing smaller challenges. It will then be easier to draw on them during a truly significant challenge. This is exactly in line with what Soldiers frequently say in combat: "The shooting started, and my training just kicked in." In the Army, we now recognize how important it is that Soldiers have *all* the training needed to be more successful both in combat and in life, not just the tactical and technical skills.

Certainly, many people learn these things without formal education. They learn from the examples of parents, grandparents, and experiences, and this is likely a significant factor in why we see a wide spectrum of resilience in our data. But regardless of

U.S. Army (Jason Fetterolf)

Soldiers perform four-count flutter kicks during physical training, Fort Bliss, Texas

U.S. Army (Kimberly K. Fritz)

Fort Lee senior chaplain teaches resiliency during new 9-week course using biblical principles

the level of competence with these skills on entry into the military, the training is nevertheless valuable. First, it allows Soldiers who already have skills to recognize when to use them and to capitalize on them, which reinforces their use. Second, Soldiers who already have the skills learn to teach them, resulting in a more successful team rather than just successful individuals. Third, this training gives everyone in the Army a common vocabulary with which to discuss emotionally significant issues and may help to destigmatize the entire concept of psychological health.

Some Lessons Learned on Implementation

How the program is implemented in the field is probably the most important matter to examine. We are all familiar with things that seemed to work well when a professional did them, but the results were quite different when we tried them at home. In most cases, the outcome is better when the task is performed by a professional. As Comprehensive Soldier Fitness rolled out across the Army, we had to accept that a suboptimal solution in some areas would have to be acceptable in the short term in order to get the training to those needing it most. For example, we recognized that Master Resilience Training would be taught by leaders who likely had little training in psychology. Therefore, it was vital to ensure that the training could work in the average operational unit without causing harm. Given that, we stood up a robust data analysis cell that provided CSF with evidence of the program's effectiveness. Constant data analysis allowed CSF to make minor program changes as required. Another challenge facing us was local training management. Initially, as MRTs were trained and returned to their units, we recognized that many of them were not formally trained in how to properly plan, schedule, and implement a program such as CSF. Given that, CSF published clear training guidance that helped the MRTs implement the program within battalions and brigades.

Yet even from the beginning, pockets of light began to emerge. For example, in units where resilience training was instituted as a regular, habitual event that was on the training calendar and had proper command emphasis, commanders reported that Soldier behavior gradually improved. One unit at Ft. Leonard Wood required 2 hours of training per week and witnessed a marked reduction in Soldier attrition. The Eighth United States Army in Korea sent MRTs as a mobile training team to reach the entire force in small groups and showed a sharp drop in discipline issues. Elsewhere, one brigade commander went from 10 days of physical training every 2 weeks to 9, with 1 day devoted to the other "PT," which they refer to as psychological training. The staff at CSF collects these best practices and distributes both a printed and virtual implementation guide for unit leadership. Additionally, MRTs going through the course now spend more time on proper program implementation.

A vital commonality in units successfully implementing resilience training is that the training is led by recognized unit leaders. In parallel with this, we recommend that MRTs talk to their commanders and training planners as soon as they graduate to get the resilience course on the training calendar. But a second, equally important aspect of successful implementation is co-opting the first-line supervisor level of leadership because those leaders are our best way of diffusing the resilience lexicon. They are also likely the best suited leaders for describing to junior enlisted Soldiers how to make meaning of the training and incorporate the skills into daily life. That is usually done by first teaching the skills to the first sergeants and platoon sergeants of the unit, making "Resilience Teaching Assistants," or RTAs, out of the senior enlisted leadership of each small unit. These RTAs are helpful when the MRT is leading small group training because they serve as a bridge for the MRTs to Soldiers who are new to resilience training. These Soldiers then see that the leadership has a basic understanding of, and has bought into, resilience training. This helps to enhance the training experience during practical exercises and role-playing assignments.

Using Science to Evaluate the Program

At the same time the program was instituted across the Army, a parallel initiative of program evaluation was launched. The Army was committed to ensuring the program was effective and was prepared to modify it. One challenge was that CSF could not train enough MRTs fast enough to meet the Army's demand. While this was initially seen as a threat to the program, it became an opportunity to apply science to determine the program's effectiveness. Quite simply, the throughput constraints of the MRT course naturally created a wait list control group to be compared against units who had MRTs. By deliberately tracking where MRTs were assigned, and comparing the subsequent GAT scores of the brigades who had MRTs embedded in them with brigades that did not yet have them, the potential effect of the training on psychological health was measurable. Initially, the evaluation was planned to continue for 3 years, but it was ultimately shortened to 15 months. Subsequently, those brigades on the wait list were moved up in priority at the conclusion of the evaluation. We felt compelled to end the evaluation because, as commanders shared the value of having MRTs with other commanders who did not have them, demand for MRTs grew dramatically, and it became obvious that we needed to "surge" MRT production to get the trainers spread across the force more rapidly. To answer the demand, an aggressive mobile training team method was initiated.

For a variety of reasons, all data analyses were done by independent scientists who had no vested interest in seeing Comprehensive Soldier Fitness succeed, but this situation parallels a critical cultural norm within the Army—when it comes to training evaluations, units do not formally assess themselves. What can be said about the effect of having MRTs doing psychological fitness training in an operational environment? First, we can say that the skills taught by MRTs have a measurable positive effect on some of the most important characteristics of psychological fitness of the force. Units that conducted MRT skill training saw their resilience and psychological health scores—as measured by the GAT—improve significantly more than units that did not have MRTs. Specifically, units with MRTs witnessed improved Soldier-reported emotional fitness, coping characteristics, quality of friendships, and character strengths, while catastrophic thinking was significantly reduced.

When the analysis was confined to younger Soldiers (18–24 years old), the effects were three to four times larger than seen in older Soldiers, and improvements were seen in more areas measured by the GAT. Specifically, the younger cohort showed increased optimism, organizational trust, adaptability, family fitness, and family satisfaction in the units that had MRTs. This suggests that MRT skills accelerate the development and maintenance of psychological health in younger people and bring them closer in line with the psychological health of those who are older and more experienced. As previously noted, we also witnessed greater effects in units that regularly did the training, selected confident leaders to deliver it, and had command emphasis on MRT skill training. Because some of these brigades are still deployed, determining the effect on postdeployment and reintegration is still in the future. Nevertheless, it is noteworthy that using the scientific method allowed CSF to determine that the improvements were due to the MRT skill training and not to organizational factors such as quality of unit leadership and unit cohesion.

while the training modules and videos use actors in Army uniforms who use Army lexicon, those could easily be converted for use by other Services

Taking CSF Purple

Does Comprehensive Soldier Fitness nest within the CJCS instruction for developing Total Force Fitness? There are obvious links between the eight domains of fitness embraced by the CJCSI and the five dimensions of CSF. While the CSF program was developed by and for the Army, there is nothing Service specific about it. For example, the GAT only references "the Army" and "units" a few times, so it could easily be adapted to the other Services. While the training modules and videos use actors in Army uniforms who use Army lexicon, those could easily be converted for use by other Services. The coping, communication, and decisionmaking skills taught by MRTs are all equally applicable whether the individual is military or civilian, and without regard to Service affiliation. These are, after all, commonly needed life skills that help us all regardless of the uniform we each wear.

Additionally, CSF has already reached out to other Services and offered them training opportunities. For example, the Air Force's Air Combat Command has participated almost since CSF's inception, and to date CSF has trained 110 Air Force MRTs and 22 higher level training facilitators, and it has trained Navy and Marine Corps personnel as well. The GAT and resilience modules are offered free of charge and are available to anyone who is part of the Defense Enrollment Eligibility Reporting System regardless of Service affiliation.

Lastly, an opportunity exists within the fact that the Army is rapidly becoming self-sufficient in training resilience. Over the next few years, the CSF directorate will offramp much of the external support the Army needed to successfully stand up a force-wide resilience development program, and it will soon take full operational control of training MRTs. Army culture has steadily accepted the importance of resilience training, and the CSF lexicon is rapidly diffusing across Army units. Likewise, the Army is investing in other smaller programs endorsed by other Services, such as mindfulness training used by the Marine Corps, and this is also being done under the banner of CSF. Other training development continues in additional domains of psychological health. Accordingly, CSF was intentionally positioned to serve as a catalyst of change within the Army. Much has been learned, the sunk cost has largely been paid, and CSF is poised to transfer this knowledge to other Services if the desire exists.

Conclusions

Comprehensive Soldier Fitness is, as it was intended to be, a continuously evolving strategy. For example, an assessment of the individual's physical health is being added to the feedback everyone gets on the GAT this year. Taken together, a matrix of health indicators including percent body fat, PT test score, blood pressure, lipid profile, sleep and smoking habits, and the number of chronic

U.S. Air Force (D. Myles Cullen)

Soldiers review Master Resilience Trainer course curriculum at University of Pennsylvania

medications and diagnoses give a rough estimate of how physically healthy a person actually is. This "score" is then compared to how healthy the person could be if all the parameters were optimized. The person gets individualized feedback indicating what he or she can do to sustain the factors that are good and improve the factors that are not. Comprehensive Soldier Fitness is in the process of establishing online links between the individual factors comprising the physical domain and the real experts in each area in order to give each Soldier the best information to effect change.

Developing additional training for the future should be informed by what we see in the force today. Surveillance of the physical and psychological strengths and vulnerabilities within the entering cohorts is constantly being analyzed to determine which factors are associated with attrition, retention, and performance. When the psychological strengths and vulnerabilities of Soldiers who manifest a specific outcome (positive or negative) are compared with the rest of the force, the results should be used to inform where resources should be concentrated to best effect change in the desired direction. An example is our finding that social isolation and loneliness are two individual factors that were most divergent between Soldiers who subsequently functioned well and those who did not. Other factors such as organizational trust were identical between these two populations. When taken together, knowing this served as the impetus to fund research on training interventions aimed at building the skills to make and maintain healthy relationships, rather than how to enhance organizational trust. We describe this as data-driven decisionmaking, and the science supporting such decisionmaking should be used to help all of DOD to assist senior leaders in focusing resources where they are most needed.

As resources dwindle, greater reliance must be placed on using the behavioral sciences to determine resource allocations—to place a spotlight on where efficiencies exist and where the Services might get their greatest return on development. The joint force cannot afford to solve problems that do not exist or simply observe problems that do while taking no action; rather, it must focus on problems that really do exist and be willing to take action when it can. There are plenty of problems needing attention, and programs focused on preventive health strategies such as Comprehensive Soldier Fitness have demonstrated that such problems are actionable. **JFQ**

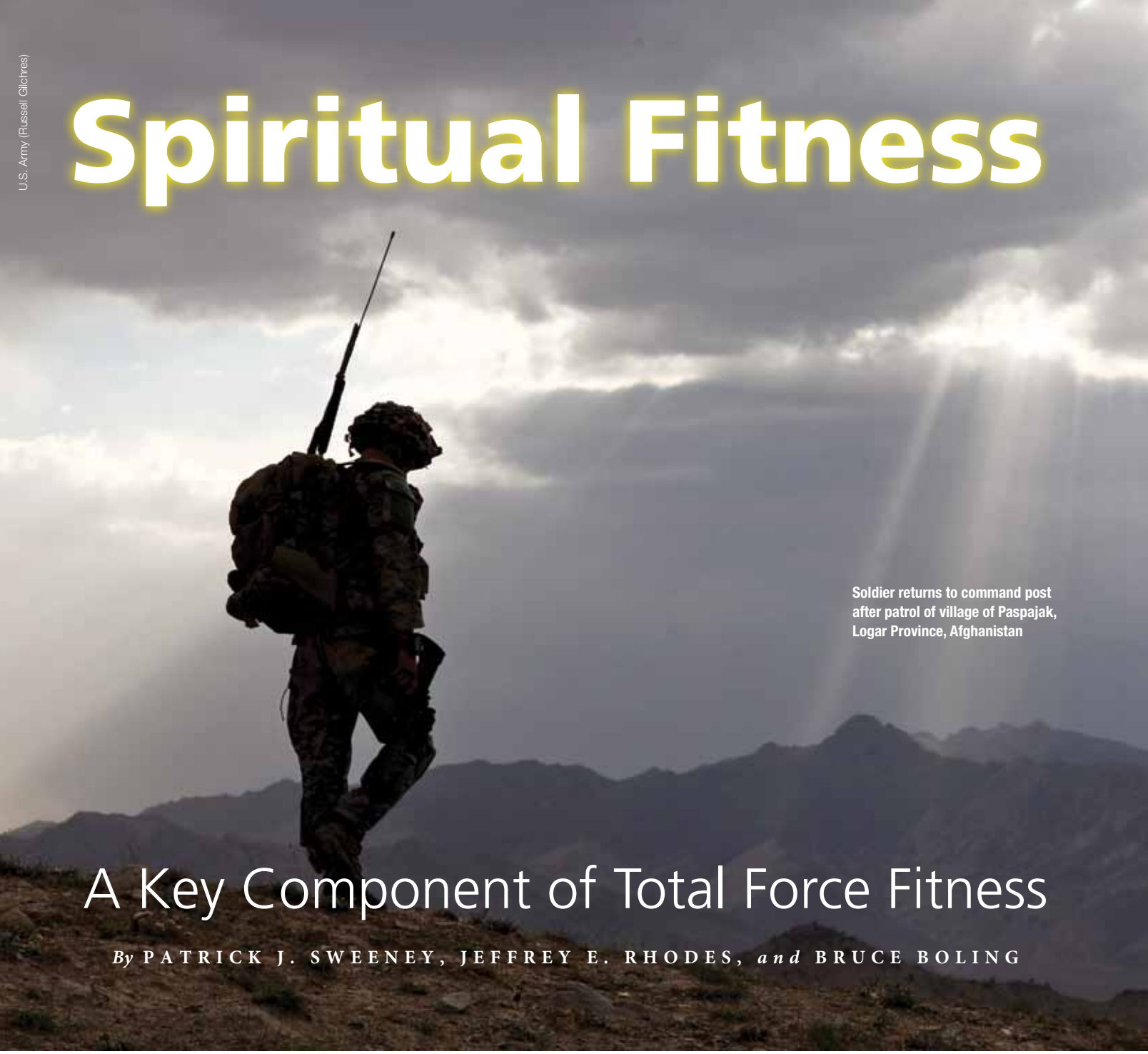
NOTES

[1] Wayne B. Jonas et al., "Why Total Force Fitness?" *Military Medicine*, vol. 175 (August 2010), 6–13, available at <www.siib.org/news/1099-SIIB/version/default/part/AttachmentData/data/Total%20Force%20Fitness%20for%20the%2021st%20Century--A%20New%20Paradigm.pdf>.

[2] *American Psychologist* 66, no. 1 (January 2011).

[3] Albert Ellis, *Reason and Emotion in Psychotherapy* (Secaucus, NJ: Citadel Press, 1962).

Spiritual Fitness



U.S. Army (Russell Gilchres)

Soldier returns to command post after patrol of village of Paspajak, Logar Province, Afghanistan

A Key Component of Total Force Fitness

By PATRICK J. SWEENEY, JEFFREY E. RHODES, *and* BRUCE BOLING

Wars may be fought with weapons, but they are won by men. It is the spirit of the men who follow and of the man who leads that gains the victory.

—General George Patton

Commanders throughout history have understood the importance of the human spirit to overcoming challenges and great odds to achieve victory. General Patton's words highlight that the outcomes of battles and history often rest in the strength of spirit of Soldiers, Sailors, Marines, and Airmen. Leaders have the responsibility to facilitate the development of each member's human spirit to ensure he has the spiritual fitness necessary to accomplish the mission, bounce back from adversity, and make meaning out of his experiences.

The development of spiritual fitness also helps mitigate moral injury to Servicemembers by fostering the strength of will to behave

Colonel Patrick J. Sweeney, USA, is a Professor in the Department of Behavioral Sciences and Leadership at the United States Military Academy. Dr. Jeffrey E. Rhodes, of Creative Computing Solutions, Inc., is contract support for the Defense Centers of Excellence for Psychological Health and Traumatic Brain Injury. Master Sergeant Bruce Boling, USAF, is assigned to 325th Operational Support Squadron, Tyndall Air Force Base, Florida.

U.S. Navy (Nicolas C. Lopez)

Sailors attend Easter sunrise service aboard USS *Carl Vinson*

in accordance with individual and organizational values. Moral injuries occur when Servicemembers perpetrate, fail to prevent, or bear witness to acts that transgress their values or beliefs. Such moral and ethical challenges can shatter an individual's beliefs about "the rightness of the world," degrade trust in leaders, and breed a sense of disillusionment and moral conflict.

A 10-year war on terror has stressed our forces and families to the point where members are bending and swaying under the pressures of multiple deployments and separation from family and friends. In an effort to address stress-related issues that the Armed Forces are facing and to enhance the effectiveness of the force, the Chairman of the Joint Chiefs of Staff (CJCS) directed the creation of Total Force Fitness (TFF, pronounced *tough*). This program challenges Service leaders to reorient their thinking and training programs and to adopt a new holistic prevention paradigm to bolster military readiness and force preservation. Under this proposed paradigm, total fitness is more than just an appreciation for and development of members' physical prowess. The TFF concept encompasses eight domains: physical, medical, environmental, social (including family), behavioral, spiritual, psychological, and nutritional. The program also concentrates on bolstering the fitness of units, families, and communities. This article introduces a framework to assist Department of Defense (DOD) leaders and personnel in understanding and developing spiritual fitness.

Definitions

Before developing a common framework for understanding spiritual fitness, three terms need to be initially defined: *human spirit, spirituality,* and *spiritual fitness*. The following definitions are broad enough to include the diversity of spiritual practices in DOD and also precise enough to avoid ambiguity.

The *human spirit* is the essence and animating force of the individual. It is the deepest part of the self, which includes one's core values and beliefs, identity, purpose in life, vision for creating a meaningful life, knowledge and truth about the world (perspective), autonomy to lead one's life, connection with others, and the quest to realize potential. In this sense, the human spirit propels people forward to take on challenges to further growth, serves as a guide to determine what is right and wrong, serves as a source of courage and hope, and provides the strength of will to live with integrity and meet responsibilities. The development of the human spirit is about shaping the essence of character.[1]

Spirituality refers to the continuous journey people take to discover and develop their human spirit. It is the process of searching for the sacred in one's life; discovering who one is; finding meaning and purpose; establishing interconnectedness with others and, if one so believes, with the divine; and charting a path to create a life worth living. While the definitions of spirituality and religion are sometimes blurred, they are two distinct concepts. Spirituality is both a process and path people use to discover their inner selves and develop their human spirit. *Religion* refers to institutions that propose and promote specified belief systems. It is one approach people can use in the process of developing their spirit.[2]

Spiritual fitness refers to an individual's overall spiritual condition. A spiritually fit person has the ability to continuously gain understanding of who one is in terms of core values and identity; live in accordance with core values; find purpose and meaning in life; be open to and continuously seek education and experiences that broaden one's view of the world; manage thoughts, emotions, and behavior; be uplifted by strong connections with others; demonstrate the strength of will and resilience to persevere when faced with challenges and adversity; make meaning out of their experiences; and exercise the autonomy to create a meaningful life that will realize one's full potential.[3]

Domain of the Human Spirit Model

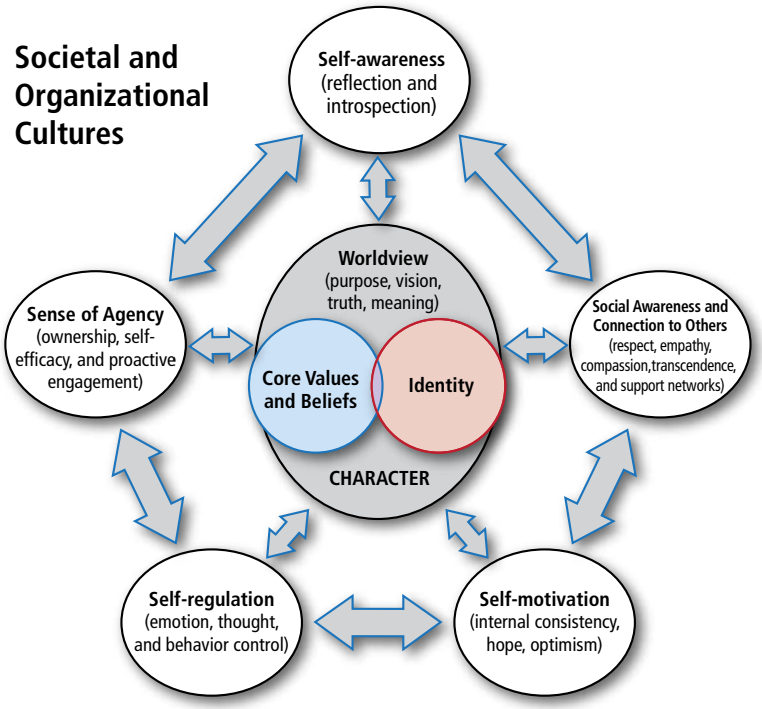
The domain of the human spirit model provides DOD personnel a common framework and language to understand and discuss human spirit development. The model was created by examining what develops when people engage in spiritual practices. By focusing on the psychological targets, the model goes beyond any particular means or approaches people use to develop their spirit to create a universal developmental model that is within the law. The domain of the human spirit consists of the psychological and social components depicted in the figure below.

These components are interrelated, and taken together they promote the development of the human spirit. The model provides leaders and mentors insights on how to best facilitate their own and others' development. A description of each component of the domain of the human spirit and its relevance to development follows.

Worldview consists of an individual's most central core values and beliefs, identity, character, and sense of purpose and meaning. Worldviews are the lenses people use to view and interpret events, determine how to act, and make meaning from their experiences. They are largely shaped through the socialization processes of the organizations that a person has been a member of, such as family, schools, teams, belief groups, communities, and military organizations. Servicemembers develop their worldviews by seeking out experiences such as overseas assignments, college courses, volunteering for nonprofits that serve the underprivileged, traveling, and seeking diversity in friends who challenge their current perspectives. A broad, complex worldview promotes openness to diversity and enhances individual adaptability to operate in dynamic and culturally diverse settings.[4] Worldview needs to be the central target of development in any program preparing leaders, Servicemembers, civilians, and family to meet the psychological and social demands of operating in dangerous environments, serving the Nation, and having loved ones serving away from home.[5]

Core values define who the person is and what the person stands for. They serve as a guide in determining right from wrong and appropriate behavior, especially in ambiguous and dynamic situations. Core values serve as a reservoir for a person to draw strength and courage to fulfill his duties and live with integrity. For Servicemembers, living daily by the mottos or the core values of their Service branches may be the most fundamental examples of practicing spirituality. Connecting to something beyond oneself is a central component of spirituality and the main theme for these mottos and values. The Air Force's core values—"Integrity first, Service before self, and Excellence in all we do"—explicitly stress the importance of putting service

Conceptualization of the Domain of the Human Spirit



Spiritual Fitness Outcomes

- Values-based Behavior
- Strength of Will
- Resilience
- Purpose and Meaning in Life
- Uplifting Relationships
- Openness and Acceptance
- Quest for Knowledge and Truth
- Enhanced Motivation to Leverage Skills to Realize Potential
- Greater Satisfaction and Commitment
- Increased Happiness

Adapted from Patrick J. Sweeney, Sean T. Hannah, and Don M. Snider, "The Domain of the Human Spirit," in *Forging the Warrior's Character: Moral Precepts from the Cadet Prayer*, ed. Don M. Snider and Lloyd J. Matthews (Boston: McGraw-Hill, 2008).

for the collective good before self-service. The Army's recruiting motto—"Army Strong"—implies that the collective body of all Soldiers is greater than the individual. The Navy core values—"Honor, Courage, and Commitment"—are all spiritual virtues that the Service asks its members to practice daily for the greater good of the unit and the Navy. And the Marine Corps motto—"Semper Fidelis"—demands its members to be "Always Faithful" to each other and the Corps. These mottos and core values share a basic tenet of spirituality: an individual understanding of and experience with that which transcends the self. This spiritual practice of fulfilling Service mottos and following core values supports a framework for managing daily unit demands, and provides a commitment for Service membership and mission accomplishment.[6]

Identity is a multifaceted psychological construct consisting of values, traits, knowledge, experiences, memories, and expectations that influence how a person views himself and his role in the world. Identity influences and controls the processing of any self-relevant information.[7] The following four facets provide DOD members a common identity: warrior, person of character, servant of the Nation, and global citizen.[8]

- *Warrior* is used to describe DOD members who view themselves as people who take on tough challenges, place duty first, complete assigned tasks, never quit or accept defeat, and never leave a fellow member in need. While each Service understands "warrior ethos" somewhat differently, once members integrate the Service's understanding of warrior ethos into their identities, they approach duties and living with a proactive, resilient, learning, and winning spirit.[9]
- A *person of character* is an individual who views himself as having the responsibility to seek the truth, decide what is right, and demonstrate the courage to act with integrity in all aspects of his life. The ideal state is to have each member of the DOD team perceiving himself as a person of character.[10]
- DOD members who view themselves as *servants of the Nation* foster the commitment necessary to step beyond self-interest to serve something greater. Contributing to the common good of the Nation and Service provides members with a sense of purpose and a way to make a difference with their lives, which provides a sense of meaning. This commitment to serve the citizens of the country also entails a sense of duty and a commitment with liability in terms of time, effort, and potential injury.
- Members who perceive themselves as *global citizens* not only take on the responsibility to serve and assist in making their local communities and the Nation better, but they also assume the responsibility to contribute to making the world a better place. This entails an active commitment to increase individual understanding of the issues facing the various levels of community they belong to and engage in activities to solve problems. Global citizens work to bring about the change they would like to see in their communities.

Character is shown through consistent moral and ethical actions for the purpose of maintaining congruence with individual and organizational values and beliefs. This

DOD (Linda Hosek)

Military family in play area at Warrior and Family Support Center, Brooke Army Medical Center, San Antonio

U.S. Air Force (Rachel Martinez)

Members of Air Force Special Tactics Squadron pray before starting 821-mile march to honor fallen comrade Tim Davis

integration of values and beliefs into self-identity assists in forming and strengthening character. DOD members' characters provide the moral compass to guide decisions and behavior, which is especially important when the potential for use of lethal force exists. They behave in a moral and ethical manner because to do otherwise would violate their sense of self. Thus, in all settings and situations within DOD, leaders and members with demonstrated character clearly establish the moral and ethical boundaries to ensure that operations are carried out within the law, and in combat settings, within the rules of engagement.

Providing Servicemembers the opportunity to serve and actually teaching *purpose and meaning* in serving is important in preparing and sustaining DOD members to meet the challenges of leading, operating in, and supporting operations in both dangerous and safe areas of operation. Purpose is a powerful motivational force that gets members to transcend self-interest and face the risks of injury or death in order to serve others. Core values linked with a sense of purpose provide a framework to find the strength of will to serve and make meaning out of adverse or traumatic experiences.

Self-awareness involves reflection and introspection, which enhance development of the human spirit. Through these processes, people gain insights into their most pressing questions about life: Who am I? What is my purpose in life? How do I create a life worth living? Who do I want to become? What can I believe in? How can I create a life that will make a difference and lead to happiness? And what happens after I die?[11] Answers to these introspective questions help individuals take responsibility for the development of their human spirit, form and shape their worldviews and characters, and create identities. Through dedicated reflection, people discover and build their human spirit. Reflection and introspection are important for people to make sense out of their own and others' experiences and, in the process, create new meaning and knowledge about themselves and the world. People use various activities to facilitate reflection and introspection such as journaling, listening to music, working out, sitting in a quiet location, meditating, hiking, watching the sun rise or set, and biking. The type of activity or location is not important: the keys are solitude and quiet time to reflect and assess the inner life. Through self-awareness, people gain the ability to chart and focus their quest to develop their human essence.[12]

Sense of agency means that people assume responsibility for the development of human spirit and that they have confidence they can successfully guide this quest. Agency empowers individuals by providing a sense of control over the development of their spirit.[13] DOD organizations can better facilitate a sense of agency by providing access to various resources including formal education opportunities that expose Servicemembers to topics relating to the development of the human spirit, traditional and online libraries that are well resourced with diverse materials, access to chaplains, and free use of spiritual and human development centers. Leaders must understand and appreciate that spiritual development is an individual journey and that there are multiple paths to developing one's spirit.[14]

Self-regulation is the ability to monitor, understand, assess, and control one's thoughts, goals, emotions, and behavior, or the ability to lead the self.[15] Self-regulation is a prerequisite to practice integrity, authentic leadership, and development as both a leader and a person.[16] There are three components to self-regulation: *standards, monitoring*, and *willpower*. Standards consist of individual core values, identity expectations produced by various facets (character, servant of the Nation, and global citizen), and the organizational ethical guidelines and core values.[17] Monitoring is simply individuals watching their behavior and comparing it against their standards. Willpower is the ability to change behavior to persevere in living by a cultural standard or by achieving goals. Willpower is a limited resource that gets depleted with use and fatigue.[18] Self-regulation plays a pivotal role in allowing DOD members to meet unique challenges, particularly in dangerous and high stress contexts.

Self-motivation refers to the ability to motivate oneself to act with integrity even in situations of risk and to persist toward one's vision of creating a life worth living even when faced with challenges. DOD members want to continuously expand internal sources of motivation to drive their actions and quests to develop their spirit. An individual's belief that he has the ability to control the development of his spirit also enhances internal motivation. Another important source of internal motivation comes from the integration of core values into individual identities. People are motivated to behave congruent with their values in order to preserve their sense of self.[19] Striving to achieve a *worthy purpose* is also a powerful internal motivating force that influences people to act in accordance with their individual and organization values. In DOD operations, members' self-motivation impacts strength of will, physical and moral courage, resilience to stress and adversity, meaning-making, and trust development. The strength of members' will or spirit rests in their motivation to act in a manner consistent with their core values and beliefs, identity, and the achievement of their purpose.[20]

Social awareness and connection to others refers to an individual's realization that relationships with others play an essential role in the development of the human spirit. To harness the developmental power of relationships, an individual needs to have the skills and abilities necessary to connect with people in a positive manner. These basic social skills and abilities include respect, empathy and compassion, transcendence of self-interests, effective communication, and trust of others.[21] Positive connections with others are critical for development and social resilience.[22] Support networks are critical in assisting individuals in meeting life's psychological and social challenges, especially when leading and operating in dangerous and stressful contexts, as well as in managing stress and promoting resilience. The bonds that unite people in social networks are based on trust. Social support networks also serve as powerful motivational forces to encourage Servicemembers to behave courageously and honorably.

The journey to develop one's spirit is influenced by multiple levels: *individual self-development, relationship networks*, and *organizational cultures*. Most people's worldviews are shaped by their families, philosophical or faith groups, schools, teams, communities, and society. Groups possess, communicate, and hold members accountable to a set of common values, norms, assumptions about how to operate and function, collective identity, and purpose—or culture.[23] Living and working in various organizational cultures creates social realities that influence members' perceptions of what is right and wrong, what the values are to lead and live by, how we should treat each other, what provides meaning to work and life, and what are noble purposes to pursue. Leaders can promote organizational culture to assist in reinforcing each member's development of their worldviews and the various psychological attributes that support these views.

social support networks serve as powerful motivational forces to encourage Servicemembers to behave courageously and honorably

Techniques for Leaders to Encourage Spiritual Fitness

Promote Organizational Culture. Clearly communicate core organizational values and purposes and discuss how conducting business by these values enhances both the organization and its people. An organization that serves a higher purpose and has a moral and ethical culture has the potential to positively influence members' worldviews, especially concerning purpose, values, and identity.

Ask Reflective Questions. In daily interactions, ask questions to get members to think about and question how they view the world to include assumptions, values, purpose, life vision, liability associated with serving, emotional reactions, behavior, and morality. These daily reflective prompts have the potential to enhance members' self-awareness, agency, self-regulation, and worldviews. Conducting reviews after significant organizational events is an opportunity to raise reflective questions. In units that apply lethal force, prompt members to reflect on how they would make sense out of taking another human's life, the potential of losing their own lives, and giving orders that result in the loss or injury of a group member.

Model Respect. Assume that all humans have value and that value systems are honored by understanding and learning from people who hold different beliefs and practices. Respecting others and being open to diversity creates opportunities for DOD members to experience and share different perspectives that encourage reflection and the expansion of worldviews.

Encourage Meaning-making. Promote opportunities to share perspectives and rationale for making decisions, especially if the decisions have moral or ethical implications. Sharing perspectives exposes members to a different perspective, reinforces how the organization's values are put into action, and encourages open communication. These meaning-making sessions are good forums for exposing members to multiple perspectives to help them learn and make meaning out of their experiences.

Empower and Challenge. Provide members experiences that will challenge their perspectives and skills. Overseas assignments, temporary duty in another country, working with members from another culture, and working on a diverse

team are opportunities to broaden members' worldviews.

Network Connection Checks. Establish uplifting relationships with group members and encourage subordinate leaders to do the same. Regularly check to ensure all members are connected to the group's social network. When operating in dangerous areas, social support provides members with strategies to manage stress, make meaning out of their experiences, sustain perseverance, bolster resilience, and promote post-adversity growth.

Offer Resources. Provide members with access to and time to use resources such as spiritual well-being centers, chaplains, enhancement performance centers, and places to practice their beliefs. That way, leaders can facilitate the development of subordinates' human spirit.

Conclusion

The spiritual fitness of DOD members is a critical component of force readiness. The domain of the human spirit model provides DOD with a common framework and language to think about, discuss, and take purposeful action to enhance members' spiritual fitness within the law. Individuals can use the model to assess their own spiritual fitness and to design plans to enhance the development of their spirits. It empowers members and leaders as active participants in strengthening the spirit of the force. Leaders have an array of simple techniques they can use daily. Promoting spiritual fitness is a vital component of the DOD TFF initiative and fully complements growth in the other seven domains. **JFQ**

NOTES

[1] Patrick J. Sweeney, Sean T. Hannah, and Don M. Snider, "The Domain of the Human Spirit," in *Forging the Warrior's Character: Moral Precepts from the Cadet Prayer*, ed. Don M. Snider and Lloyd J. Matthews, 23–50 (Boston: McGraw Hill, 2008).

[2] Ken I. Pargament, *Spiritually Integrated Psychotherapy: Understanding and Addressing the Sacred* (New York: Guilford Press, 2007).

[3] Sweeney, Hannah, and Snider, 23–50.

[4] Patrick J. Sweeney and Michael D. Matthews, "A Holistic View of Leading in Dangerous Contexts," in *Leadership in Dangerous Situations: A Handbook for Armed Forces, Emergency Services, and First Responders*, ed. Patrick J. Sweeney, Michael D. Matthews, and Paul Lester (Annapolis, MD: Naval Institute Press, 2011).

[5] Ibid., 64–66.

[6] Alfred Bandura, "On the Psychosocial Impact and Mechanisms of Spiritual Modeling," *International Journal for the Psychology of Religion* 13, no. 3 (2003), 167–174.

[7] Hazel Markus and Elissa Wurf, "The Dynamic Self-Concept: A Social Psychological Perspective," *Annual Review of Psychology* 38 (1987), 299–337.

[8] United States Military Academy (USMA), *Building the Capacity to Lead: The West Point System for Leader Development* (West Point, NY: USMA, 2010), 9–14.

[9] Field Manual 6-22, *Army Leadership: Competent, Confident, and Agile* (Washington, DC: Headquarters Department of the Army, 2006), 4–10.

[10] Ibid., 10–11.

[11] Carl R. Rogers, *On Becoming a Person* (Boston: Houghton Mifflin, 1961), 164–181.

[12] Sweeney, Hannah, and Snider, 67–68.

[13] Albert Bandura, "Social Cognitive Theory: An Agentic Perspective," *Annual Review of Psychology* 52 (2001), 1–26.

[14] Sweeney, Hannah, and Snider, 68–71.

[15] Roy F. Baumeister, *The Cultural Animal: Human Nature, Meaning, and Social Life* (New York: Oxford University Press, 2005), 310–315.

[16] David Day, Michelle Harrison, and Stanley Halpin, *An Integrative Approach to Leader Development* (New York: Taylor & Frances Group, 2009), 191–194.

[17] Richard Ryan and Edward Deci, "On Assimilating Identities to the Self: A Self-determination Theory Perspective on Internalization and Integrity within Cultures," in *Handbook of Self and Identity*, ed. Mark R. Leary and June P. Tangney, 253–272 (New York: Guilford Press, 2003).

[18] Baumeister, 310–315.

[19] Augusto Blasi, "The Development of Identity: Some Implications for Moral Functioning," in *The Moral Self*, ed. Gil G. Noam and Thomas E. Wren, 99–122 (Cambridge, MA: MIT Press, 1993).

[20] Sweeney, Hannah, and Snider, 55–99.

[21] Rogers, 37–38.

[22] John T. Cacioppo, Harry T. Reis, and Alex J. Zautra, "Social Resilience: The Value of Social Fitness with an Application to the Military," *American Psychologist* 66, no. 1 (2011), 43–51.

[23] Edgar H. Schein, *Organizational Culture and Leadership*, 3rd ed. (San Francisco: Jossey-Bass, 2004), 3–23.

NASA (Pat Izzo)

NASA Center for Climate Simulation "Discover" supercomputer contains 15,000 processors

TECHNOLOGICAL STRATEGY IN THE AGE OF EXPONENTIAL GROWTH

By CARLO KOPP

Dr. Carlo Kopp is an Associate Fellow of the American Institute of Aeronautics and Astronautics, a Senior Member of the Institution of Electrical and Electronic Engineers, and a Member of the Association of Old Crows.

There can be little doubt that the definitive technological strategy problem at this time is how to deal with exponential growth in digital technologies. Exponential growth is producing effects that are pervasive across the global industrial base and having an impact on almost every aspect of developed societies in both constructive and destructive ways. While exponential growth is producing important changes in how societies and their respective militaries function, technological strategies underpinning the definition and development of contemporary weapons systems are frequently not well aligned with the seismic growth in the basic technologies employed in such systems. Whenever the evolution of a technology base outstrips technological strategy and operational technique, there is potential for disaster in battle. Excellent case studies exist where formerly new weapons were deployed and used without a well-defined technological strategy or commensurate conceptual coupling with tactics, operational technique, and theater-level strategy, resulting in difficulties and often failure.

Exponential growth in digital technologies used for information-gathering, processing, storage, and distribution is arguably the defining trend in this decade, yet it is frequently not well understood. Some observers regard such growth with unbounded optimism.[1] A common misconception is that exponential growth is pervasive, but this is seldom true. Even within rapidly evolving areas, exponential growth may be limited to a small number of constituent components in larger systems.

To appreciate the manner in which exponential growth affects technological strategy, the inevitable starting point is to determine how exponential growth works, and which technologies grow exponentially and which do not. Only then is it possible to divine the broader and deeper implications of the problem and its concomitant effect on technological strategy, operational strategy, and ultimately, grand strategy.

This article explores the social and technological effect termed *exponential growth*, contemplates how it affects military systems and technological strategy, and considers a number of related problems in aligning technological strategy with an exponentially growing technology base.

Exponential Growth Laws

The term *exponential growth* describes an observed effect in some basic technology, where performance per dollar multiplies over time. The best known example is Moore's Law, under which the density of microprocessors doubles over an 18- to 24-month period.[2] The behavior observed is, in mathematical terms, no different to that observed in continuously compounded interest in finance. The gains experienced in one time interval set the starting point for the next. As a result, the gains are continuous and can be enormous over periods of time. Moore's Law presents the best example in recent times where computing power in handheld devices now matches or exceeds that of the largest computer systems built and used during the 1960s at costs which are trivial in comparison with their predecessors.

exponential growth is seldom sustained indefinitely and usually ceases when some bounding condition is encountered

In practice, exponential growth is seldom sustained indefinitely and usually ceases when some bounding condition, determined by physics or mathematics, is encountered, or when research and development funding collapses due to shifts in a commercial marketplace or government funding priorities.

An important observation is that unlike many laws in hard science, which have a basis in mathematics and physics, "exponential growth laws" have no such basis and represent an empirical generalization of the observable interaction of technology and social behavior. Unlike laws in hard sciences, which are immutable, exponential growth laws may collapse at any time if the social conditions producing them change.[3]

In recent decades, the sustained exponential growth in digital technologies used for information-gathering, processing, storage, and distribution shows that the market for consumer and industrial digital equipment has yet to saturate, and key physics bounds have yet to be encountered.

Nonexponential vs. Exponential Growth

Nonexponential growth is the more common situation across the technology base. This is important because most military systems comprise many components, few of which will grow exponentially. Technologies that are mechanical or chemical, such as structural materials, aerodynamics, hydrodynamics, and all forms of propulsion, do not exhibit exponential growth because the underlying physics do not permit it.

While we have seen strong improvements in jet and rocket propulsion since their advent in modern military systems during the 1940s, jet engine fuel efficiency has improved over that time by a factor of three at best, while rocket propellants have improved in specific impulse only by a slightly better margin. Improvements in structural materials, either in weight or strength, have also been on a similar scale over a half-century of continuous research and development. Much the same can be said of chemical explosives, armor materials, and many other pivotal technologies used in military systems.

A common misconception is that computer software grows exponentially in performance over time. While software has shown evidence of exponential growth in raw complexity, this is typically at the expense of computational efficiency and thus the speed with which a computation can be performed.

When considered against the technology base in military use today, technologies with exponential growth behavior are uncommon. Even so, they have forced significant changes and will continue to do so.

Exponential Growth in Computing Technology

Computer hardware is at the heart of the information age and pervades all digital technologies used for information-gathering, processing, storage, and distribution, often in ways not obvious to the casual observer. Whether we look at embedded computers in military equipment, consumer devices of all shapes and sizes, or traditional desktop and server computers used for data processing, at the heart of all of these devices are one or more processor chips—each a single-chip computer. Nearly all processor chips exhibit growth following Moore's Law, and with a half-century of empirical data to prove it, Moore's Law has become a defining driver for planning within the computer industry.

Moore's Law exists because the technology used to fabricate processing chips, whether based on silicon or other more advanced materials, is centered in photolithography, which is used to sculpt the features that form the transistor switches within the chip, permitting the fabrication of ever smaller transistors over time

Chief of Naval Research addresses Naval Science, Technology, Engineering and Mathematics Forum

U.S. Navy (John F. Williams)

as photolithographic technology improves. Smaller transistors typically switch faster, dissipate less power, and permit more complex internal structures on the chip.[4]

Until recently, Moore's Law tracked true both for the density of processors and for how quickly they could execute, producing exponential growth in chip density and switching speeds. The actual improvements in computing performance were frequently better than exponential, as increasingly sophisticated performance improving architectural features could be employed. A reality little appreciated outside the computer architecture community is that a contemporary processor chip in an iPhone, notebook, or iPad/Kindle has an internal architecture not unlike a mainframe or supercomputer of the 1960s or 1970s.

The technology base, however, is approaching the limits of photolithographic techniques. At this time, internal heat dissipation is putting limits on how fast processors can switch internally. This has resulted in the increasing use of multicore or parallel processors where a single chip hosts two, four, six, or many more processors or cores, rather than a much faster single core. More important, transistor sizes are approaching the limits of what physics permits and where quantum physical effects begin to impair operation. Current estimates by the industry suggest that Moore's Law, using photolithographic fabrication techniques, may hit hard limits within 5 to 15 years, assuming no significant physics breakthroughs in other areas.[5] To place this in perspective, a rule of thumb in science-based futures predictions is that reliable estimates more than 11 years into the future are scarce because unexpected breakthroughs can and often will result in unpredicted outcomes.[6] Therefore, it is possible that unexpected and intractable obstacles may be encountered later or sooner than current estimations.

Unfounded Optimism in Parallel Processing

When a processor is not fast enough to solve a problem, the most common solution is to employ more than one processor—a technique known as parallel processing whereby the computing workload is split across multiple processors. Unfortunately, not every type of computation can be easily split up to permit faster computation. The optimism surrounding the use of computational clouds and other highly parallel systems is frequently unrealistic, as such systems will not realize any performance gain if the problem to be solved does not "parallelize" readily. This has been understood by computer scientists since Gene Amdahl published his now famous 1967 paper.[7]

When Moore's Law eventually plateaus, the fallback strategy of aggregating vast numbers of processing cores to improve performance will only produce effect for some types of computations. In many applications, Amdahl's Law will present an intractable obstacle to further performance growth.

Exponential Growth in Storage Technology

Storage technologies are in many respects as important as processing technologies in many military applications. Currently, this area is dominated by three technologies: encompassing semiconductor memories, rotating magnetic "hard" disks, and rotating optical disks, such as the CD-ROM and DVD. All of these technologies have exhibited strong and sustained exponential growth in storage density, comparable to or stronger than seen in processing chips.

Semiconductor memories such as modules used in computers, nonvolatile flash memories used in USB thumbdrives, and digital camera SDHC cards all follow Moore's Law and will closely track growth in processor technology. Rotating magnetic hard disks follow Kryder's Law, with strong sustained exponential growth in recent years. Similar growth is observed in optical storage technologies.[8] While data storage density has been strongly exponential, access times, or how long it takes to find an item of data, have not been. The mechanical nature of rotating media has at best seen access times halved over the last two decades. While the use of semiconductor cache memories on such drives has much improved access times for frequently used data, infrequently used data will continue to suffer the speed limitations imposed by mechanical designs ever since the 1960s.

Exponential Growth in Networking Technology

Networks have been a central part of the explosive growth seen in information technologies over the last two decades and indeed have been a prominent feature of the high operations tempo paradigm of network-centric warfare (NCW). In fixed cabled networks, especially those using optical fibers, growth has been exponential due in part to the enormous bandwidth of optical fiber and in part to the photolithographically fabricated semiconductor laser chips employed. In such networks, exponential growth will continue until hard limits are encountered in laser fabrication.

The performance of wide area wireless radio networks, pivotal in military systems, is generally not growing exponentially in throughput performance and never will. Many advocates of NCW appear to have assumed otherwise. While Edholm's Law argues for exponential growth in wireless technologies such as WiFi and WiMax, it fails to consider the critical constraint of transmission range, a central need in military networks.[9]

The dichotomy between cabled optical networks and wireless radio networks reflects the different transmission physics that apply to guided versus unguided transmission media.[10]

Radio frequency transmission effects thus impose much stronger limitations on data throughput than the density of the chips in the equipment used within the link or the network. Increasing congestion across the radio frequency spectrum presents further difficulties, which will not be overcome easily. Another problem unique to military radio networks is resilience to hostile jamming, always at the expense of data throughput.

Exponential Growth in Optical and Radio Frequency Sensor Technology

Digital imaging chips have produced a revolutionary impact in consumer and professional photography, as well as military intelligence, reconnaissance, and surveillance (ISR) applications. No differently, MMIC (Monolithic Microwave Integrated Circuit) technology has produced similar effects in consumer wireless products, as well as military radar and passive radiofrequency sensors. Both technologies, fabricated using the same photolithographic techniques as processor chips, have exhibited exponential density growth, but much slower than that observed in processors and memories.

The more sedate growth observed is an inevitable byproduct of the need to accommodate unique design constraints, such as photosite performance in optical chips or electrical impedance matching in MMICs. These constraints are frequently much stronger than gains arising from density improvement.

The Nonexponential Realities of Software Algorithms

Computer algorithms used in software do not commonly display exponential performance growth and, given the mathematical realities involved, never will. The observed improvements in performance are mostly asymptotic, where progressive refinements over time push the performance of the algorithms ever closer to some fundamental mathematical limit in ever smaller increments. Prima facie, this would suggest that overall performance of hardware and software should improve exponentially over time as hardware performance tracks Moore's Law. The reality is otherwise.

The most pronounced effect we see in software performance over the last three decades is the "bloatware problem," where software progressively grows in complexity over time, soaking up any gains in hardware performance, often at rates faster than exponential growth in hardware can accommodate.[11] Such complexity growth is endemic in both civilian and military software products, whether intended for office or real-time embedded applications. The causes are partly accidental and partly essential.[12]

Accidental complexity and its growth is partly the byproduct of attempting to maintain compatibility with legacy software and hardware interfaces and data formats while accommodating new interfaces and data formats, as well as new features and operating modes. In a sense, this effect is akin to increasingly complex DNA in evolving biological organisms—adaptation requires growth in complexity. Essential problems in software development relate to the problem being solved, encompassing the complexity of the problem, and the typically asymptotic behaviors of algorithms.

Far more problematic, however, are the other accidental causes of growth, which more often than not reflect undisciplined requirements by customers and vendors alike. Whether a commercial product is being dressed up with features to expand its market footprint, or a military system is being overfeatured to satisfy the wish lists of multiple stakeholders with diverse agendas, the effect is the same, and the problem is rooted in human social behavior rather than technology.

This problem has been understood for decades, yet no common solution has been devised to overcome it. The competitive internal dynamic of groups defining designs, or implementing them, is at the root of the problem. Individuals seek to improve the product or attach their personal signature to it by adding to it, a problem arising in product definition and/or development. For the foreseeable future, the outlook for improved military software applications performance is not good, as the primary cause of the bloatware problem is rooted in the internal social dynamics of organizations rather than in any basic technology. In this respect, the power of software to be rapidly adapted becomes a weakness in its own right.

Impact of Exponential Growth and Evolutionary Strategies

Exponential growth produces positive and negative effects. In digital technologies used for information-gathering, processing, storage, and distribution, it has produced its greatest positive impact in ISR applications and military communications and networking. Other areas have also seen major positive impacts, such as navigation systems, weapons guidance, vehicle control and management systems, and, most recently, directed energy weapons.

lateral evolution can frequently produce highly disruptive effects, as the new solution will often exploit systemic weaknesses in an opponent's capabilities

The most common negative effect is the premature obsolescence of digital processing chips embedded within weapons systems, forcing frequent hardware upgrades and often expensive software changes to maintain the supportability of the equipment. Where not addressed properly, this has significantly contributed to the life-cycle costs of maintaining and operating equipment.

Positive effects are typically produced in two distinct ways. The first and most frequent is by a linear evolution strategy, where the performance, capability, compactness, reliability, or functionality of some existing system or subsystem is improved or enhanced by replacement of a legacy technology with an exponentially growing new technology. It is termed *linear*, as the growth follows an earlier direct or linear evolutionary pattern in the technology.

The second and less frequent way in which exponential growth produces impact is through *lateral* evolution strategy, where new technology presents opportunities to devise entirely new solutions to longstanding, or entirely new problems, reflecting the Edward de Bono model of "lateral thinking."[13] Lateral evolution can frequently produce highly disruptive effects, as the new solution will often exploit systemic weaknesses in an opponent's capabilities that cannot be easily overcome by established means.

There is an abundance of good case studies to be considered. Linear evolution includes the use of monolithic chips in visible band and infrared imaging systems, where


U.S. Army (Jennifer Spradlin)

Netherlands air force pilot checks RecceLite tactical reconnaissance pod at Kandahar Airfield, Afghanistan, prior to mission

smaller, more sensitive, more reliable, and higher resolution sensors have yielded revolutionary improvements against legacy wet film technology. The advent of Gallium Arsenide radio frequency chips for use in radar has seen revolutionary improvements in the transition from legacy mechanically steered radar and communications antennas to contemporary Active Electronically Steered Array (AESA) antennas. Three recent case studies of lateral evolution are worth careful consideration, as they show how a shift in basic technology becomes an enabler in areas that were not even considered when the new technology was developed.

The first case study considers the emergence of gigapixel imagers, such as the Defense Advanced Research Projects Agency/BAE System Autonomous Real-Time Ground Ubiquitous Surveillance Imaging System, which aggregates hundreds of consumer commodity megapixel-class cell phone imaging chips to permit simultaneous wide angle, high-resolution imaging of large areas. The designers of these cell phone camera chips had no conception of the military potential of the devices. Yet the technology has significant long-term potential across a wide range of ISR applications, not only in counterinsurgency environments.[14]

The second case study focuses on the use of high power AESA radars to produce radio frequency weapons effects intended to disrupt or electrically damage opposing aircraft or guided weapon sensors or systems. The availability of high-peak power emissions in larger AESA radars became the enabler for this technique, which has considerable long-term potential given the established trends in AESA design.[15]

The third case study concerns the use of solid-state laser diodes and doped optical fiber amplifier technology, both initially developed for communications applications as optical pump technology for electrically powered high-power laser weapons. Both of these technologies have been adapted to develop pumping sources for laser weapons that overcome the historical "magazine depth" problem associated with chemically pumped lasers that depend on the in situ chemical propellant supply.

All of these case studies present capability surprises to opponents of the United States that will significantly complicate their operations in combat situations and demonstrate the highly disruptive effects that can be produced by lateral evolution.

Technological Strategy and the Technological Strategist

The discipline of technological strategy has been part of warfare for millennia but was without doubt most actively practiced during the Cold War when the United States confronted a technologically competent and often highly creative peer competitor in the Soviet bloc. The seminal work on modern technological strategy dates back to the most intensive phase of that contest during the latter 1960s.[16]

Technological strategists use advanced technology to outmaneuver and often economically defeat opponents by forcing disproportionate expenditures in peacetime and disproportionate attrition in wartime. Most technological strategists are gifted scientists or engineers by training with a talent for strategic thought and considerable natural creativity.

While technological strategy is not a strong feature of contemporary Western defense planning, it remains a central feature of highly successful corporate players within the electronics and computing industries. The astounding resurgence of Apple, via its innovative Mac, iPod, iPhone, and iPad product families, represents without doubt the best recent commercial case study, an effort that was largely driven by Steve Jobs, who was both a gifted engineer and a strategic thinker.[17]

It is abundantly clear that technological strategy can be explained, codified, and systematically taught. However, the historical record suggests that genuine breakthroughs require a strong element of talent and vision. As a result, a fundamental challenge to most organizations is that the talent required to produce outstanding results in technological strategy tends to be scarce and must be nurtured and developed.

Effective technological strategists must have deep expertise in the technological areas of interest, considerable experience to know what can and cannot be built, and an understanding of what will and will not work operationally. They must also possess the gift for strategic thought. Accomplished past practitioners across the Western defense industry include Vickers's Barnes Wallis, who devised the modern bunker-busting bomb, Lockheed's Kelly Johnson and Northrop's John Cashen, and within the Armed Forces the often controversial yet gifted Colonel John Boyd, who was able to articulate and effectively propagate his revolutionary vision of energy maneuverability.

The inevitable consequence of failing to practice good technological strategy is that opponents will produce breakthroughs. A smart opponent will produce repeated "capability surprise" events to an advantage, as the United States did to the Soviet Union, contributing crucially to the eventual bankruptcy of the Soviet bloc.

Technological Strategy vs. Exponential Growth

The presence of exponential growth in key current technologies is a double-edged

sword because these technologies have been commodified and are globally accessible in the commercial marketplace. A Russian or Chinese weapons developer will have access to much of the same basic technology as his peers in the United States. This represents a leveling of the technological playing field unseen since World War II. For instance, the well-developed Russian technological strategy intended to defeat U.S. airpower is disciplined and well-considered, leverages exponential growth in key technologies, and displays a deep understanding of critical ideas and how to leverage globalized exponentially growing technologies.[18]

a smart opponent will produce repeated "capability surprise" events to an advantage, as the United States did to the Soviet Union

On a level playing field, with exponential growth in critical technologies, the player who can best exploit talent to an advantage—all else being equal—will inevitably win. For the United States and its technologically competent allies, this period should be one of critical reflection. Many recent high-profile programmatic failures display numerous symptoms of poor practice and implementation of technological strategy during program definition and later development, beginning in the decade following the end of the Cold War. Moreover, poor understanding of exponential growth and concomitant early component obsolescence has contributed to severe life-cycle cost problems across a wide range of programs.

A good case can be made that these failures directly reflect the diminished role of technological strategists in the post–Cold War environment, where imperatives other than defeating peer competitor nation-states became ascendant and dominant, while the last generation of Cold War–era technological strategists progressively retired from government service or retired altogether, with few if any replacements trained or appointed.

While entities such as the Defense Science Board and respective Service science boards and chief scientists have remained active in technological strategy and continue to provide valuable inputs, all of these entities perform roles that are essentially advisory rather than serving as directly integrated and organic components of the capability development cycle, where technological strategists were most active during the Cold War.

In a period of exponential growth in many critical technologies, maintaining an advantage over nascent technological peer competitors requires that technological strategy be a tightly integrated component of the capability development cycle and that an ample population of gifted technological strategists exists both within government organizations and within the contractor community. If the United States wishes to retain its primacy in modern nation-state conflicts, technological strategy must be restored to the prominence it enjoyed during the Cold War period. **JFQ**

NOTES

[1] The best example is Ray Kurzweil's *The Singularity Is Near: When Humans Transcend Biology* (New York: Viking, 2005). Kurzweil's "singularity" is a projected future point in time where machine intelligence exceeds human intelligence. While the science underpinning Kurzweil's projections is frequently weak, his work has stimulated important ethical, philosophical, and strategic arguments about how to manage advanced artificial intelligence.

[2] Gordon E. Moore, "Cramming More Components onto Integrated Circuits," *Electronics*, April 19, 1965, 114–117.

[3] In a strict scientific sense, exponential growth laws should not be called "laws" but rather "curves." A more exact model is that these laws are convolutions of multiple S-curves for specific technologies employed. See Murrae J. Bowden, "Moore's Law and the Technology S-Curve," *Current Issues in Technology Management* 8, no. 1 (Winter 2004).

[4] Carver Mead and Lynn Conway, *Introduction to VLSI Systems* (Reading, MA: Addison-Wesley, 1980).

[5] R.W. Keyes, "Fundamental Limits in Digital Information Processing," *Proceedings of the IEEE* 69, no. 2 (February 1980), 267–278; R.W. Keyes, "Fundamental Limits of Silicon Technology," *Proceedings of the IEEE* 89, no. 3 (March 2001), 227–239; K.K. Likharev, "Classical and Quantum Limitations on Energy Consumption in Computation," *International Journal of Theoretical Physics* 21, no. 3–4 (May 1982), 311–326; V.V. Zhirnov et al., "Limits to Binary Logic Switch Scaling: A Gedanken Model," *Proceedings of the IEEE* 91, no. 11 (November 2003), 1934–1939; and Laszlo B. Kish, "End of Moore's Law: Thermal (Noise) Death of Integration in Micro and Nano Electronics," *Physics Letters A* 305, no. 3–4 (December 2002), 144–149.

[6] J. Birnbaum, "The Next 50 Years," ACM97 Conference Talks, Association for Computing Machinery, 1997.

[7] Gene M. Amdahl, "Validity of the Single Processor Approach to Achieving Large Scale Computing Capabilities," from the proceedings of the April 18–20, 1967, spring joint computer conference, AFIPS 1967 (Spring), 483–485, New York, NY, 1967.

[8] Chip Walter, "Kryder's Law," *Scientific American*, July 25, 2005.

[9] Steven Cherry, "Edholm's Law of Bandwidth," *IEEE Spectrum*, July 2004.

[10] Unguided media depend on antenna design, radio propagation through the atmosphere, hostile radio frequency jamming, emission stealthiness, and Shannon's information theory. See R.C. Hansen, "Fundamental Limitations in Antennas," *Proceedings of the IEEE* 69, no. 2 (February 1981), 1934–1939; R.K. Crane, "Fundamental Limitations Caused by RF Propagation," *Proceedings of the IEEE* 69, no. 2 (February 1980), 196–209; and C.E. Shannon, "A Mathematical Theory of Communication," *Bell System Technical Journal* 27 (July, October 1948), 379–423, 623–656.

[11] Niklaus Wirth, "A Plea for Lean Software," *Computer* 28, no. 2 (February 1995), 64–68; and Joel Spolsky, "Strategy Letter IV: Bloatware and the 80/20 Myth," March 23, 2001, available at <www.joelonsoftware.com/articles/fog0000000020.html>.

[12] Frederick P. Brooks, Jr., "No Silver Bullet: Essence and Accidents of Software Engineering," *Computer* 20, no. 4 (April 1987), 10–19.

[13] Edward de Bono, *The Use of Lateral Thinking* (London: Cape, 1967).

[14] Graham Warwick, "ARGUS: DARPA's All-Seeing Eye," February 10, 2010, available at <www.w54.biz/showthread.php?138-BAE-Persistent-Surveillance-System>.

[15] See, for instance, D.A. Fulghum, "Hornet's Electronic Sting," *Aviation Week & Space Technology*, February 26, 2007, 24–25.

[16] Stephan T. Possony et al., *The Strategy of Technology* (1970), available at <www.jerrypournelle.com/slowchange/Strat.html>.

[17] Richard Gourlay, "Strategy: How Steve Jobs Changed the World," *Businesszone*, August 30, 2011, available at <www.businesszone.co.uk/blogs/richard-gourlay/do-you-have-vision-or-are-you-just-dreamer/strategy-how-steve-jobs-changed-wor>.

[18] Carlo Kopp, "Evolving Technological Strategy in Advanced Air Defense Systems," *Joint Force Quarterly* 57 (2nd Quarter 2010), 86–93.

U.S. Air Force (William Green)

IDF participate in training exercise

FORGING JOINTNESS UNDER FIRE

Air-Ground Integration in Israel's Lebanon and Gaza Wars

By **BENJAMIN S. LAMBETH**

In July and August 2006, the Israel Defense Forces (IDF) waged a 34-day war against Hizballah, an Iranian proxy terrorist organization based in Lebanon, in response to a raid by a team of Hizballah combatants into northern Israel that resulted in the abduction of two Israeli soldiers to be held as hostages. That escalated response, code-named Operation *Change of Direction*, ended up being the most disappointing IDF performance in its nearly six-decade history in that it represented the first time a major war had ended without the achievement of a clear-cut military victory by Israel.

The main reason for the IDF's poor showing in that campaign was the failure of Prime Minister Ehud Olmert and his government to size up the enemy correctly, set achievable goals, apply a strategy suited to the attainment of those goals, and manage expectations as the campaign unfolded. No less at fault, however, was a near total breakdown in the effective integration of air

Benjamin S. Lambeth is a Senior Fellow at the Center for Strategic and Budgetary Assessments. This article is an excerpt from his *Air Operations in Israel's War against Hezbollah: Learning from Lebanon and Getting It Right in Gaza* (RAND, 2011), available at <www.rand.org/pubs/monographs/MG835.html>.

and land operations that had been allowed to develop in Israel after the onset of the Palestinian intifada in 2000 and the almost exclusive fixation of IDF ground forces on that domestic uprising ever since.

A little more than 2 years later, the IDF conducted a more satisfactory campaign against Hamas in the Gaza Strip in which the problems of air-ground integration that had been unmasked during the second Lebanon war were all but completely corrected. The net effect of that success was to replenish Israel's stock of deterrence that had been badly depleted in the aftermath of the IDF's more uneven performance in 2006.

A Wakeup Call in Lebanon

At the time Operation *Change of Direction* first got under way on July 6, 2006, neither IDF ground forces nor the Israel Air Force (IAF) had had any first-hand experience against a well-armed opponent such as Hizballah after the country ended its 18-year military presence in Lebanon in 2000. Its only use of force during those 6 years had consisted of recurrent low intensity policing operations against the intifada in the West Bank and Gaza Strip. On the premise that the era of major wars against first-tier Arab opponents was over, at least for the time being, IAF leaders, with ground-force concurrence, had removed their fighters from the close air support (CAS) mission area altogether. There even was a signed contract between the IAF and Israel's ground forces affirming that the latter would provide any needed fire support with their own organic artillery and rockets, leaving the IAF free to concentrate exclusively on whatever independent deep battle missions might be assigned by the General Staff.[1] Throughout the years since the IDF withdrew from Lebanon, it conducted no exercises in which its joint command and control system was tested from top to bottom in a realistic training environment. As a result, ground force preparation for any combat challenges other than countering the intifada had lapsed badly, and operational integration between the IAF and Israel's ground forces had become all but nonexistent.

Not surprisingly in light of that lapse, the IAF encountered numerous challenges in providing effective air support to Israel's ground forces once the campaign against Hizballah shifted from standoff attacks alone to a more joint and coordinated air-land counteroffensive. One problem that persisted throughout most of the campaign had to do with the division of responsibility between the IAF and Northern Command, which oversaw ground operations, for dealing with the enemy's Katyushas and other short-range rockets that rained continually into northern Israel throughout the course of the fighting. In this division of labor, the IAF was the supported command for servicing Hizballah's medium- and long-range rockets, virtually all of which were kept north of the Litani River beyond the area where most of the ground fighting was taking place. For its part, Northern Command was the supported command with primary responsibility for negating the Katyushas and other shorter-range rockets that were stored and operated mainly within its battlespace most closely adjacent to the Israeli border.[2]

Because so much of the war during its last 2 weeks entailed combat in or near built-up villages, there was no fire support coordination line (FSCL) to manage IAF CAS operations in southern Lebanon. However, once the ground fighting got under way, there was a terrain bisector just north of Israel's border with Lebanon that was analogous to the FSCL in its effect on the efficiency of joint operations. At IAF insistence, a "yellow line" paralleling Israel's northern border not far south of the Litani River was drawn on maps used by both services to allow IAF aircrews unfettered freedom to attack Hizballah's medium-range rockets as they were detected and geolocated on the premise that if there were no commingled IDF troops in that battlespace, there would be no need for the IAF to conduct time-consuming prior close coordination of any attacks with Northern Command and its field commanders.[3]

This yellow line occasioned many of the same interservice disagreements regarding the control of joint battlespace that have long plagued American joint combatants at the operational and tactical levels. Yet it was accepted by Northern Command as the most convenient means for deconflicting the respective taskings assigned to Israel's air and land forces. In this arrangement, Northern Command bore responsibility for all targets and operations from the yellow line southward to Israel's northern border. Everything north of the line up to the Litani was the IAF's responsibility as the supported command in the hunt for medium-range rockets. The IAF could only attack identified short-range rocket launch areas south of the line if it received prior permission from Northern Command.

Much as in the case of American kill-box interdiction and CAS inside the roughly similar FSCL during the 3-week major combat phase of Operation *Iraqi Freedom*, a predictable problem arose in the relatively thin band of battlespace between the yellow line and Israel's northern border. Upward of 70 percent of the short-range Katyushas were stored in and fired from this region, yet any attempted IAF operations against them required prior close coordination with Northern Command because IDF troops were also operating in that battlespace. For a time, there was a serious disagreement between the IAF and Northern Command over the placement of the yellow line, with the IAF wanting the line moved southward, as far away from the Litani as possible. Moving the line thusly would enable the IAF to conduct the barest minimum of coordination with Northern Command in the course of its pursuit of time-sensitive targets. Northern Command, for its part, wanted the line placed as far northward as possible, out of an understandable concern that it would otherwise bear the brunt of any criticism that might arise after the war ended for having failed to address the Katyusha threat satisfactorily.[4]

for battlespace management, the IDF used designated kill boxes in a common geographic grid reference system

In the end, Northern Command prevailed in this disagreement. The line was occasionally moved in small increments by mutual consent between the two services, but it mostly remained fixed at around 4 to 5 miles north of the Israeli border, where it embraced most of the terrain in southern Lebanon that contained Hizballah's dispersed Katyushas, yet within which the IAF could not operate without prior coordination with Northern Command. Only toward the campaign's end was the mission of attacking targetable short-range rockets assigned directly to the IAF in the interest of circumventing that

delay in the sensor-to-shooter cycle. Accordingly, only a few short-range rocket storage and launch sites were hunted down and neutralized by either service.[5]

There also was a recurrent struggle between the IAF and Northern Command for tactical control of various IAF CAS assets. One example of such disagreement concerned who should control IAF attack helicopters working with IDF ground units—the IAF or the engaged ground commander? On the books, there was formal joint doctrine for such a situation that the IAF had agreed to regarding the allocation of tactical control. In accordance with that joint doctrine, tactical control of attack helicopters could be delegated by the IAF to a ground commander for 24 to 48 hours. In addition, there was a published provision for the assignment of air liaison officers (ALOs) to IDF formations at the division level who were empowered to approve air support requests from their supported units.[6]

However, such doctrinal contracts on paper often broke down in practice. Habituated almost entirely by its limited base of recent experience in providing on-call CAS in connection with the IDF's relatively slow-motion effort against the intifada, the IAF commander insisted at first on micromanaging air operations at the tactical level so as to ensure the closest possible control over them in the interest of avoiding any untoward collateral damage incidents, much as U.S. Central Command did regarding responsive strike operations conducted from time to time by allied aircraft enforcing the no-fly zone over southern Iraq for nearly a decade.[7]

Israel Air Force

Then–Major General Dan Halutz, Israel Air Force, became Israel's first airman to become IDF chief of staff as lieutenant general responsible for Israel's military forces

As the campaign progressed, however, a consensus gradually developed between the IAF and Northern Command that both attack and utility helicopters should be treated as the ground commander's assets when it came to tactical control and that risk management concerning the commitment of helicopters in the face of enemy fire should be conducted by means of a mutually agreed-upon contract between the engaged ground commander and those helicopter pilots tasked at any moment to work his particular problem. In the end, the IAF concluded that the most effective approach would be to make its helicopters available on demand by the requesting ground commander while retaining operational control of them at all times.[8]

A different situation prevailed, however, when it came to the integration of fixed-wing fighters into the IDF's ground scheme of maneuver. Tactical control of IAF F-15s and F-16s invariably remained the sole prerogative of the IAF's main Air Operations Center (AOC) throughout the war. One of many problems encountered in this particular area of joint operations entailed the use of unfamiliar terms of reference by fighter aircrews and ground combatants. Often the same targets had as many as three different names depending on whose maps were being referred to. Also, the engaged ground commander often would not know whether a requested target had been successfully struck.

The management of airspace directly above the ground fighting worked out reasonably well, despite the presence of as many as 70 aircraft simultaneously operating over southern Lebanon at any time. Regarding helicopters in the lowest altitude blocks, achieving the needed deconfliction turned out to have been simply the result of an eventual IAF decision to stay out of the process. In time, IAF helicopter pilots came to work fairly harmoniously with the ground forces, although ground commanders repeatedly complained about inadequate support from attack helicopters owing to IAF reluctance to employ those aircraft at lower altitudes and closer slant ranges in the face of an ever-present threat posed by enemy antiaircraft artillery and man-portable infrared-guided surface-to-air missiles.[9]

For battlespace management, the IDF used designated kill boxes in a common geographic grid reference system much along the lines of American practice in joint air-ground operations.[10] That approach proved to be problematic at times, however, because ground commanders often lacked a clear picture of their battlespace. For their part, airborne aircrews could never be sure that friendly ground troops were not inside a given kill box. Fortunately, no fratricide occurred as a result of IAF attack operations within kill boxes controlled by Northern Command.

In all, as attested by these and similar examples, most IAF officers would readily agree with the retrospective conclusion that the IDF's "ability to use close air support [had] declined in recent years, largely due to the degeneration of the liaison system that [had been] established in the past between the air force and the ground forces."[11] On this point, the Winograd Commission established by Olmert to assess his government's and the IDF's performance throughout the campaign found that IAF support to ground combat operations had revealed "many flaws" emanating from multiple shortcomings in planning, readiness, and training.[12] It further found that those flaws were the result of conscious prior investment choices by a succession of IDF chiefs to concentrate ground-force readiness almost exclusively toward meeting the immediate needs of combating Palestinian terrorist operations in the occupied territories.

Regarding the air support provided to friendly ground troops during the IDF's war against Hizballah, the commissioners noted "significant deficiencies" in peacetime training for cross-service integration.[13] They also determined that those failings were attributable to the IAF and to the ground forces in equal measure because neither had planned nor exercised the requisite measures for proper air-ground coordination during their normal peacetime training in recent years. For his part, the IAF's commander at the time, Major General Eliezer Shkedy, later explained that a major factor behind this lapse in joint peacetime training was simply the fact that it was "hard for the IAF to practice CAS with a ground force that isn't practicing."[14]

F-16I Sufa multirole fighters participate in training over Nevada

Incorporating Lebanon's Lessons

If there ever was an instance of lessons indicated by a disappointing combat performance becoming truly lessons *learned* and assimilated by a defense establishment in preparation for its next challenge, the IDF response to the insights driven home by its experience during the second Lebanon war offered a classic case of institutional adaptability and self-improvement. The often badly flawed attempts at air-ground integration once the land offensive entered full swing drove home forcefully the fact that each service's expectations of the other were in dire need of adjustment. Those well-intentioned missteps further confirmed that because of their failure to train together over the preceding 6 years, the IAF and Israel's ground forces spoke different languages and had become entities that did not even know each other.

Accordingly, in the early aftermath of the ceasefire in Lebanon, IDF leaders moved with dispatch to assess and correct the revealed deficiencies in joint force readiness that, by then, had come to be widely recognized as having figured prominently in accounting for the war's less than decisive outcome. That comeuppance got the attention of the IAF and Israel's ground forces in equal measure, both of which lost no time in pursuing a better approach to joint combat that would address the identified insufficiencies and in duly preparing the IDF for its next test. As a first order of business, the IDF Directorate of Operations (J-3) organized and led a systematic lessons learned effort that brought together senior leaders from all three services to correct those deficiencies and to revise and update joint tactics, techniques, and procedures.[15]

The IAF also took new looks at its existing practices when it came to seeking better ways of conducting integrated combat operations. Throughout most of the second Lebanon war, General Shkedy had insisted on retaining close control of IAF attack helicopters that were supporting IDF ground operations out of an understandable concern that even a single major tactical error, such as an egregious friendly fire incident, could have a disproportionate strategic downside effect. Yet the inefficiencies introduced into attack helicopter operations as a result of this insistence until the campaign's last days were later acknowledged by all to have been a self-inflicted source of friction that demanded immediate corrective attention.

As another outgrowth of the IDF's disappointing experience, it became apparent to all that the IAF had evolved by that time into two almost separate air arms within the same service—its fixed-wing fighters and its attack helicopter community—in terms of mindset and culture. It also became apparent that a similar divide had come to separate the IAF and Israel's ground forces when it came to their respective techniques and procedures at the operational and tactical levels. The two services planned and trained almost as though the other did not exist. Recognition of this across service lines soon led to a series of joint command post exercises between the IAF and Israel's ground forces aimed at inculcating a new pattern of regular joint contingency planning and training.[16]

One conclusion driven home by the IAF's rocky experience with CAS delivery in Lebanon was the criticality of having an authoritative senior representative attached directly to the commander of all IDF regional land commands as, in effect, the designated head of an Air Component Coordinating Element to the land component. There was often a lack of sufficient understanding by the ground commander of what the IAF could and could not do on his behalf. All too often, the tendency was to ask for a particular platform or type of munition rather than for a desired combat effect. The most important next step toward ameliorating that assessed deficiency was widely seen as the institution of a serious air-ground dialogue on a routine basis in peacetime.

Another lesson highlighted by the ground fighting in southern Lebanon was the need for the IAF to think, plan, and train in closer conjunction with Israel's ground forces. For 6 years, as a result of the IDF's preoccupation with the intifada, the IAF had put itself out of the business of CAS provision and found itself forced to rediscover the most basic principles of the mission as the IDF's operations against Hizballah unfolded. Prompted by that arresting experience, the IAF moved to convene periodic roundtable discussions in the campaign's early aftermath, in which IAF squadron and IDF brigade commanders would engage in capability briefings and solutions-oriented discussion of identified joint issues.

In connection with this unprecedented dialogue, the IAF also flew a select few IDF brigade commanders in the back seats of fighters so they might gain a more intimate appreciation of the strengths and limitations of high performance aircraft in air-land operations. In these repeated instances of searching cross-service engagement, there was little petty parochial swordplay over doctrinal differences and related issues. On the contrary, all participants appeared genuinely committed to forging a more common language and better mutual understanding.[17]

In addition to these initiatives, the IAF, for the first time in 6 years, began a regular regimen of joint training with IDF ground forces. Before long, combat units in both services in ever increasing numbers found themselves training together in live exercises featuring scenarios that often

involved the participation of tanks and other armored vehicles.

As these teachings from the IDF's sobering experience in Lebanon were gradually being assimilated, the Olmert government began redirecting its attention to Hamas as the next regional troublemaker that would eventually require a substantial response by the IDF. That hardcore sect of radical Palestinians who ruled the Gaza Strip as a de facto enemy enclave within Israel's borders had repeatedly fired short-range rockets into southern Israel's population centers in a continuing display of defiant hostility ever since the government of Ariel Sharon voluntarily withdrew both its forces and all civilian Israeli inhabitants from Gaza in 2005.

Finally, in December 2008, the government decided that it had had enough of that sometimes lethal daily harassment and chose to proceed with a determined effort to put an end to it. By that time, both the IAF and IDF ground forces were ready with a new repertoire that had been carefully honed through repeated joint planning efforts and large-force training exercises over the preceding 2 years.

A Better Showing in Gaza

The IDF counteroffensive against Hamas, code-named Operation *Cast Lead*, began on the morning of December 27, 2008, with an air-only phase that lasted 8 days. The campaign next featured an air-supported ground assault into the heart of Hamas's main strongholds in the Gaza Strip, followed by an endgame consisting of a unilateral ceasefire declared by Israel on January 18, which Hamas honored with a reciprocal ceasefire announced 12 hours later. Repeatedly throughout the air-land portion of the campaign, IDF ground maneuver elements supported the IAF rather than the other way around by shaping Hamas force dispositions and thereby creating both targets and a clear field of fire for IAF fighters and attack helicopters.[18]

At both the operational and tactical levels, the extent of cross-service cooperation displayed by the IAF and IDF land forces was unprecedented when it came to the integration of unmanned aerial vehicles (UAVs) and attack helicopters with the ground scheme of maneuver. This greatly improved performance was a direct result of the heightened interaction between the two services that had first developed during the early aftermath of the second Lebanon war.

During Operation *Change of Direction*, IAF attack helicopters and UAVs had been under the tactical control of the IAF's forward AOC collocated with Northern Command until almost the very end. In Operation *Cast Lead*, those assets were now instead directly subordinated to IDF brigade commanders, with each now able to count on dedicated, around-the-clock support from them on request.[19] By the time the counteroffensive against Hamas had become imminent, the IAF attack helicopter force has essentially become army aviation in the manner in which it was employed.[20]

the brigade headquarters enjoyed substantial autonomy from higher headquarters both at Southern Command and in Tel Aviv

For the first time in Operation *Cast Lead*, the brigade headquarters was the nerve center of combat activity, and it enjoyed substantial autonomy from higher headquarters both at Southern Command and in Tel Aviv. Regarding air operations, the brigade headquarters controlled all IAF attack helicopter and UAV assets, along with some F-15s and F-16s. To ensure the most effective exploitation of airpower in support of ground operations, the ground commander, an IDF brigadier general, had constantly at his side an IAF colonel who saw to the uninterrupted provision of direct air influence on the planning and conduct of combat operations. The supporting presence of other IAF officers in the brigade headquarters further contributed to the enhancement of trust and understanding between Southern Command's air and land components.[21]

In addition to these improved arrangements at the brigade headquarters level, every participating ground-force brigade had an embedded Tactical Air Control Party (TACP) comprising five IAF team members who sorted raw information and converted it into actionable intelligence for time-critical targeting. Each TACP included both an attack helicopter pilot and a fighter pilot or weapons systems officer as assigned ALOs. TACP members also coordinated CAS attacks and deconflicted the airspace over each brigade's area of operations.

Each brigade also now had the support of a dedicated attack helicopter squadron, which provided a pilot to the TACP who communicated with airborne attack helicopter aircrews. To reduce the workload on brigade commanders and on Air-Ground Coordination and Cooperation Unit at IAF Headquarters, TACP members were authorized to call in air support on their own initiative. ALOs also had constant access to real time streaming UAV imagery. New operating procedures allowed attack helicopters to deliver fire support in some cases to within 100 feet of friendly troop positions.[22]

To be sure, IAF attack helicopters retain an independent deep-strike responsibility for which they remain under the tactical control of the IAF commander. When their immediate tasking is on-call CAS, however, they are now controlled directly by those brigade commanders who are the intended beneficiaries of their support.[23] In a clear response to its lessons learned from Lebanon, IAF leadership consented to assign to each involved brigade a TACP including at least one terminal attack controller with the rank of major or lieutenant colonel to ensure that all would have their own dedicated fighter, attack helicopter, and UAV support. As a result of this changed IAF mindset, the application of airpower in integrated air-land operations, which had been centralized in the IAF's main AOC throughout most of the second Lebanon war, was now pushed down to the brigade level and, in some cases, even lower.[24]

Furthermore, during the IDF's counteroffensive against Hizballah in 2006, the IAF commander's personal approval had been required for IAF aircrews to conduct CAS in so-called danger close conditions, meaning that friendly forces were 600 meters or less from a designated target. In the subsequent Gaza operation, IAF terminal attack controllers assigned to engaged ground units were cleared to grant that approval, which naturally entailed a great deal of personal responsibility on their part.[25] Also, in a major departure from its practice throughout the second Lebanon war, the IAF's main AOC this time was completely out of the command-and-control loop other than for transmitting rules of engagement and special instructions to participating IAF aircrews. Most nonpreplanned targets were now nominated by IDF brigade commanders.

In all, the IDF showed in its conduct of Operation *Cast Lead* that it had ridden a clear learning curve from the second Lebanon war to Gaza when it came to refining an effective air-land battle repertoire. In the lead-up to its campaign against Hamas, the IDF, having drawn the right conclusions from its earlier experience in Lebanon, envisaged a joint campaign from the first moments of its options planning. It further showed a willingness to run greater risks by putting attack helicopters into airspace above hot areas on the ground that were concurrently being serviced by bomb-dropping fighters, thereby increasing the effectiveness of its CAS efforts. It also went from providing on-call CAS to offering up proactive CAS, in which the IAF took the initiative by asking, via daily phone conversations with the engaged brigade commanders, what they needed rather than waiting passively for emergency requests for on-call CAS from IDF troops in actual contact with enemy forces.[26]

For their part, IAF aircrews found their exertions in actual combat to have been relatively undemanding, thanks in large part to their earlier cooperative training with IDF ground forces that familiarized them beforehand with virtually any friction point that might arise. After it was over, CAS delivery by the IAF was uniformly adjudged to have been more than satisfactory, reflecting a clear payoff from the intensified joint training and associated cross-service trust relationships that the IAF and IDF had both cultivated during the 2 years that followed the end of the second Lebanon war.[27]

So What for Us?

As for its teaching value for the U.S. joint community, the successful IDF response to its disappointing performance in Lebanon in 2006 showed convincingly how an adaptive military organization determined to improve its readiness and repertoire can muster the needed wherewithal not only to identify and understand but also to learn and profit from lessons offered by a flawed but instructive combat experience. With respect to the opportunity costs incurred by the IDF's excessive fixation on the intifada until corrective measures were introduced, there is a cautionary note here for all U.S. leaders who would continue deferring needed investment against potential near-peer challengers in years to come in order to concentrate all of our limited defense resources against the country's lower intensity counterinsurgency preoccupations of the moment.

By the same token, on the force-employment front, the IDF's proven approach toward ensuring the fullest possible exploitation of airpower during its subsequent Gaza campaign 2 years later has direct relevance to continuing U.S. combat operations in Afghanistan. It is testimony to the need for decentralized control of air assets against hybrid opponents such as the Taliban, along with a duly empowered air command and control entity below the level of the AOC staffed by airmen of appropriate rank and experience to provide effective air influence in joint warfare at the tactical level.[28] The IDF's Gaza experience further bore witness to the merits of getting the most skilled and credible air operators out of the AOC and deployed forward as ALOs working directly with those on the ground in need of on-call air support in the sort of fourth-generation warfare that has been the principal form of American joint force engagement since the end of major combat in Iraq in 2003. **JFQ**

NOTES

[1] Interview with Brigadier General Yohanan Locker, Israel Air Force (IAF), Tel Nof Air Base, Israel, March 29, 2009.

[2] David A. Fulghum and Robert Wall, "Learning on the Fly: Israeli Analysts Call for More Flexibility and Renewal of Basic Combat Skills," *Aviation Week & Space Technology*, December 3, 2007, 63–65.

[3] Interview with the Head of the IAF's Campaign Planning Department during Operation *Change of Direction*, Tel Nof Air Base, Israel, March 29, 2009.

[4] Fulghum and Wall, 63–65.

[5] Major General Isaac Ben-Israel, IAF (Res.), *The First Israel-Hezbollah Missile War* [in Hebrew] (Tel Aviv: Tel Aviv University, May 2007), 64.

[6] Interview with the Head of the IAF Campaign Planning Department, IAF Headquarters, Tel Aviv, March 26, 2008.

[7] For further discussion on the latter count, see Michael Knights, *Cradle of Conflict: Iraq and the Birth of the Modern U.S. Military* (Annapolis, MD: Naval Institute Press, 2005), 213–217.

[8] Interview with Brigadier General Gabriel Shachor, IAF, Palmachim Air Base, Israel, March 27, 2008.

[9] Alon Ben-David, "Israel Introspective after Lebanon Offensive," *Jane's Defence Weekly*, August 23, 2006, 18–19.

[10] For a concise description of that U.S. practice, see Colonel Robert B. Green, USAR, "Joint Fires Support, the Joint Fires Element and the CGRS [Common Grid Reference System]: Keys to Success for CJSOTF West," *Special Warfare*, April 2005.

[11] Colonel Gabriel Siboni, IDF (Res.), "The Military Campaign in Lebanon," in *The Second Lebanon War: Strategic Perspectives*, ed. Shlomo Brom and Meir Elran, 65 (Tel Aviv: Institute for National Strategic Studies, 2007).

[12] "Arms, Combat Support Units, and Special Operations," in *Final Winograd Report on the Second Lebanon War* (Reston, VA: Open Source Center, February 2008); see also "The Air Force, Lessons," ibid., para. 30. The Winograd Commission was named for its appointed chairman, Judge Eliahu Winograd, a retired president of the Tel Aviv District Court.

[13] "Recommendations for the IDF," in *Final Winograd Report*.

[14] Interview with Major General Eliezer Shkedy, IAF Headquarters, Tel Aviv, March 27, 2008.

[15] Barbara Opall-Rome, "Interview with Major General Eliezer Shkedy, Commander, Israel Air and Space Force," *Defense News*, May 19, 2008.

[16] Interview with Brigadier General Yohanan Locker, IAF, Tel Nof Air Base, Israel, March 29, 2009.

[17] Interview with Brigadier General Ya'akov Shaharabani, IAF Headquarters, Tel Aviv, March 31, 2009.

[18] "Operation 'Cast Lead': IAF Missions and Operations," briefing charts provided to the author by Brigadier General Nimrod Sheffer, IAF, Head of the Air Division, IAF Headquarters, Tel Aviv, March 31, 2009.

[19] Barbara Opall-Rome, "Major General Ido Nehushtan, Commander, Israel Air and Space Force," *Defense News*, August 3, 2009, 30.

[20] Interview with Colonel Meir (last name withheld), Commander, Doctrine Department, IDF Ground Forces, at an IDF installation near Tel Aviv, March 30, 2009.

[21] *The 2008/09 Gaza Conflict—An Analysis*, RAF Waddington (United Kingdom: Air Warfare Centre, The Air Warfare Group, 2009), 5, 7.

[22] David Eshel and David A. Fulghum, "Two Steps Forward . . . Israeli Technologies and Coordination Detailed in Gaza Strip Combat Analyses," *Aviation Week & Space Technology*, February 9, 2009, 61.

[23] Interview with Brigadier General Gabriel Shachor, IAF (Res.), Palmachim Air Base, Israel, March 31, 2009.

[24] Interview with Major General Eliezer Shkedy, IAF (Res.), Tel Aviv, March 26, 2009.

[25] Interview with the commander of 160 Squadron, Palmachim Air Base, Israel, March 31, 2009.

[26] Ibid.

[27] Interview with the former deputy commander of 105 Squadron during Operation *Change of Direction*, Palmachim Air Base, Israel, March 31, 2009.

[28] For a further development of this point, see the informed and thoughtful commentary by Lieutenant Colonel Jeffrey Hukill, USAF (Ret.), and Daniel R. Mortensen, "Developing Flexible Command and Control of Air Power," *Air and Space Power Journal* (Spring 2011), 53–63.

U.S. Air Force (Rusty Baker)

F-35 Joint Strike Fighter

AIRPOWER DOLLARS AND SENSE

RETHINKING THE RELATIVE COSTS OF COMBAT

By LEE T. WIGHT

Since the end of the Cold War and the realization that few adversaries can compete directly with American conventional military power, the term *asymmetric warfare* has become a staple of the contemporary lexicon. Yet asymmetric warfare is hardly a new concept. Ever since man learned that a club improved his ability to batter his fellow man, he has sought an asymmetric edge over his opponent. Once aviation was added to the military arsenal, visionaries imagined bypassing the indecisiveness of trench warfare to strike directly at the heart and home of the enemy. Giulio Douhet and Billy Mitchell took the concept further—possibly to airpower's immediate detriment—and argued airpower alone could win wars, igniting a debate which rages unchecked to this day.[1] This article illustrates how history has rendered the "decisiveness" argument moot and studies eight contemporary military operations—half of them land-centric and half air-centric—in terms of their relative "costs" (see table). It then makes prescriptive recommendations for future American policy based on airpower's apparent lower "costs" and its potential ability to enable indigenous ground forces.

Can Airpower Be Decisive?

A reasonable but critical analyst might argue that airpower's ability to win wars depends heavily on the nature of the adversary, objectives of the conflict, and capabilities at hand. For example, he could argue that air-delivered nuclear weapons proved decisive in ending the World War II conflict with Japan. Others may argue that even absent an invasion of the Japanese homeland, the Japanese would have eventually collapsed from the combined effects of Curtis LeMay's firebombing campaign and the starvation being forced on the Japanese people by the air and naval blockade of their islands. Contemporary airpower theorists such as John Warden would argue that airpower can be decisive against an adversary led by a single charismatic individual or leadership group by decapitating the leader(s), resulting in a collapse of the organization.[2] Regardless, there are those who maintain airpower alone cannot ever be decisive and its primary purpose is to provide supporting fires, intelligence, and mobility to the land elements that must close with the enemy to achieve victory.

Logically, objectives are the key to determining when victory is achieved. If conquering a country or retaining territorial integrity is the objective, significant land forces will likely be required. If regime change is the objective, however, can that be achieved without the physical occupation of an enemy's territory by American forces? Recent events in Libya confirm this potential, while Kosovo and Operation *Enduring Freedom* in Afghanistan offer earlier but similar precedents. Although the specified objectives of *Enduring*

Colonel Lee T. Wight, USAF, is Chief of the Air Force Strategy Division (A8XS) on the Air Staff at the Pentagon.

Comparison of Recent U.S. Air- and Land-centric Military Operations

Conflict	Type	Duration	Direct Costs (FY10$)[1] (M: million; B: billion; T: trillion)	U.S. Casualties[2] (D: dead) (W: wounded)	Civilian Casualties[3] (estimated)	Strategic Objective(s)[4]	Objectives Achieved?
Vietnam	Land	1956–1975	$677B–$1.04T	58,236(D)/153,452(W)	486,000–1,200,000	Preserve government of South Vietnam	No
Panama 1989 (*Just Cause*)	Land	7 days	$287.5M	23 (D)/322 (W)	500	Regime change	Yes
Iraq 1991 (*Desert Storm*)	Air	42 days	$97.7B	148 (D)/467 (W)	1,000–5,000	Liberate Kuwait	Yes
Kosovo 1999 (*Allied Force*)	Air + Indigenous ground	78 days	$19.6B	0 (D)/0 (W)	500–5,000	Stop ethnic cleansing	Yes
Afghanistan 2001–2003 (*Enduring Freedom I*)	Air + Indigenous ground	2001–2003	$42B[5]	109 (D)/137 (W)	3,100–3,600	Regime change/ destroy terrorist infrastructure	Yes
Iraq 2003 (*Iraqi Freedom*)	Land	2003–2011	$800B	4,400(D)/32,000(W)	34,832–793,663	Regime change/foster democracy, liberal values	Yes/ Unknown
Afghanistan 2004 (*Enduring Freedom II*)	Land	2004–2014?	~$958B[6]	~2,160(D)/~20,000 (W)[7]	10,960–46,000[8]	Foster democracy/ liberal values	Unknown
Libya 2011 (*New Dawn/ Unified Protector*)	Air + Indigenous ground	8 months, 8 days	$1.1B	0 (D)/0 (W)	9–85[9]	Protect civilians/ regime change	Partially/ Yes

1. All costs are approximate as referenced in the text and converted to fiscal year 2010 dollars using previously described methodology.
2. Numbers are for U.S. forces only, although coalition/friendly forces generally suffered losses also, but at lower rates. Breakouts by nationality are available at Web sites *icasualties.org* and *wordIQ.com*. Fatalities are combat-related only, where available. Most wounded numbers do not specify origin of the injury, but are presumed to be combat-related.
3. Numbers are estimated as cited and described in the text. They include postulated minimum and maximum numbers and are those attributed to U.S./coalition military combat operations, not those due to ethnic cleansing, civil war, disease outbreaks, and so forth, even though those may be related.
4. Although complete objectives are detailed in the text, this table illustrates only the major specified or implied strategic objectives.
5. "Estimated War-Related Costs, Iraq and Afghanistan," November 22, 2011, available at www.infoplease.com/ipa/A0933935.html.
6. Estimated through 2014, less 2001–2003 costs previously referenced.
7. Estimated numbers if present trends continue through 2014, less approximate Operation *Enduring Freedom* numbers for deaths.
8. Actual high estimate is 49,600 corrected to account for Operation *Enduring Freedom* figures cited in the same estimate.
9. Nazish Fatima, "NATO accused of having minimized civilian casualties in Libya," *AllVoices.com*, May 14, 2011.

Freedom were aimed at removing the Taliban's military capability, removing the regime from power was at least an implied objective immediately following the 9/11 terror attack on the U.S. homeland. These objectives were successfully completed using airpower to back indigenous ground forces (the Northern Alliance) supported by a cadre of U.S. special forces.[3] What if the objective of combat is forcing a regime to alter such policies as committing genocide or acquiring nuclear weapons? North Atlantic Treaty Organization (NATO) air operations over Kosovo were an example of the former during Operation *Allied Force*, while Israeli air raids on both Iraqi and Syrian nuclear facilities[4] were airpower approaches to the latter. Certainly a strong argument could be made that airpower was the most significant, if not completely decisive, contributor to expelling Iraqi forces from Kuwait during Operation *Desert Storm*.[5]

What about Land Forces?

Even casual observers of current events are aware of several recent land-centric approaches to regime change for affecting an adversary's strategic decisionmaking. Forcible regime change using a U.S.-led ground force (although supported by the full spectrum of joint fires including a large air component) was accomplished during Operation *Iraqi Freedom* and led to an even larger American land force presence in support of subsequent stability operations.[6] The 2005 Taliban resurgence in Afghanistan eventually led to a significant expansion of American, NATO, and other coalition land forces deployed there, resulting in a "surge" to over 150,000 land troops to interdict the terror networks of al Qaeda and its affiliates, while setting conditions for the return of security and governance to the Afghans in support of the current version of Operation *Enduring Freedom*.[7] By contrast, Operation *Just Cause* featured a relatively small U.S. land force of approximately 21,000, supported lightly by airpower, to rapidly effect regime change in Panama by capturing Manuel Noriega.[8] As all


U.S. Air Force (Christopher Bush)

B-2 Spirit

of these examples illustrate, under the right circumstances, either predominantly air- or land-centric operations can be successfully used to achieve national military objectives.

The Limits of Military Power

Everything has its limits. Military power is certainly not an exception to this rule. In all of these studied operations, military forces achieved operational objectives. Even in Vietnam, U.S. forces won almost every significant military engagement. As history has shown, though, tactical military victories failed to achieve the strategic political objective of preventing the fall of the South Vietnamese government. While the *Just Cause* operations appear to have been successful on both military operational and political strategic levels, other examples are less clear cut. *Desert Storm* is generally regarded as an overwhelming military success; however, it is debatable whether the stated national policy objectives of "ensuring the security and stability of Saudi Arabia and other Persian Gulf nations" and "[ensuring] the safety of American citizens abroad"[9] are achievable by any military means, let alone whether or not *Desert Storm* air and land operations contributed positively or negatively to either of them. Likewise, while the military was able to end the regime of Saddam Hussein during *Iraqi Freedom*, defending the American people requires more than an invasion of Iraq, an action that history may ultimately judge as indecisive.[10] *Enduring Freedom* operations share the same challenge. Terrorist operations and training camps in Afghanistan have certainly been disrupted since October 2001, but the cessation of all terrorist operations in Afghanistan is something that is likely beyond the potential of military operations to achieve.[11]

Notably, this article lists cases in which both air- and land-centric military operations have achieved their objectives, as well as several in which success has been or may prove elusive. While success is certainly possible, one should also recognize that either form may also prove indecisive or fail entirely. This article does not intend to argue that one form of warfare can prove more decisive than the other. Astute policy analysts recognize there are some tasks unsuitable for military actions alone that must involve other levers of national power in order to have real potential to succeed. Therefore, we turn to the central thesis of this article, a comparison of the relative costs of land- versus air-centric operations—independent of their potential or actual success.

What Do Military Operations Cost?

Those who continue to debate whether air-centric operations can be successful risk being labeled pedantic or parochial and miss the point entirely in today's financial climate. Former President Bill Clinton famously stated, "It's the economy, stupid!" In the current budget environment, that statement could equally apply to military operations. With the U.S. deficit at a record $15 trillion,[12] the Department of Defense is already executing approximately $400 billion in cuts. At least that much more is anticipated for the next 10 years, especially now that the congressional budget "super committee" has failed to reach agreement. Fiscal issues have become one of the most critical calculi for military and political decisionmakers today.

Money aside, there are other costs to military operations. Traditional statecraft measures military actions in terms of the cost to the nation in "blood and treasure." Whether the cost in terms of blood in this context refers directly to deaths, injuries, or long-term rehabilitation, war always has a human toll. These human and economic costs, combined with the conflict's duration and perceived effect (or lack thereof) on the American public, shape what is often described as the U.S. "center of gravity"—public opinion. Indeed, in a democracy, this ultimately determines how long the government will remain engaged in a conflict. Thus, with our definition of *cost* as national blood and treasure, this article first compares recent land- and air-centric military operations to determine which might be considered more cost effective in the national interest.

Costs of Land Operations

Looking first to Iraq (Operation *Iraqi Freedom*), where the U.S. presence has recently been declared over by President Barack Obama,[13] the most frequently advanced dollar cost estimates are in the neighborhood of $800 billion, although some observers note ongoing medical treatment and replacement equipment could bring the eventual total to over $4 trillion.[14] Total U.S. casualties number around 32,000 over a period of almost 9 years, including approximately 4,400 deaths.[15] In terms of objectives, a tyrant was removed, the Iraqi people were liberated, and Iraq did not

acquire nuclear weapons. Long-term stability, by any observer's estimate, is fragile at best and whether the state ultimately survives intact is anyone's guess. Assessing whether the invasion achieved the stated objective of defending the American people has been widely debated and is much more difficult to assess.

Operations in Afghanistan (*Enduring Freedom*) continue, and if American forces remain as projected until at least 2014, it will have taken 13 years in total (albeit several of those years were low intensity while operations were focused in Iraq), and if trends continue, it will cost upward of $1 trillion, approximately 2,300 deaths, and approximately 20,000 wounded.[16] While it is imprudent to assess objectives from an operation yet to be completed, so far thousands of terrorists have been killed and the Taliban have certainly been removed from leadership of the government. Yet they are still present in the country, remain active, and may eventually be reincorporated into the government (by Afghan choice). Much like Iraq, a crystal ball is needed to determine whether democracy, rule of law, and human rights will ultimately bloom from the seeds planted by the International Security Assistance Force, and doubters will continue to cite the strong tribal structure of Afghanistan and limited history of an effective or accepted national government.[17]

The proverbial elephant in the room in terms of these types of large, land-centric occupations is, of course, Vietnam. Almost 20 years of conflict there cost approximately 60,000 U.S. Servicemembers killed or missing and over 303,000 wounded. Direct dollar cost estimates vary between $130 and $200 billion (approximately $677 billion and $1.04 trillion in 2010 dollars),[18] with an approximate indirect dollar cost at least equaling that in terms of rehabilitation, debt interest, and payments to veterans and their families.[19] Despite this investment and the valor of those involved, in the final analysis, the effort failed to prevent the South Vietnamese government from falling.[20] In fairness, however, success or failure of the "proxy war" against the Soviet Union must be judged in the context of the eventual U.S. Cold War victory and subsequent collapse of the Soviet empire. Whether or not the will of the United States to engage in Vietnam at that cost ultimately affected the outcome of the larger strategic contest must be considered but can never be proven.

A much easier example to assess is the 1989 U.S. intervention in Panama (Operation *Just Cause*). There, approximately 20,000 ground troops, supported to some degree by airpower, engaged in a week-long operation to capture Manuel Noriega. At a cost of 23 U.S. troops killed, approximately 322 wounded, several helicopters lost,[21] and approximately $163.6 million in direct costs[22] (estimated to be approximately $287.5 million in 2010 dollars),[23] regime change occurred. Noriega was captured, and after serving prison sentences in the United States and France, has been returned to Panamanian custody to face additional charges for allegedly murdering political opponents.[24] After the intervention, the United States additionally pumped several billion dollars into the Panamanian economy to facilitate recovery.[25]

Costs of Air Operations

Turning to air-centric operations, the opening stages of *Desert Storm* consisted of over a month[26] of airstrikes, credited with so gutting the Iraqi ground forces that they placed "Iraq in the position of a tethered goat," according to the war's air boss, General Charles Horner, USAF.[27] A land force built around 17 divisions and approximately 500,000 coalition soldiers and marines required only 100 hours to expel the decimated Iraqi forces from Kuwait.[28] During the operation, 20 airmen were lost (14 battle-related), and there was a total of 293 U.S. fatalities (148 battle-related fatalities) with 467 wounded.[29] When President George W. Bush announced the operation complete, all Iraqi forces had been withdrawn from Kuwait, the legitimate government of Kuwait was restored, and the security and stability of Saudi Arabia and other Persian Gulf nations were ensured for the near term.[30] Cost estimates in this case are difficult to determine, as multiple nations participated and some costs were eventually reimbursed to the United States; regardless, direct U.S. costs are estimated to have been between $47.5 and $61 billion with the General Accounting Office estimating total costs at approximately $61.1 billion[31] (approximately $97.7 billion in 2010 dollars).

Kosovo (*Allied Force*) took 78 days of combat operations, with the loss of an F-16, an F-117, and zero U.S. lives, and is estimated to have cost £2.63 billion (approximately $4.2 billion) in direct costs for all NATO military forces, with an estimated total cost of £31.67 billion (approximately $50.67 billion), including aid, follow-on peacekeeping, and reconstruction.[32] The direct U.S. cost was approximately $15 billion (approximately $19.6 billion in 2010 dollars), not including subsequent foreign aid and peacekeeping costs.[33] Since 1999, the United States has provided over $1.2 billion in assistance for Kosovo reconstruction, restoring self-governing institutions, and a viable economy.[34] At the conclusion of NATO combat operations, Serbian forces were driven out of Kosovo and Serbian President Slobodan Milosevic unconditionally accepted the peace terms presented by European Union and Russian envoys.[35] Milosevic was subsequently arrested in 2001 for war crimes, tried in The Hague, and eventually died in custody.[36] Similar to recent NATO operations in Libya, an indigenous ground force aided by NATO airpower gained effectiveness toward the end of the operation and may have contributed in part to Milosevic's eventual capitulation.

Turning to the post-9/11 response to al Qaeda in Afghanistan (*Enduring Freedom*), the air-centric portion of the operation, where the United States enabled the Northern Alliance forces with support from U.S. and British special forces on the ground, ran from approximately October 7, 2001, through the start of Operation *Anaconda* in March 2002,


U.S. Air Force

Billy Mitchell

when significant U.S. ground forces began to be introduced—although the operation officially ran through May 2003 when Secretary of Defense Donald Rumsfeld announced the end of Afghan combat.[37] Its original objectives were the destruction of terrorist training camps and infrastructure in Afghanistan, capture of al Qaeda leaders, and cessation of terrorist activities in Afghanistan.[38] As a result of these actions, the Taliban were driven from power and al Qaeda operations were significantly disrupted, although Osama bin Laden survived in Pakistan until 2011. During the operation, approximately 140 total coalition casualties were suffered through the end of 2003, with 109 of them U.S. lives lost.[39] Costs to date are estimated at $443 billion along with 1,523 U.S. military lives lost.[40] Overall, of course, the results remain a work in progress and history will judge their eventual success or failure.

In the example du jour—Libya—airpower protected, to a degree, the civilian populace from slaughter by Muammar Qadhafi's supporters, enabled regime change, and facilitated the overthrow of Qadhafi himself (whether or not that was a specified objective of the operation). The cost was zero American or NATO lives lost, one F-15E lost, and about $1.1 billion in direct costs over the course of the 8-month conflict.[41] One relatively unique aspect of the Libya operations was the rapid handover of combat operations to NATO, placing the United States in an active but supporting role.[42]

Adding Up the Costs

A review of these land- and air-centric operations shows fairly clearly that some costs are an "apples to oranges" comparison—so different in some cases that one might say an "apples to transmissions" analogy is more apt. As far as monetary or treasure costs go, in some cases, units failed to document them to such an extent that even the General Accounting Office was unable to accurately determine costs.[43] In other cases, costs were reimbursed (or planned to be reimbursed) by other nations.[44] Whether or not the U.S. Government ever received full reimbursement, or goods or services in exchange, is likewise difficult to decipher. Furthermore, some cost reports only include direct costs, while others are "total" costs.

Deciding the total cost of an operation is somewhat subjective, as one has to draw a line at some point regarding veteran's compensation, survivor and social security benefits, reconstruction, and foreign aid. Some of these factors are never completely known or they continue to develop through the lifespans of those who participated in the operation. Total costs, in theory, would also include all of the research and development costs of the weapons systems and equipment used, along with the weapons themselves, as well as the training, education, and accession costs of the personnel who employ them.

Furthermore, all costs must be normalized for the effects of inflation in order to provide a relevant basis of comparison. For operations spanning several years—such as Vietnam, Iraq, and Afghanistan—direct and indirect costs for each year of the operation would have to be calculated and similarly adjusted to arrive at a total cost—a project worthy of its own study.

After considering all of the above factors, it becomes apparent that when comparing the relative costs in terms of treasure, the most useful monetary metric is the generalization that dollar costs increase as a function of the time required to complete the operation and the amount of American forces committed to the fight. Generally speaking, as supported by each of the cases considered in this article, we can conclude that shorter duration operations cost less financially. As previously noted, time may also be relevant—but not necessarily decisive—in terms of its effect on U.S. public opinion. The American public has supported long-duration conflicts: almost 20 years in the case of Vietnam and over 20 years combined in Iraq and Afghanistan. The most costly operations have included large American ground forces. In this context, airpower has generally been able to achieve results significantly faster, and thus was less costly in terms of treasure than were land-centric means. No rule is without its exception, however, as the land-centric Operation *Just Cause* required only a week for completion.

airpower has been able to achieve results significantly faster, and thus was less costly than land-centric means

Another aspect to consider is the long-term sustainability of the changes implemented by the military operations. The gains in Iraq are fragile, nascent, and easily reversible, as they also appear to be in Afghanistan to date. A counterargument to extended American presence is the development of a perceived dependence on the United States so long as its forces perform security and governance tasks for a population that is either uncommitted or ambivalent to the changes (at least from a liberal, human rights, and democracy perspective). As with the experience in Vietnam, there is a strong possibility that many if not all of these changes may fail upon the complete withdrawal of U.S. forces. While it is again far too early to tell, there is a strong argument to be made that in airpower-centric actions where airpower enabled an indigenous ground force (Kosovo, Libya, *Enduring Freedom*), ground forces had more of a personal stake in the outcome because they shared in both the sacrifice of combat and the fruits of victory. They also remain long after U.S. or other foreign combat forces are withdrawn—leading to a higher level of commitment to the changes for which they fought and potentially making them more sustainable over the long term. One could also make the argument that even if the operations ultimately prove indecisive, whether spearheaded by either air- or land-centric means, the lower cost operations would still be a better choice from an American perspective.

Additionally, the supporting role template used in Libya may also have the benefit of reducing indirect reconstruction and rebuilding costs. In a U.S.-led operation, there appears to be a long-term sense of ownership of the problem, similar to the retail "you break it, you buy it" mantra. As previously documented, all U.S.-led air- or land-centric operations have entailed significant reconstruction costs. However, in Libya, there does not appear to be the same sense. The U.S. decision to yield political leadership of the NATO-sponsored operation to the United Kingdom and France (while still providing the bulk of the support, enabling operations, and initial strikes) may reduce the long-term costs to U.S. taxpayers.[45]

Although attempting to reconcile the financial costs of these operations is difficult, this study does make abundantly clear that

U.S. Air Force (William Greer)

A-10 Thunderbolt

in terms of blood costs, airpower-centric operations have been dramatically cheaper for friendly forces. Despite the tremendous reduction in land force casualties from Vietnam (approximately 60,000 killed) compared to either Iraq or Afghanistan (approximately 6,200 total killed to date), these reduced casualties pale in comparison to the combined costs of the air-centric operations of Kosovo, *Enduring Freedom*, and Libya, which featured an unprecedented loss of zero U.S. or NATO lives. From an airpower perspective, *Desert Storm* only took the lives of 14 aviators in battle-related deaths, for a loss rate that was "lower than normal training" according to General Horner.[46] By comparison, even the shortest land-centric operation studied here, *Just Cause*, cost 23 killed and over 320 wounded.[47] To put that in perspective, less American blood was spilled in four complete air-centric operations, totaling over 3 years of combat, than was lost in a single, 1-week land-centric conflict.

A critic might argue that these low casualty figures were the result of the air-centric conflicts occurring against an opponent that was unable or unwilling to directly face American airpower. The ultimate ease of the coalition victory in *Desert Storm* tends to obscure the fact that prior to 1990, Iraq had the world's fifth-largest military, including a substantial and integrated air defense, and had added so much capability it was described as "the world's largest arms market,"[48] making it the largest military in the Middle East, including over 700 modern military aircraft.[49] Furthermore, the Soviet-trained Serbian air defenses were highly capable, effectively integrated, and, for the most part, willing to fight. In fact, NATO never gained air supremacy and suffered the loss of one of its most technologically sophisticated aircraft—a "stealth" F-117.[50] Even Afghanistan had air defenses that troubled the Soviets during their occupation.[51] That American airpower achieved such incredible results in those conflicts at such a low cost in blood and the fact that other adversaries chose to concede air dominance rather than fight is exactly the point. American airpower is a tremendous asymmetric advantage and has proven that it can achieve results at costs other means cannot match.

Everyone Matters

When coldly calculating the "military" costs of an operation, it can be easy to overlook the fact that noncombatants traditionally pay an equally heavy or even heavier cost in blood than the military participants on either side.[52] While accurate civilian casualty statistics are notoriously difficult to obtain and their interpretation is wildly speculative, the "faster is better" mantra related in this article regarding the cost of military operations also appears relevant in terms of reducing civilian casualties—regardless of the predominantly air- or land-centric nature of the combat.

Considering short-duration operations on one hand, the week-long land-centric invasion of Panama reportedly caused about 500 civilian casualties.[53] A similar figure is noted by Human Rights Watch for *Allied Force*, although other estimates range between 1,200 and 5,000.[54] Another relatively short-duration combat operation, *Desert Storm*, resulted in civilian deaths allegedly ranging from 1,000 to 5,000.[55] The standard-bearer for low civilian casualties, however, may be the recently concluded Libya operation, in which only a few civilian deaths were reported as a result of NATO combat.[56]

On the other hand, as one might predict, longer duration operations tend to have significantly higher associated civilian casualty figures. While again subject to a wide number of estimations, Afghanistan civilian death figures are placed by one source at approximately 2,777 in 2010 alone, although the U.S. military has been fighting there since 2001.[57] This casualty figure is similar to the total estimated for the duration of *Desert Storm*. Furthermore, the numbers for *Iraqi Freedom*, where a low estimate of 34,832 dead to a high estimate of 793,663,[58] and Vietnam, with estimates ranging from 486,000 to over 1.2 million fatalities, illustrate the far end of the spectrum.[59] Interestingly, the Iraq and Afghanistan data are especially

telling, inasmuch as coalition forces have placed an especially high priority on avoiding such casualties and friendly combatants are using the latest in precision weaponry under very strict rules of engagement.[60]

Thus, despite all efforts to reduce the potential for harm to civilians, it appears almost inevitable that some will die as collateral damage of military conflicts. However, the data reviewed here appear to support the proposition that generally speaking, shorter conflicts can reduce the number of civilian casualties. If airpower indeed can shorten a conflict, then it can also reduce the cost in terms of civilian blood indirectly involved in these hostilities.

Implications

Returning to President Clinton's exhortation about the economy and looking at the bottom line, the inescapable conclusion is that airpower—in terms of blood and treasure as defined in this article and under certain circumstances—while not the sole answer to all military problems, can provide cheaper and generally more rapid solutions to many national security challenges. Moreover, when used to enable indigenous ground forces, such an approach may lead to greater indigenous commitment and a more enduring outcome. An airpower-centric approach may also offer less long-term entanglement, reducing the perceived need for the United States to effectively buy the broken country for an extended reconstruction period.

It is worth restating this does not mean that airpower is a panacea for all political ills, or does it mean that it provides an absolute guarantee against any future American or civilian loss of life. It is also critical to note that senior decisionmakers may not always have a choice to employ air or ground forces exclusively. The nature and makeup of forces required will always depend on the desired objectives and the situations at hand. Capable indigenous ground forces may not always be available to be enabled by airpower. Our nation will likely always need a full complement of military capabilities spanning the range of military operations, and there may well be future conflicts in which having the world's best land forces is the only guarantee of success.

This article is not intended to argue for the abandonment of our unmatched land force capabilities. Under the right circumstances, both land- and air-centric operations can each achieve desired outcomes, either individually or in combination. However, as purse strings tighten to the breaking point and one assesses long-term security challenges along with American will to remain engaged abroad in large numbers, it appears that in many future conflicts, airpower may offer American taxpayers the best return on their investment of blood and treasure. When given a choice—as an accountant and a certain former President might say—it is the bottom line that really matters. **JFQ**

our nation will likely always need a full complement of military capabilities spanning the range of military operations

NOTES

[1] See, for example, Stephen O. Fought and O. Scott Key, "Airpower, Jointness, and Transformation," *Air and Space Power Journal* (Winter 2003), available at <www.airpower.au.af.mil/airchronicles/apj/apj03/win03/fought.html>; and Randy Kee, "Brig Gen Billy Mitchell's Continuing Legacy to USAF Doctrine," *Chronicles Online Journal*, October 25, 2011, available at <www.airpower.maxwell.af.mil/airchronicles/cc/kee1.html>.

[2] David R. Mets, *The Air Campaign: John Warden and the Classical Airpower Theorists*, rev. ed. (Maxwell Air Force Base, AL: Air University Press, April 1999), 59–60.

[3] See "History of Operation Enduring Freedom," available at <www.wordiq.com/definition/Operation_Enduring_Freedom>; and "President Bush Announces Military Strikes in Afghanistan," *GlobalSecurity.org*, available at <www.globalsecurity.org/military/library/news/2001/10/mil-011007-usia01.htm>.

[4] David E. Sanger and Mark Mazzetti, "Israel Struck Syrian Nuclear Project, Analysts Say," *The New York Times*, October 14, 2007, available at <www.nytimes.com/2007/10/14/washington/14weapons.html>.

[5] For a debate over the relative importance of airpower vis-à-vis ground forces, see Richard P. Hallion, *Storm Over Iraq: Air Power and the Gulf War* (Washington, DC: Smithsonian Institution Press, 1992); and Martin Wojtysiak, "Another View of the Myths of the Gulf War," *Aerospace Power Journal* (Fall 2001), available at <www.airpower.au.af.mil/airchronicles/apj/apj01/fal01/wojtysiak.html>.

[6] Jim Garamore,"Rumsfeld Lists Operation Iraqi Freedom Aims, Objectives," American Forces Press Service, March 21, 2003, available at <www.af.mil/news/story.asp?storyID=32403155>.

[7] "Obama Announces Quick Surge and Exit Plan," Fox News, December 2, 2009, available at <www.foxnews.com/politics/2009/12/01/obama-announces-plan-dispatch-troops-afghanistan/>.

[8] See "Operation *Just Cause*," *GlobalSecurity.org*, available at <www.globalsecurity.org/military/ops/just_cause.htm>; and Air Combat Information Group, Central and Latin America Database, Panama, 1989, Operation "Just Cause," available at <www.acig.org/artman/publish/article_160.shtml>.

[9] General Accounting Office (GAO), "Operation Desert Storm Objectives," in *Operation Desert Storm: Evaluation of the Air Campaign*, June 12, 1997, appendix V, available at <www.fas.org/man/gao/nsiad97134/app_05.htm>.

[10] Garamore.

[11] "History of Operation Enduring Freedom."

[12] See <www.brillig.com/debt_clock/>.

[13] Ben Feller, "Iraq War Over, U.S. Troops Coming Home, Obama Says," Associated Press, October 22, 2011.

[14] David R. Francis, "Iraq War Will Cost More Than World War II," *The Christian Science Monitor*, October 25, 2011, available at <www.csmonitor.com/Business/new-economy/2011/1025/Iraq-war-will-cost-more-than-World-War-II>.

[15] Department of Defense, Operation Iraqi Freedom, New Dawn, Enduring Freedom Casualty Status as of October 24, 2011, available at <www.defense.gov/news/casualty.pdf>.

[16] Ibid.

[17] Dave Schuler, "What Are Our Strategic Objectives in Afghanistan?" *OutsidetheBeltway.com*, August 10, 2009, available at <www.outsidethebeltway.com/what_is_the_strategic_objective_in_afghanistan>.

[18] Oregon State University Political Science Department, 2011, "Individual Year Conversion Factor Tables," available at <http://oregonstate.edu/cla/polisci/individual-year-conversion-factor-tables>. All dollar costs cited in this article were converted to 2010 dollars using the methods detailed in this reference.

[19] See John S. Bowman, ed., *The Vietnam War: Day by Day* (New York: Bdd Promotional Book Co., 1989), which uses the $150 billion direct cost figure; and 25th Aviation Battalion Web site, "History of Vietnam," available at <http://25thaviation.org/id795.htm>, which uses $130 billion, but references a Cornell University study that calculated $200 billion in direct costs.

[20] "Vietnam War Casualties," available at <http://vietnamwar-database.blogspot.com/2010/11/vietnam-war-casualties.html>.

[21] U.S. Army Center of Military History, *Operation "Just Cause": The Incursion into Panama*, available at <www.history.army.mil/brochures/Just%20Cause/JustCause.htm>.

[22] GAO, *Panama: Cost of the U.S. Invasion of Panama*, NSIAD-90-279FS (Washington, DC: GAO, September 1990), available at <www.legistorm.com/score_gao/show/id/19610.html>.

[23] Oregon State University Political Science Department, 2011.

[24] "Noriega returns to Panama a largely forgotten man," Associated Press, December 11, 2011.

[25] Air Combat Information Group. U.S. foreign aid to Panama since 1996 alone has totaled over $1.1 billion. See "Just the Facts," available at <http://justf.org/Country?country=Panama&year1=1996&year2=2012&funding=All+Programs&x=92&y=9>.

[26] The actual length of the air campaign is debatable. Randy Roughton's dates result in 37 days and other sources show 38 days, but a GAO report lists 43 days. See Randy Roughton, "Desert Storm 20 Years Later: Lessons from Vietnam Guided Commanders as They Planned Gulf War Strategy," *Airman Magazine*, January 1, 2011, available at <http://periodicals.faqs.org/201101/2262756361.html>; and GAO, *Operation Desert Storm: Evaluation of the Air Campaign*, Letter Report, "Appendix V: Operation Desert Storm Objectives," NSIAD-97-134 (Washington, DC: GAO, June 12, 1997), available at <www.fas.org/man/gao/nsiad97134/app_05.htm>.

[27] Roughton.

[28] Tim Thompson, "The U.S. Military and the Persian Gulf War," available at <www.tim-thompson.com/desert-storm.html>.

[29] Roughton.

[30] GAO, *Operation Desert Storm: Evaluation of the Air Campaign*.

[31] See, for example, "Desert Storm, Operation," available at <www.talktalk.co.uk/reference/encyclopaedia/hutchinson/m0031881.html>; and "15 Year Anniversary of Start of First Gulf War, Desert Storm," available at <http://ptsdcombat.blogspot.com/2006/02/15-year-anniversary-of-start-of-first.html>, which lists the Department of Defense as the source of its figures. The GAO's *Operation Desert Shield/Storm: Costs and Funding Requirements* (Washington, DC: GAO, September 1991), lists $47.1 billion as the total funding requirement and $61.1 billion as total incremental costs, although the report states the lower figure may be overstated and documents the challenges with units failing to record incremental costs of the operation; available at <http://archive.gao.gov/t2pbat7/145082.pdf>.

[32] "Kosovo War Cost £30bn," BBC News, available at <http://news.bbc.co.uk/2/hi/europe/476134.stm>.

[33] "The Cost of Kosovo," *The Economist*, May 27, 1999, available at <www.economist.com/node/322101>.

[34] U.S. Agency for International Development, "Kosovo," available at <www.usaid.gov/locations/europe_eurasia/countries/ko>.

[35] "Operation Allied Force," *GlobalSecurity.org*, available at <www.globalsecurity.org/military/ops/allied_force.htm>.

[36] Sylvia Poggoli, "Milosevic: The Life and Death of a Strongman," National Public Radio, March 10, 2006, available at <www.npr.org/templates/story/story.php?storyId=5257846>.

[37] "History of Operation Enduring Freedom."

[38] Ibid.

[39] "Operation Enduring Freedom," *iCasualties.org*, available at <www.icasualties.org/OEF/index.aspx>.

[40] Devin Dwyer, "Afghanistan War Costs Loom Large over Obama Troops Announcement," *ABC World News*, June 22, 2011, available at <http://abcnews.go.com/Politics/afghanistan-war-costs-soar-obama-troops-announcement/story?id=13902853>.

[41] Julian E. Barnes and Adam Entous, "NATO Air Strategy Gains Renewed Praise," *The Wall Street Journal*, October 21, 2011, available at <http://ebird.osd.mil/ebfiles/e20111021849381.html>.

[42] Adam Levine, "Lead from Behind or Leave That Strategy Behind in Libya," *CNN.com*, October 21, 2011, available at <http://security.blogs.cnn.com/2011/10/21/lead-from-behind-or-leave-that-strategy-behind-in-libya>.

[43] GAO, *Operation Desert Shield/Desert Storm*.

[44] "The Cost of Kosovo"; and GAO, *Evaluation of the Air Campaign, Operation Desert Storm*.

[45] Max Boot, "Did Libya Vindicate 'Leading From Behind'"? *RealClearWorld.com*, September 1, 2011, available at <www.realclearworld.com/articles/2011/09/01/did_libya_vindicate_leading_from_behind_99654.html>.

[46] Roughton.

[47] U.S. Army Center of Military History.

[48] "Iraqi Army," *GlobalSecurity.org*, available at <www.globalsecurity.org/military/world/iraq/army.htm>.

[49] Department of State, "Iraq," available at <www.state.gov/r/pa/ei/bgn/6804.htm>.

[50] Benjamin S. Lambeth, "Kosovo and the Continuing SEAD Challenge," *Aerospace Power Journal*, June 3, 2002, available at <www.airpower.maxwell.af.mil/airchronicles/apj/apj02/sum02/lambeth.html>.

[51] Rebecca S. Grant, "The Afghan Air War," Air Force Association, September 2002, available at <www.afa.org/media/reports/afghanbook/>.

[52] Phillip S. Meilinger, "Lowering Risk: Air Power Can Reduce Civilian Casualties," *Armed Forces Journal*, July 2009, available at <www.armedforcesjournal.com/2009/07/4079006>.

[53] "Operation Just Cause."

[54] "Kosovo: Civilian Deaths in the NATO Air Campaign," Human Rights Watch, February 1, 2000, available at <www.unhcr.org/refworld/country,,HRW,,SRB,,3ae6a86b0,0.html>.

[55] Francis.

[56] See Laurent Thomet, "NATO Declares Oct. 31 End to Libya Mission," *Defense News*, October 28, 2011, available at <www.defensenews.com/story.php?c=MID&s=TOP&i=8083842>; Amnesty International, "NATO Urged to Investigate Civilian Deaths during Libya Air Strikes," August 11, 2011, available at <www.infowars.com/nato-urged-to-investigate-civilian-deaths-during-libya-air-strikes>; and Nazish Fatima, "NATO accused of having minimized civilian casualties in Libya," *AllVoices.com*, May 14, 2012.

[57] Jim Michaels, "Taliban Behind Most Afghan Civilian Casualties," *USA Today*, June 22, 2011, available at <www.usatoday.com/news/world/afghanistan/2011-06-22-afghan-civilian-casualties_n.htm>.

[58] Hannah Fischer, *Iraqi Civilian Deaths Estimates*, RS22537 (Washington, DC: Congressional Research Service, August 27, 2008), available at <www.fas.org/sgp/crs/mideast/RS22537.pdf>. The most commonly accepted figures appear to be those compiled by the "Iraq Body Count," which shows 86,661 and 94,558 deaths between 2003 and 2008. Clearly that number is higher when extrapolated to the present.

[59] For a historical assessment of civilian casualties since the invention of airpower as well as an argument that airpower can reduce the risk of civilian deaths, see Meilinger. For a wide-ranging estimation of civilian deaths during the Vietnam conflict, see "Vietnam War Casualties."

[60] Thom Shanker, "NATO Tries to Reduce Afghan Casualties," *The New York Times*, September 16, 2008, available at <www.nytimes.com/2008/09/17/world/asia/17gates.html>.

ShinyCapstar.com

SCIENCE VS. the Art of War

Germans confront Serbs in World War I (drawing by Richard Caton Woodville)

By MILAN VEGO

War is an art and as such is not susceptible of explanation by fixed formula.

—GENERAL GEORGE S. PATTON

Dr. Milan Vego is Professor of Operations in the Joint Military Operations Department at the Naval War College.

People generally do not feel comfortable with uncertainty. Hence, there is a constant search in life—including in the military—for deriving various principles or rule sets and making things more controllable and predictable. Since ancient times, militaries have been engaged in an endless quest for certainty in the command in war.[1] They have striven to precisely know all the key elements of the situation including the enemy force and its intentions and reactions to their own actions.

Warfare as a Science

The idea that the conduct of war is a science is almost as old as warfare itself. In ancient times, military theorists started to search for certain principles and rules guiding the conduct of war. During the Renaissance, art, music, philosophy, government, science, and warfare underwent a gradual but profound transformation.[2] In that era, Europeans rediscovered the military treatises written by ancient military theorists, specifically Xenophon (430–354 BCE), Julius Caesar (100–44 BCE), and Publius Flavius Vegetius Renatus (4th century CE). The classical legacy formed the intellectual background

and source of historical reference for military thinking until the end of the 18th century.[3]

The scientific revolution in the late 17th and 18th centuries was the result of new ideas and advances in physics, chemistry, astronomy, biology, and medicine. Because of great thinkers such as Isaac Newton (1643–1727), scientific discourse took the preeminent role in reordering society within Western civilization. There was a closer association with technology.[4] The first techno-scientific revolution in European warfare was articulated around a clockwork metaphor, which became the symbol of order, regularity, and predictability. The clock concept was emulated by European militaries as exemplified by Frederick the Great (1712–1786).[5]

Moreover, bombardments and fortifications became increasingly guided by geometrical principles and the great advances in ballistics. The most influential practitioner of siegecraft was the French Marshal Sébastien Le Prestre de Vauban (1633–1707). He used his understanding of geometry, architecture, and gunnery to advance the science of fortifications.[6] In his 30 years of professional activity, Vauban personally designed a number of fortresses and conducted nearly 50 sieges—all of them successful.[7]

The Italian-born Austrian field marshal Raimondo Montecúccoli (1609–1680) was one of the most influential practitioners and theorists in the late 17th century. He was one of the first who tried to explain warfare "scientifically."[8] Montecúccoli observed that like all sciences, the science of war aims to reduce experiences to universal and fundamental rules.

The French marshal Jacques-Francois de Chastenet, Marquis of Puységur (1656–1743), was a distinguished soldier who undertook a systematic treatment of war. He believed that experience was not the only approach to understanding war. Puységur's intent was to reduce warfare to a set of rules and principles, as had already been done for sieges.[9] Like Montecúccoli, he observed that war was the most important of all sciences and arts. He further claimed that war during his life lacked a systematic theoretical study, with people relying on tradition and personal experiences. In his view, field warfare needed to be made as scientific as siegecraft had been by Vauban. Hence, the emphasis should be on the study of geometry and geography and their applications to the art of war.[10]

The writings of French military theorist and soldier Jean-Charles de Folard (1669–1752) were the main precursors of "enlightened military thought." Folard was fascinated with classical Greece and Rome. He examined war from a scientific perspective in order to discover universal principles guiding its conduct. He also addressed psychological dimensions in combat. His writings influenced many military theorists and practitioners of the Enlightenment era, such as Maurice de Saxe, Frederick the Great, and Napoleon Bonaparte I (1769–1821).[11] Saxe (1696–1750) was one of the most successful generals of the era of musketry. He wrote the famous *Reveries on the Art of War* (1757). In the preface, he stated that "war is a science so obscure and imperfect that custom and prejudice confirmed by ignorance are its sole foundation and support; all other sciences are established upon fixed principles . . . while this alone remains destitute."[12] To understand war, Saxe argued that without knowledge of the human heart, one is dependent on the favor of fortune, which sometime is inconsistent.[13]

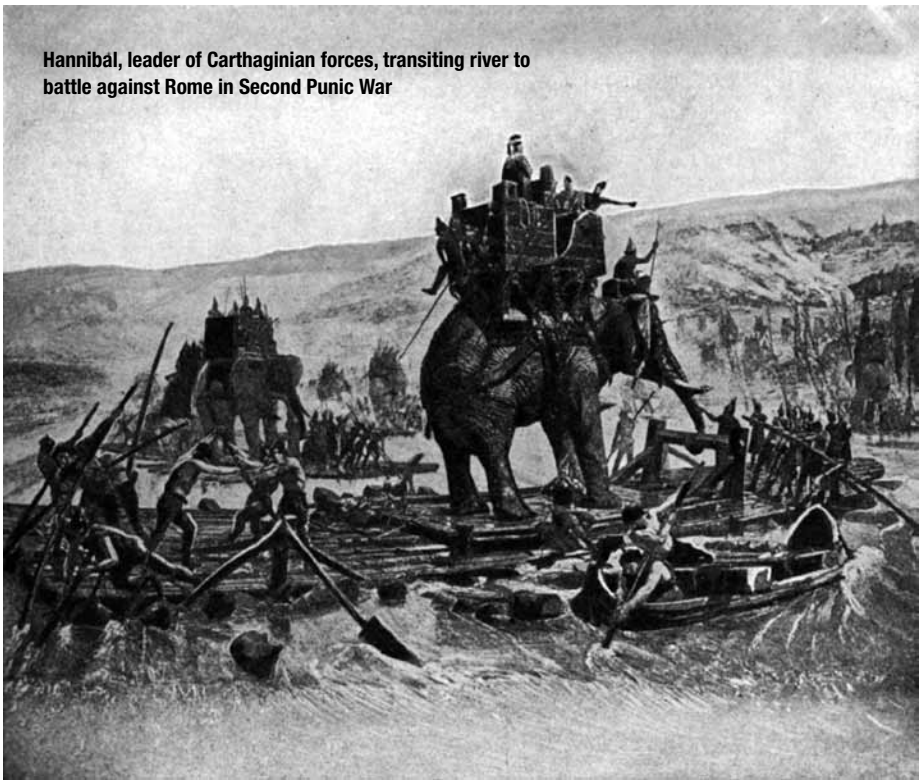
The Enlightenment Era, 1750–1800

The scientific revolution of the 17th century, and the beginning of Newtonian science in particular, led to widespread belief among European intellectuals that the human mind is capable of mastering all realities. Another influence during the Enlightenment was French neoclassicism, which taught that each art is governed by certain universal and immutable principles and rules.[14]

Military officers, mostly from the ranks of nobility, became influenced by the philosophical, intellectual, and cultural trends of the late 18th century. They concluded that war, like other sciences, has to be studied systematically, and then a clear and universal theory of war could be created. Hence, the military profession must be studied theoretically and not only by using combat experiences. This new emphasis on the study of war resulted in a significant increase of published works dealing with military theory.

Dominant ideas in military thought during the Enlightenment were rudiments of appreciation of the political side of war, especially in Prussia under Frederick the Great (1712–1786); the realization of the role of psychological factors in combat; and the unprecedented application of pseudoscientific principles to the study of warfare.[15] The most important military theorists of the Enlightenment were Count Turpin de Crissé (1709–1799), Paul Gideon Joly de Maizeroy (1719–1780), Frederick the Great, Pierre-Joseph de Bourcet (1700–1780), Jacques Antoine Hippolyte, Comte de Guibert (1743–1790), Henry E. Lloyd (1720–1783), and Dietrich Heinrich Freiherr von Bülow (1757–1807).

In the late Enlightenment era, military theory was dominated by the advocates of the so-called geometrical or mathematical school. These proponents firmly believed that the true art of war was not in fighting bloody battles but in conducting skillful maneuvers to checkmate the enemy through calculated marches and movements.[16] The ideal was to defeat the enemy not by fighting a bloody battle but to skillfully outmaneuver him. Strategy was based on abstract mathematical foundations. The commander was required to be like a chess player capable of mastering all combinations, while the army in the field was like a figure on a chessboard. Personal and creative performance



Hannibal, leader of Carthaginian forces, transiting river to battle against Rome in Second Punic War

on the battlefield did not play a great role. The actions of the great captains were explained by their adherence to rules of the art of war.[17]

The Welsh general and theoretician Henry E. Lloyd was one of the strongest proponents of the scientific approach to the study of war. He compared the army to a mechanical device, which, "like all other machines," is composed of various parts. Its perfection depends first on its parts, and second, on the manner in which these parts are arranged. He wrote that war is a branch of Newtonian mechanics. Lloyd believed that the exact knowledge of the country, as well as the science of position, camps, and marches, were essential disciplines to be mastered by a general.[18]

Unlike the other representatives of the geometrical school, Lloyd was one of the first thinkers who highlighted the need to pay attention to the morale of the troops. This was evident in his discussion of human passions as motivating factors including fear, honor, shame, and desire for riches. He wrote that the most powerful of all is the love of liberty and religion.[19]

The Prussian officer Freiherr von Bülow, one of the most influential theorists of the Enlightenment, wrote *Spirit of the New System of War* (1799). He reinforced Lloyd's scientific approach or geometric science of strategy.[20] In his view, the modern conduct of war was based on lines of operation and the introduction of firearms.[21] Bülow provided mathematically precise theory. He firmly believed that his theories could offer the key to victory by enabling scientific precision of the outcome before armies engaged in battle. He claimed to discover mathematical secrets of strategy and established them as a science. In Bülow's view, "From now on, there will be no need of crude considerations and the hazardous trial of battle in order to plan and decide the fate of campaign. If the attacker relied on an unsound base [of operations], the defender could force him to retreat without resorting to battle." Battle was made unnecessary by the scientific perfection of strategy: "War will be no longer called an art, but science. . . . The art itself will be a science, or be lost in it."[22] In contrast to Lloyd and some other theorists of the Enlightenment, who alongside the scientific parts of war left room for the creativity of a genius, Bülow asserted that "the sphere of military genius will at last be so narrowed, that a man of talents will no longer be willing to devote himself to this ungrateful trade."[23]

Postmilitary Enlightenment Era

The views of the proponents of the geometrical school were proved false with the advent of decisive warfare as practiced by the French revolutionaries and Napoleon I. However, the proponents of the military ideas of the Enlightenment did not lose influence. Their ideas were largely adopted, although in a modified form, by Antoine-Henri Jomini (1779–1869) and the Austrian Archduke Charles (1771–1847). In fact, the great majority of military theoreticians in the 19th century based their ideas on the theories developed during the Enlightenment.[24]

The Swiss-born French general Jomini avoided the trend of developing increasingly complex geometric systems of warfare, yet he built his theories on foundations laid in the Enlightenment. This, in turn, led him to take a fundamentally reductionist and predictive approach.[25] Jomini wrote that "war in its ensemble is not a science, but an art, and strategy in particular may be regulated by fixed laws resembling those of positive science but this is not true if war is viewed as a whole."[26] He argued that tactics are the only part of war that can be subjected to fixed rules.[27]

Jomini sought to identify universal principles central to the art of war and to discern them through his study of the campaigns conducted by Frederick the Great. In his seminal *Summary of the Art of War* (1838), Jomini wrote that there are some fundamental principles of war that cannot be deviated from without danger, while their application has been always crowned with success.[28] He provides a list of four maxims that made an overarching principle; even seemingly simple principles consisted of a set of subordinate tenets. Although he revised his system of principles, he never significantly diverged from the ideas that he developed by studying Frederick the Great's campaigns through the lenses of Lloyd and Bülow.[29]

Despite his obvious fixation on the principles of war, Jomini recognized the importance of moral factors in war. In his view, these factors prevented a theoretical determination of tactics. He firmly believed that despite technological changes, "strategy alone will remain unchanged, with the principles the same as under Scipios and Caesars, Frederick and Napoleon, since they are independent of the nature of the arms and organization of the troops."[30]

Archduke Charles, the son of Emperor Leopold II, was regarded as one of the best generals of the Habsburg monarchy and of Continental Europe as well. The Archduke

was also one of the better known military theorists of his era. His work was based on the ideas of the late Enlightenment. In his *Principles of Higher Art of War* (1806), he stated that "The principles of the science of war are few and unchanging. Only their application is never the same. Every change in the conditions of armies; in their arms, strength and positions, and every new invention, involved a different application of these rules."[31] In his *Principles of Strategy* (1814), Archduke Charles also adopted almost entirely Bülow's general theory of war and his geometrical concept of operations, but with less emphasis on mathematical aspects.[32]

The view that the conduct of war is largely a science and not an art was not limited to Jomini's interpreters and followers. One of the leading military theorists in the 20th century, British General J.F.C. Fuller (1878–1966), was also a firm believer that the conduct of war is largely a science. He was much influenced by Lloyd's theories. In his *Foundations of the Science of War*, Fuller wrote that scientific methods are a common sense approach on how to know the truth about the past and how we can apply this truth to the conditions that surround us now and that will probably exist during the next war.[33] Fuller asserted that war is as much a science as any other human activity because it is built on facts and that war must be reduced to science before it can be practiced correctly as an art.[34]

The Marxist-Leninist theoreticians believed that war was essentially based on scientific principles. Vladimir Lenin's (1870–1924) predilection for dialectical-materialist principles of objectivism, regularities in the nature of society, and the possibilities of knowledge strongly influenced the post-1917 development of Soviet military theory. Lenin's philosophical views were compatible with more objective scientific methods in military affairs and led toward the development of military foresight. Hence, in the Soviet military, virtually every aspect of military affairs was influenced by Lenin's ideological views.[35] The main reason for those and for similar beliefs was an unbounded faith in the extraordinary value and impact of materiel on the conduct of war. Friedrich Engels (1820–1895), one of the early and influential Marxist military theoreticians, believed that all great revolutions in warfare were the result not of great masters of war but of inventions of better weapons and changes in materiel. For him, military power was based on weapons and military equipment whose quality was dependent on the status of the development of what he and other Marxists called "production forces."[36]

The Soviet obsession with scientific Marxism-Leninism and its attendant preoccupation with history, laws, principles, norms, and rules and its attention to "objective" algorithms and formulae all artificially reduced the dynamics of the battlefield to a sterile process more akin to calculus than human struggle.[37]

Fuller wrote that scientific methods are a common sense approach on how to know the truth about the past and how we can apply this truth to the conditions that surround us now

Modern Theories

Traditionally, the Western approach to conducting war has been influenced by the Newtonian quest to identify universal laws of combat by which all problems can be resolved and the results of combat predicted. Hence, extensive efforts are made to quantify everything in war. Since the mid-1990s, the systems (or systemic) approach to warfare has gradually emerged as the dominant school of thought in the U.S. military, most other Western militaries, and the North Atlantic Treaty Organization (NATO). This was exemplified by the wide acceptance in the United States and NATO and some other militaries of the claims by advocates of network-centric warfare (NCW)/network-centric operations (NCO), effects-based operations (EBO)/effects-based approach to operations (EBAO), and systemic operational design (SOD), which mutated to *operational design* and ultimately to *design*. Since their heyday in the early 2000s, the influence of NCW/NCO advocates has been greatly diminished. U.S. Joint Forces Command officially abandoned the more mechanistic elements of EBAO in the summer of 2008. However, some theoretical aspects of EBAO were retained in the main U.S. joint doctrine documents and are still used, although in a modified form, by NATO. A common characteristic of NCW/EBO/SOD is that they are based on new and largely unproven technologies. They were adopted without proper testing and were not backed by empirical evidence. They reflect the neo-Newtonian, not the Clausewitzian, view of the nature of war.

The effects-based warfare proponents embraced so-called systems of systems analysis (SoSA) to assess situations and then identify centers of gravity. SOD is based on both general systems theory and complexity theory.[38] *Design* itself is defined as a "repeatable methodology of reasoning that helps commanders understand how to change a complex-adaptive system."[39] Its declared purpose is to bridge the gap from the situation that exists at the beginning of an operation—that is, the observed-system—to the situation when operations end—that is, the desired system. The design uses some theoretical aspects of SOD and EBO but supposedly does not rely on either concept to achieve its main purpose.[40] Proponents of design acknowledge that warfare is a complex, adaptive system rather than a closed system. This, in turn, makes anticipating and evaluating the effect of one's physical actions on the enemy's behavior a significant challenge.[41]

Quantifying the Unquantifiable

Since the advent of the modern era, there have been numerous attempts to apply some elements of quantitative analysis to understanding the sources of victory. This is especially the case with those who view the conduct of war as a science. Claims have been made that the use of various quantifiable methods is more "objective" than using the commander's judgment and experience. Yet this is not true because, among other things, the decision of what to measure is highly subjective. Carl von Clausewitz (1780–1831) warned that so-called mathematical factors can never find a firm basis in military calculations. In his view, war most closely resembles a game of cards.[42]

The Russians relied on various mathematical solutions to military forecasting problems since the late 19th century. The Soviet propensity to use mathematical methods was the result of more than 75 years of study, self-criticism, and refinement.[43] The Russians derived multiple combat models for optimizing courses of action and predicting relative rates of advance on the battlefield. These

measurements were based on the outcomes of major operations and battles in the Great Patriotic War (1941–1945). The Soviets considered their methodologies dialectically and scientifically sound and, moreover, consistent with Marxist-Leninist teachings. By the early 1960s, the mathematics of armed conflict was categorized as a branch of Soviet operations research, the social science that rationally organizes goal-directed human activity.[44] The Soviet operations research tried to reduce certain tactical and technical aspects of military science to measurable objective indices so decisions could be made or substantiated. The Soviets especially emphasized the so-called correlation of forces method as a tool for tactical and operational commanders to make sound decisions. This method dealt with direct or numerical comparisons of forces, quantification of selected battlefield elements, and mathematical expressions or equations related to those elements in such a manner as to support decisionmaking.[45] Yet the Soviets did not rely solely on quantitative methods such as correlation of force and means. They also took into account the enemy's use of surprise and deception.[46]

In the West, various mathematical methods known as operations research (OR) were used for enhancing the effectiveness of certain weapons and developing tactics in their employment. The origins of OR are found in World War I. In 1914, the British mathematician F.W. Lanchester devised the so-called N-square law, which quantified the relationship between victory and superiority in numbers.[47] The OR was used in the United Kingdom in the late 1930s to find a solution to the seemingly impossible problem of successful defense against the enemy's air attacks on the British Isles. In World War II, OR was generally used in scarce radar stations and in devising the optimal search techniques and the size of convoys in antisubmarine warfare (ASW). OR also reduced the loss rate of convoys when analysts realized that larger convoys could travel more safely.[48] The United States followed the British lead and used OR in greatly increasing the effectiveness of mine warfare, ASW, and air attacks.

Systems analysis (now known as policy analysis) is another quantifiable method used in the public sector and adopted by the military. This method is concerned with the allocation of resources and is aimed to maximize the value of objectives achieved minus the value of resources used. In business, this reduces itself to maximizing profits.[49] By using mathematical methods, analysts systematically emphasized quantifiable aspects of warfare, which were susceptible to being integrated into mathematical models and input-output calculations. Anything that could not be quantified was therefore excluded. Such elements of the commander's personality as intuition, courage, and willpower were devalued.[50]

One of the strongest advocates of systems analysis in the U.S. military was Secretary of Defense Robert McNamara. During his tenure (1961–1968), he extensively used systems analysis for making key decisions pertaining to force requirements and weapons design and procurement. McNamara is perhaps best known for using quantifiable methods not only in assessing the progress of the war in South Vietnam but in making decisions based on these methods—that is, trying to conduct war as a science rather than an art. The Pentagon applied the so-called body count as the principal measurement to determine what the United States should be doing to win in Vietnam while putting U.S. troops at the least risk.[51] Yet such metrics proved meaningless. The statistical indicators pointing to U.S. success were frequently erroneous and misleading. The models on which war managers relied were equally faulty. Trapped in the mindset that the war was a purely technical problem, U.S. high officials failed to grasp the sheer determination of their opponents and the extent of the success of their political strategy.[52]

Clausewitz warned that so-called mathematical factors can never find a firm basis in military calculations

The Pentagon's emphasis on business practices has led since the late 1990s to an extensive reliance on various "metrics" in evaluating progress toward accomplishing objectives on the battlefield. These quantification methods in essence have replaced the commander's judgment, intuition, and independence of execution.[53] The use of metrics is highly subjective because higher authority arbitrarily selects which aspects of the situation should be counted and evaluated. But even if the metrics are correctly determined, it is often difficult to evaluate hidden elements in the situation.

The proponents of the systems approach to warfare also rely on some quantifiable methods to evaluate the combat potential of the opposing forces and the rate of accomplishing one's objectives. For example, the effects-based warfare proponents expanded the use of various metrics compared with their use in the traditional Military Decision Making Process. The main quantifiable methods used in EBO are so-called measures of merit. These are in turn divided into measures of effectiveness and measures of performance.

War as an Art

The view that the conduct of war is largely an art is not entirely new. Several military theorists during the Enlightenment, notably Saxe and Lloyd, realized the great importance of psychological factors in warfare. Yet they never went a step further and viewed warfare as complex and full of uncertainty, chaos, unpredictability, and even irrationality.

The most dramatic changes in military theory that led to a more refined view of warfare occurred in Germany in the late 18th and early 19th centuries. The major cultural trends in Germany were romanticism, nationalism, and idealism. German romanticism challenged the fundamentals of the French-dominated Enlightenment's worldview. It was opposed to the French cultural and political imperialism. It led to the awakening of German national sentiment. German thinkers of the "counter-Enlightenment" believed that concepts of knowledge and reality are fundamentally false, or at least exaggerated. For them, the world was not simple but highly complex, composed of innumerable and unique elements and events, and always in a state of flux. They were not as enthusiastic about Newtonian science.[54] The German Romanticists increasingly focused on the inherent complexity of nature. They argued that this complexity could not be explained by the Newtonian scientific model. The German Romanticists took a historical approach to their understanding of reality.

Soldiers return fire during firefight with Taliban forces in Barawala Kalay Valley, Afghanistan

U.S. Army (Cameron Boyd)

All comprehension was seen as the subjective result of the dynamics of one's time and place. These and similar ideas led German intellectuals to believe that reality does not conform to universal laws or principles.[55]

The new cultural trends that started as a reaction to the Enlightenment also had considerable influence on German military theorists and practitioners, notably Georg Heinrich von Berenhorst (1733–1814), Johann Gerhard von Scharnhorst (1755–1813), and Clausewitz. The first work that challenged the prevalent ideas of the military Enlightenment was Berenhorst's three-volume *Reflections on the Art of War: Its Progress, Contradictions and Certainty* (1796–1799). Berenhorst observed that the ancient Greeks and Romans brought the art of war to the pinnacle of perfection. For him, they were more "artistic" than anyone else.[56] He wrote that during the Enlightenment, the art of war, like the rest of the sciences and arts, advanced knowledge and supported innate talent. In his view, the art of war is not based on immutable laws but rather is associated with the unknown and uncontrollable modifications of the human spirit. Moral forces animate the troops; therefore, they are a major factor in the conduct of war.[57] Berenhorst believed that war, in contrast to mathematics or astronomy, could not be formulated as a science. He considered various rules and principles derived from experiences as artificial and dogmatic. They were often applied indiscriminately to a changed situation.[58]

Scharnhorst viewed the systems of conducting operations that were fashionable in his day as artificial and one-sided. The art of war was a practical science and its meaning could only be based on the study of reality. If that link is broken, then the art of war leads to abstractions.[59] In his essay "The Use of Military History, the Causes of Its Deficiencies" (1806), Scharnhorst wrote that great generals throughout history studied the principles of the art of war. Some branches of this art are even susceptible to mathematical formulation, but others are dependent on circumstances and cannot be studied mechanically. This is why study alone without genius will never make a great general.[60]

Clausewitz was the first theoretician who systematically presented a philosophy of war in all aspects. Influenced by the ideas of German romanticism, he saw the world differently from the military thinkers of the Enlightenment. He was also greatly influenced by Scharnhorst's pragmatism and relativist approach. He considered war as a complex and unpredictable phenomenon. Clausewitz believed only in broad generalities, none of which consistently held true in the fog and friction of actual combat.[61] He argued that a system fails to account for the "endless complexities involved" in war and therefore results in a theoretical construct that bears little resemblance to the actual practice of war.[62] Hence, he considered any attempt to reduce the complex phenomena of war to a simple system of universal principles as an exercise in futility.[63]

Clausewitz believed that war belongs to the domain of social life; it is neither a science nor an art. It is not a science because it is a matter of action, and it is not an art because it exerts itself not on inanimate or passive human material but on reacting, living force.[64] Clausewitz wrote that the "art of war must always leave a margin for uncertainty in the greatest things and in the smallest. The greater the gap between uncertainty on the

one hand and courage and self-confidence on the other hand, the greater the margin that can be left for accidents."[65]

The human factor largely determines what is called the "nature" of war—those constant, universal, and inherent qualities that characterize any war throughout the ages. The nature of war is unchangeable regardless either of shifting motives and forms of war or of technological advances.[66] Human behavior is a major part of the nature of war. Clausewitz's greatest contribution to our understanding of war was his analysis of the importance of the human factor and the psychological element in particular in the conduct of war. He wrote that warfare is shaped by human nature, complexities of human behavior, and limitations of human and physical conditions. The material and psychological aspects of a war form an organic whole; they are inextricably linked.[67] He wrote that war is not the action of a living force on a lifeless mass but the collision of two living forces that interact.[68] Victory does not consist only in the conquest of the battlefield, but in the destruction of the physical and moral fighting forces.[69]

The principal psychological features of any war are hatred, hostility, violence, uncertainty (or fog of war), friction, fear, danger, irrationality, chance, and luck.[70] For Clausewitz, a war was a trinity composed of primordial violence, hatred, and enmity—a blind natural force.[71] Clausewitz observed that danger is "a part of the friction of war and without accurate conceptions of danger one cannot understand war."[72] Moreover, war is "the realm of physical exertion and suffering."[73] It is full of chances and probabilities within which the creative spirit is free to roam.[74] Clausewitz wrote that nowhere do accidents have such a free playing field as in war. Not only its objective but also its subjective nature makes war a gamble.[75]

Clausewitz observed that "The great uncertainty of all facts presents a peculiar difficulty in war, because all actions take place in something virtually akin to dusk, which in addition like fog or moonlight, gives the objects an exaggerated size and a grotesque view."[76] He pointed out that the only situation a commander can know fully is his own. The commander's knowledge of the enemy's situation is often based on unreliable information. His evaluation therefore may be mistaken and can lead him to assume that the enemy has the initiative when in fact he himself could have it. Such a faulty appreciation is as likely to lead to ill-timed action as to ill-timed inaction.[77] Clausewitz argued that friction is the only concept that quite generally fits the difference between real war and war on paper.[78] He argued that this "tremendous friction, which cannot as in mechanics, be reduced to a few points, is everywhere in contact with chance, and brings about effects that cannot be measured, just because they are largely due to chance. Friction is the force that makes the apparently easy so difficult."[79] Friction encompasses uncertainties, errors, accidents, technical difficulties, and the unforeseen, and their effects on one's decisions, actions, and morale.[80]

Helmuth von Moltke, Sr., stated that most of what constitutes the operation of armies is essentially grounded in science, while the art comes to the fore when the wills of opposing commanders meet.[81] For him, the scientific method was anathema. He held that nothing in war is certain. Therefore, in war as in art there "exist no general rules; in neither can talent be replaced by precepts. And given the uncertainty of war, Moltke concluded that strategy could not be more than a system of expedients."[82] He created an environment that cultivated creativity, improvisation, inventiveness, and open-mindedness.[83]

Clausewitz's greatest contribution to our understanding of war was the importance of the human factor and the psychological element in particular

During the tenure of Field Marshal Moltke, Sr., as chief of the Prussian/German Great General Staff (1857–1888), the Clausewitzian teachings on war were widely shared by the Prussian/German theorists and practitioners. The Germans believed that no sphere of human activity, conditioned as it was by its historical setting and dominated by a multitude of acts, could ever be compressed into a formal system of rules and principles. This cultural premise was introduced by Clausewitz.[84] The Germans considered warfighting more of an art than a science. They believed no one could control events in a war. Any war is full of ambiguity, confusion, and chaos. In a war, the absolute cannot be achieved, nor can uncertainty be mastered. A margin must always be left for uncertainty. Moltke explained that in war, "everything was uncertain; nothing was without danger, and only with difficulty could one accomplish great results by another route. No calculation of space and time guaranteed victory in this realm of chance, mistakes, and disappointments. Uncertainty and the danger of failure accompanied every step toward the objective." The Germans accepted the confusion of battle as an unending source of potential opportunities and built a command and control philosophy, known as the mission command (*Auftragstaktik*), in which that potential could be realized through decentralized decisionmaking.[85]

During the interwar years (1919–1939), the Germans considered war a free and creative activity, or an art. It makes high demands on human personality. At the same time, warfare is founded on scientific principles. New weapons dictate ever-changing forms. Their appearance must be anticipated and their influence evaluated. Afterward, they must be put in service quickly. Combat situations are diverse; they change often and suddenly and can seldom be anticipated in advance. Incalculable elements have a decisive influence, particularly as one's own will is pitted against the independent will of the enemy. Friction and errors are daily occurrences.[86]

Clausewitzian views on the true nature of war remain valid today. The human element is the single most critical aspect of warfare. Human nature has changed little despite vast changes in military technologies. Warfare is too complex and unpredictable an activity to be taken over by machines or explained and managed by pseudoscientific theories. Only the human brain is fully capable of reacting in a timely and proper fashion to the sudden and unanticipated changes in the situation and countering the enemy's actions and reactions. The enemy has his own will. He can react unpredictably or irrationally.

The timing and scope of irrationality cannot be predicted or measured. Irrational decisions on either side in combat can have significant consequences on both the course and the outcome of a war. Perceived irrationality is often the reflection of one's cultural values in evaluating the enemy's actions and reactions. An enemy commander is a product of a different society, traditions, and culture. Hence, he may make decisions that are considered irrational although they are fully consonant with his own societal values and military culture. Psychological states of the individuals or groups and their possible reactions under stress cannot be entirely known. This is even more true when dealing with enemy forces.

during the interwar years, the Germans considered war a free and creative activity, or an art

Conclusion

The question of whether the conduct of war is largely a science or an art is by no means settled. This is mainly due to the inherent human proclivity to seek certainty in all domains of social life, including warfare. Another factor is the influence of Newtonian scientific theories and almost blind faith in the power of advanced technologies. Yet numerous attempts to make the conduct of war largely or exclusively a science have repeatedly failed. Warfare is too complex, chaotic, and unpredictable to be conducted by using scientific methods, no matter how advanced. This is not to underestimate or ignore the importance of science in military affairs. Science and technology were and will remain major factors in the ever-changing character of war. History is replete with examples where science and technology have made the difference between victory and defeat.

Scientific methods should be extensively used in explaining the phenomena of war in general and all its aspects. Sound theories of war are based on the use of scientific methods. Various business models can be successfully applied in managing military organization, force planning, and designing of weapons. Quantifiable methods can be useful in assessing and enhancing the use of individual platforms and their weapons/sensors and their tactics. However, the utility of such methods is progressively diminished when they are applied at the operational and strategic levels of war where intangible elements play a major role in the course and outcome of war.

In short, there is a huge difference between using science and technology to enhance the combat potential of one's forces and applying scientific methods in the conduct of war. Our knowledge and understanding of warfare is a science, but the conduct of war itself is largely an art. This will not change in the future regardless of scientific and technological advances. As in the past, the character of war will change, even dramatically, but the nature of war as explained by Clausewitz will not. Warfare would be relatively simple, predictable, and controllable but for its intangibles—the human factor and its psychological elements. **JFQ**

NOTES

[1] Antoine Bousquet, *The Scientific Way of Warfare: Order and Chaos on the Battlefields of Modernity* (New York: Columbia University Press, 2009), 9–10.

[2] Donald E. Neill, "Ancestral Voices: The Influence of the Ancients on the Military Thought of the Seventeenth and Eighteenth Century," *The Journal of Military History* 62, no. 3 (July 1998), 488.

[3] Azar Gat, *A History of Military Thought from the Enlightenment to the Cold War* (Oxford: Oxford University Press, 2001), 9.

[4] Cited in Bousquet, 15.

[5] Ibid., 38.

[6] Neill, 507.

[7] Ibid., 506.

[8] Thomas M. Barker, *The Military Intellectual and Battle: Raimondo Montecúccoli and the Thirty Years' War* (New York: State University of New York Press, 1975), 5.

[9] Robert S. Quimby, *The Background of Napoleonic Warfare: The Theory of Military Tactics in Eighteenth-Century France* (New York, AMS Press, 1968), 16.

[10] Cited in Gat, 37–38.

[11] Eugene Miakinkow, "A Russian Way of War? Westernization of Russian Military Thought, 1757–1800" (MA thesis, Waterloo, Ontario, 2009), 19.

[12] Cited in J.F.C. Fuller, *The Foundations of the Science of War* (London: Hutchinson & Co., 1926), 24.

[13] Ibid., 294.

[14] Cited in Gat, 31.

[15] Miakinkow, 29.

[16] Guenther Blumentritt, Die Gedanklichen Grundlagen des Alten O.K.H in O.v. Natzmer, *Die Gedanklichen Grundlagen des OKH und deren Auswirkungen auf seine Organisation. Ein Schlusswort zur Gesamtarbeitt "OKH,"* December 1949, ZA/1 1935 P-041kk, Freiburg, i.Br, Bundesarchiv-Miliaterarchiv, 10.

[17] Reinhard Hoehn, *Scharnhorts Vermaechtnis* (Bonn: Athenaum Verlag, 1952), 67.

[18] Cited in Armstrong Starkey, *War in the Age of Enlightenment, 1700–1789* (Westport, CT: Praeger, 2003), 57.

[19] Ibid., 58.

[20] Mark T. Calhoun, "Clausewitz and Jomini: Contrasting Intellectual Frameworks in Military Theory," *Army History*, no. 80 (Summer 2011), 25.

[21] Gat, 81.

[22] Ibid., 84.

[23] Ibid.

[24] Ibid., 142.

[25] Calhoun, 27.

[26] Cited in Gurbachan Singh, "The Science of War," available at <www.mindef.gov.sg/content/imindef/publications/pointer/journals/2007/v33n1/feature7.print.html?Status=1>.

[27] Cited in Gat, 115.

[28] Singh.

[29] Calhoun, 27.

[30] Cited in Gat, 115–116.

[31] Ibid., 101.

[32] Ibid., 104.

[33] Cited in Singh.

[34] Anthony John Trythall, *"Boney" Fuller: Soldier, Strategist, and Writer, 1878–1966* (New Brunswick, NJ: Rutgers University Press, 1977), 115.

[35] James K. Womack, *Soviet Correlation of Forces and Means: Quantifying Modern Operations* (Fort Leavenworth, KS: School of Advanced Military Studies, U.S. Army Command and General Staff College, 1990), 13–14.

[36] Herfried Muenkler, *Ueber den Krieg. Stationen der Kriegsgeschichte im Spiegel ihrer theoretischen Reflexion* (Weilerswist: Velbrueck Wissenschaft, 2002), 128–129.

[37] William P. Baxter, *The Soviet Way of Warfare* (London: Brassey's Defence Publishers, 1986), 242.

[38] Cited in William G. Cummings, *Operational Design Doctrine: Hamstrung or Footloose in the Contemporary Operating Environment* (Toronto: Canadian Forces College, April 30, 2007), 74.

[39] U.S. Joint Forces Command, Joint Doctrine Series, Pamphlet 10, *Design in Military Operations. A Primer for Joint Warfighters* (Norfolk, VA: Joint Warfighting Center, September 20, 2010), 3.

[40] Ibid.

[41] Justin Kelly and David Kilcullen, "Chaos Versus Predictability: A Critique of Effects Based

Operations," *Australian Army Journal* 2, no. 1 (Winter 2004), 90.

[42] Carl von Clausewitz, *On War*, ed. and trans. Michael Howard and Peter Paret (New York: Knopf, 1993), 97.

[43] Womack, 84.

[44] Ibid., 2.

[45] Ibid., 32.

[46] Ibid., 81.

[47] Cited in M. Kirby and R. Capey, "The Air Defense of Great Britain, 1920–1940: An Operational Research Perspective," *The Journal of the Operational Research Society* 48, no. 6 (June 1997), 558.

[48] Bousquet, 141.

[49] Ibid., 149–150.

[50] Ibid., 151.

[51] Robert McNamara with Brian Vandemark, *In Retrospect: The Tragedy and Lessons of Vietnam* (New York: Random House, 1995), 237–238.

[52] Bousquet, 157.

[53] Dieter Stockfisch, "Im Spannungsfeld zwischen Technologiefortschritt und Fuehrungsverstaendniss. Auftragstaktik," *Marineforum* 12 (December 1996), 13.

[54] Gat, 144.

[55] Calhoun, 27.

[56] Cited in Gat, 154.

[57] Ibid., 155.

[58] Ibid., 156.

[59] Reinhard Hoehn, *Scharnhorts Vermaechtnis* (Bonn: Athenaum Verlag, 1952), 73.

[60] Gat, 168.

[61] Calhoun, 25.

[62] Ibid., 28.

[63] Ibid., 27.

[64] Trythall, 116–117.

[65] Clausewitz, 97.

[66] Michael Sheehan, "The Changing Character of War," in *The Globalization of World Politics: An Introduction to International Relations*, ed. John Baylis, Steve Smith, and Patricia Owens, 216, 4th ed. (Oxford: Oxford University Press, 2007).

[67] Clausewitz, 216.

[68] Ibid., 86.

[69] Cited in Beatrice Heuser, *Reading Clausewitz* (London: Random House, 2002), 81.

[70] Sheehan, 216.

[71] Cited in Ian Roxborough, "Clausewitz and the Sociology of War," *The British Journal of Sociology* 45, no. 4 (December 1994), 625.

[72] Clausewitz, 133.

[73] Ibid., 116.

[74] Cited in Roxborough, 625.

[75] Clausewitz, 96.

[76] Cited in Heuser, 89.

[77] Clausewitz, 95.

[78] Cited in Heuser, 88.

[79] Clausewitz, 139–140.

[80] Peter Paret, "Clausewitz," in *Makers of Modern Strategy: From Machiavelli to the Nuclear Age*, ed. Peter Paret, Gordon Craig, and Felix Gilbert, 202 (Princeton, NJ: Princeton University Press, 1986).

[81] Daniel Hughes, *Moltke on the Art of War: Selected Writings* (Novato, CA: Presidio Press, 1993), 172.

[82] Gabriel Serbu, "The Dangers of Anti-Intellectualism in Contemporary Western Armies," *Infantry* (November/December 2010), 45.

[83] Ibid., 47.

[84] Gat, 332.

[85] Hughes, 175.

[86] Bruce Condell and David T. Zabecki, eds., *On the German Art of War:* "Truppenfuehrung" (Boulder, CO: Lynne Rienner, 2001), 17.

U.S. Marine Forces Africa (Lydia M. Davey)

Nonlethal grenade used during Non-Lethal Individual Weapons Instructors Course, U.S. Africa Command

From Niche to Necessity

INTEGRATING NONLETHAL WEAPONS INTO ESSENTIAL ENABLING CAPABILITIES

By TRACY J. TAFOLLA, DAVID J. TRACHTENBERG, *and* JOHN A. AHO

Colonel Tracy J. Tafolla, USMC, is Director of the Joint Non-Lethal Weapons Directorate. David J. Trachtenberg is President and CEO of Shortwaver Consulting, LLC, and was Principal Deputy Assistant Secretary of Defense for International Security Policy from 2001 to 2003. Colonel John A. Aho, USMC (Ret.), is a Senior Policy Analyst at American Systems Corporation.

The Department of Defense (DOD) conducts U.S. military operations in accordance with internationally recognized and accepted laws and principles governing the use of armed force. Those laws demand that the employment of force be judicious, proportionate to the threat, and tempered wherever possible by the deliberate avoidance of noncombatant casualties. The principle of civilian casualty avoidance is embedded in the Fourth Geneva Convention of 1949 and reflects an agreement among civilized nations that, while highly destructive, warfare should not be conducted indiscriminately. Indeed, a new DOD Law of War Manual is being drafted, reinforcing America's adherence to these standards of conduct.

U.S. restraint in the application of lethal force is not unusual. For example, during North Atlantic Treaty Organization (NATO) operations against Serbia in 1999, thousands of Serbs acting as "human shields" stood on bridges in Belgrade and Novi Sad to protect the structures from allied bombing attacks that would have killed civilians and been a public relations disaster.[1] The U.S. military has sought to exercise restraint in operations in both Iraq and Afghanistan.[2] More recently, U.S. forces supporting NATO air operations against Libya took extensive precautions to avoid civilian casualties.[3]

contemporary military operations are unlike previous wars where success was measured in purely military terms

Contemporary military operations are unlike previous wars where success was measured in purely military terms. The importance of winning "hearts and minds" is now growing. Today's wars are mostly irregular conflicts fought not against countries but in complex environments against terrorists and extremists who wear no uniforms and operate within the civilian populace—often in a deliberate attempt to shield themselves from attack and maximize propaganda opportunities from civilian casualties.

Tomorrow's wars will likely see U.S. forces involved in a range of contingencies from traditional to irregular warfare operations. Former Secretary of Defense Robert Gates set DOD on course for a "rebalanced" military that is better postured to succeed in nontraditional operations while preparing for other types of contingencies. The recently released Strategic Defense Guidance notes that U.S. forces must be increasingly flexible and adaptable to deal with a dynamic security environment that "presents an increasingly complex set of challenges and opportunities."[4] In both asymmetric and conventional environments, avoiding noncombatant casualties has become increasingly important to the success of military operations. Nonlethal weapons can play a significant and strategic role in accomplishing this and helping to achieve mission success.

What Are Nonlethal Weapons?

A current working definition of *nonlethal weapons* is "weapons, devices, and munitions that are explicitly designed and primarily employed to incapacitate targeted personnel or materiel immediately, while minimizing fatalities, permanent injury to personnel, and undesired damage to property in the target area or environment. [Nonlethal weapons] are intended to have reversible effects on personnel or materiel."[5] DOD policy recognizes that the use of nonlethal weapons may occasionally result in injurious or lethal effects, though that is not the intended outcome. Their use reflects an approach to warfare that seeks to reconcile the objective of defeating the enemy with the moral imperative of sparing innocent lives.

The current generation of nonlethal weapons includes counterpersonnel and countermateriel capabilities used for controlling crowds or stopping or diverting vehicles on land and vessels at sea. They provide escalation-of-force options that allow U.S. forces to determine intent of potentially hostile individuals and groups and modify behavior.

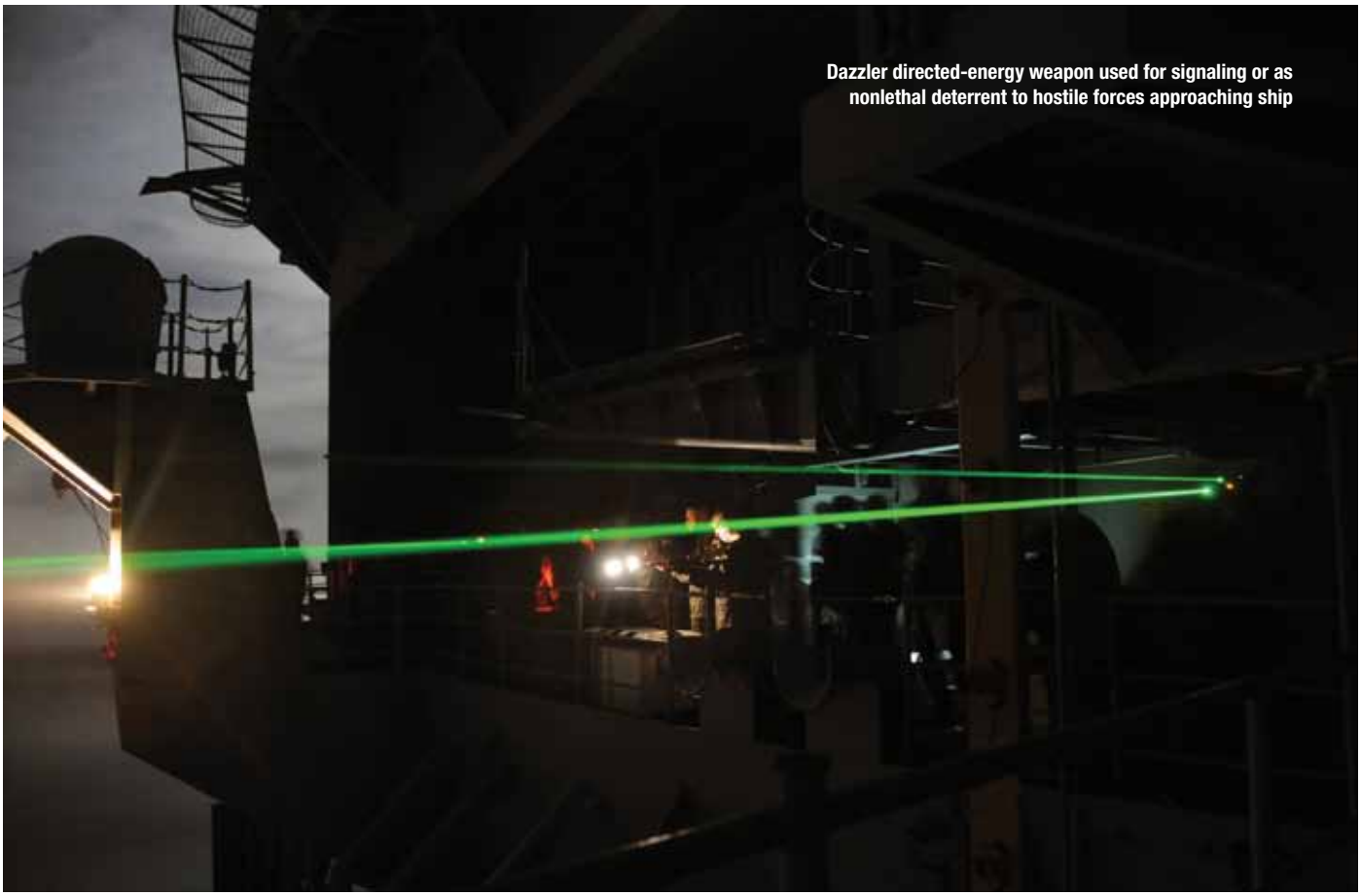
Examples of counterpersonnel systems currently used include *dazzling lasers*—optical distracters useful for temporarily overwhelming an adversary's visual sense by emitting a bright flash and glare effect—and *acoustic hailing devices* that emit loud warning tones or clear verbal commands over long distances. Also in use is an array of nonlethal munitions, grenades (and their delivery systems), and Tasers. Countermateriel systems include spike strips, caltrops (heavy-gauge steel-puncturing spikes), the Vehicle Lightweight Arresting Device, and Portable Vehicle Arresting Barriers and Running Gear Entanglers, designed to stop moving vessels.

More sophisticated nonlethal weapons are being developed with greater operational range, scalable to a variety of needs, to provide a layered defense against potential threats. These include airburst nonlethal munitions, pre-emplaced electric vehicle stoppers, and nonkinetic active-denial technology. Active-denial technology, which delivers precision nonlethal effects at extended ranges, offers promise in crowd control, area denial, and other applications. Active denial uses millimeter wave technology to create an invisible beam of directed energy that produces a strong heating sensation on the surface of the skin, which is completely reversible once an individual moves reflexively out of the beam's path.

Although applicable to a broad range of contingencies, nonlethal weapons are neither a panacea nor a substitute for lethal force, and this article is not meant to exaggerate the potential of nonlethal weapons to accomplish mission objectives. Their purpose is to complement the lethal capabilities in the warfighter's toolkit. Some current nonlethal systems have technical and operational limitations, including range, mobility, and weight considerations that necessitate tradeoffs and impact their usefulness and operational suitability to the warfighter. Those limitations, however, can be reduced through targeted investments in science and technology.

Challenges and Roadblocks

DOD began to focus coherent attention and resources on developing nonlethal capabilities as an outgrowth of U.S. humanitarian assistance efforts in Somalia in 1995, which highlighted a need for capabilities short of lethal means. In 1996, Congress directed the establishment of an executive agent for the DOD Non-Lethal Weapons Program in order to provide oversight on joint nonlethal matters, maintain insight into the various independent Service efforts, eliminate duplication and program redundancies, and facilitate the fielding of nonlethal weapons capabilities. The commandant of the Marine Corps was given this task, and the Joint Non-Lethal Weapons Directorate was established to conduct day-to-day management of joint programs and coordination of Service-unique programs on behalf of the executive agent.



Dazzler directed-energy weapon used for signaling or as nonlethal deterrent to hostile forces approaching ship

U.S. Navy (Luciano Marano)

Since then, significant progress has been made in developing nonlethal technologies and fielding existing off-the-shelf capabilities. Despite their relevance to today's contingency operations, however, nonlethal weapons remain an underutilized asset. Institutional resistance, bureaucratic inertia, competition with legacy programs for funding, inadequate training, doctrinal shortcomings, unclear requirements from the Services, and practical impediments to fielding—such as technological hurdles and insufficient quantities of nonlethal systems with greater standoff range—have impeded a more thorough integration of nonlethal capabilities into the total force. In addition, fostering a greater understanding of the role and utility of nonlethal weapons as an irregular warfare enabler, vice a niche capability commonly associated with force protection missions, remains a significant challenge.

The total cost of the DOD Non-Lethal Weapons Program, including all joint and Service-specific investment, is roughly $140 million annually. Yet the return on this investment can be disproportionate in terms of civilian lives saved, mission objectives achieved, strategic goals accomplished, and international support attained among allies and partners who appreciate efforts to protect civilians. Unfortunately, nonlethal weapons have not yet been fully embraced by military leadership and the policy community.

Importantly, in some quarters of the military, there is a cultural aversion to nonlethals. This is understandable in light of the military's training as a fighting force whose mission includes locating, closing with, and destroying the enemy. It requires a shift in mindset to convince the Nation's warriors that employing tools that allow for mission accomplishment without loss of life or highly destructive lethal fires where possible will not weaken the force.

Without a broader-based understanding of their value and a stronger commitment to their fielding, nonlethal weapons are unlikely to recognize their full potential for meeting the requirements of U.S. military strategy or the operational dictates of contingency operations.

Game-changers and Champions

Translating new, cutting-edge technologies into fielded systems has historically been difficult. Though the Global Positioning System (GPS) is ubiquitous today, its future was far from assured during its initial development. GPS was criticized as costly and unnecessary, a General Accounting Office[6] (GAO) report was highly critical, and its budget was cut. The individual Services pursued their own incompatible navigation and timing options. It was only through the vision of GPS advocates that funding was restored and the program was successful.

Similarly, as the importance of unmanned aerial vehicles (UAVs) to intelligence, surveillance, and reconnaissance missions has increased, so has resistance to shifting budgetary resources away from manned to unmanned platforms. Yet despite an initial reluctance to fund aircraft without pilots, the Air Force today "is training more pilots for advanced UAVs than for any other single weapons system."[7]

History is replete with similar examples where visionary approaches encountered

practical roadblocks. Billy Mitchell's vision of decisive airpower independent of land and sea forces was roundly criticized. And while today's operations continue to demonstrate naval and land force indispensability, many credit Mitchell's vision as a key contributor in the development of the modern-day aircraft carrier and widespread acceptance and employment of carrier-based air combat—an outcome that would have been unlikely in the absence of a high-level commitment to the concept.

The future of military technologies is often driven by cost, yet too often cost is confused with value. GPS, UAVs, and the aircraft carrier have proven their value despite the relative expense of developing them. Similarly, the value of nonlethal weapons for meeting mission requirements in today's challenging and complex military operational environments may outweigh the costs of developing these novel technologies.

Lessons for Tomorrow

The utility of nonlethal weapons in irregular conflicts, peacekeeping, and humanitarian operations is more than theoretical. As retired Lieutenant General Emil R. Bedard, USMC, has noted, "Every warfighter eventually realizes that non-lethal weapons are vital in creating the effects needed to defeat an adversary."[8] Their use in Somalia in the mid-1990s was credited with dissuading mob violence that previously had led to violent clashes between U.S. forces and Somali demonstrators.[9] During peacekeeping operations in Kosovo in 2000, U.S. forces effectively diffused an explosive situation by using nonlethal weapons during a confrontation with a crowd of hostile Serbs in the town of Sevce.[10] And in Afghanistan and Iraq, nonlethal weapons have played an important role. As one Army officer noted, their use "sends a strong message without the need to employ deadly force."[11]

Though important for irregular warfare missions such as counterinsurgency, nonlethal weapons have much broader applicability across the full range of military operations. For example, as a counterpiracy capability, the use of nonlethal counterpersonnel tools such as the acoustic hailing device not only prevented the hijacking of two vessels in the Gulf of Aden within 24 hours of each other, but also enabled the capture of 16 pirates without injury to them or to crew members[12]—a telling demonstration of their value in combating piracy and saving lives.

As the U.S. military is called upon to assist in humanitarian assistance/disaster relief operations overseas, nonlethal weapons can also be useful for crowd control and to deescalate tensions before violence erupts, helping U.S. forces maintain order during the distribution of food, water, and medical supplies to survivors after a natural disaster.

Future concepts of warfare may dictate the need for more innovative approaches to meeting mission requirements, placing greater stresses on commanders' freedom of maneuver and freedom of fires as well as flexibility and versatility in the force's response capabilities. And any future vision for nonlethal weapons must include a fully integrated inventory of scalable effects capabilities in which an individual weapons system can be "dialed up" commensurate with the scenario faced. The ability to isolate and segregate appropriate targets through nonlethal means may take on added importance, along with the ability to deny an adversary from seeing, hearing, communicating with, or reinforcing troops on the battlefield.

the ability to temporarily deny an adversary's use of infrastructure through nonlethal means allows it to be reactivated later

Because nonlethal weapons are applicable to a broad range of missions the U.S. military is likely to encounter, their potential utility across the range of military operations is increasing. To meet this growing utility, their transformation from force protection tool to force application capability to complement lethal effects is required, along with their institutionalization across the doctrine, organization, training, materiel, leadership and education, personnel, and facilities domains. Eventually, they may become as essential an enabler of mission success as GPS.

Tactical Uses, Strategic Impacts

The 2011 National Military Strategy emphasizes the importance of civilian casualty avoidance: "The risk we assume by minimizing collateral damage to innocents is balanced by a reduction of risk to turning even more people against our broader mission. Thus, the disciplined application of force is consistent with our values and international law, increases our chances of strategic and operational success, and more effectively advances national policy."[13] Nonlethal weapons are responsive to the National Military Strategy's direction.

In Afghanistan, civilian casualty avoidance has become a central warfighting requirement. The tactical directive governing the use of force acknowledges that civilian casualties have "strategic consequences" and calls the protection of Afghan civilians "a moral imperative."[14] It states, "*Every Afghan civilian death diminishes our cause* [emphasis in original]. If we use excessive force or operate contrary to our counterinsurgency principles, tactical victories may prove to be strategic setbacks."[15]

The negative consequences of civilian casualties are magnified by the instantaneous transmission of information, enabled by technology, and driven by the demands of an instant news cycle. Video and images of grieving families and destroyed homes can exacerbate negative perceptions of American military might. Greater reliance on nonlethal weapons can help mitigate this effect.

The tactical employment of nonlethal weapons can have other strategic benefits. For example, the ability to temporarily deny an adversary's use of infrastructure through nonlethal means not only allows it to be reactivated at a later date but also saves money in the long run by avoiding the need to rebuild. Likewise, employment of nonlethal devices or nondestructive fires to prevent enemy vehicles from crossing a bridge means that the bridge need not be destroyed by costly munitions. It also allows it to be used by friendly forces, thus avoiding future U.S.-borne reconstruction costs.

Estimates of the U.S. costs of reconstruction in Iraq highlight the strategic benefit that could be provided by the wider use of nonlethal weapons. By March 2011, the United States had spent approximately $61 billion on Iraq reconstruction, which included repair to economic infrastructure damaged in the conflict (for example, restoring electricity, communications, transportation, water, oil, and gas).[16] While not all of these costs could have been prevented through more extensive use of nonlethal capabilities, significant expenses might have been avoided if damage to Iraq's infrastructure had been minimized

U.S. Marine Corps (Daniel Balmer)

Marine demonstrates capabilities of X26E Tazer

by the application of appropriate and effective nonlethal technologies and capabilities.

Likewise, in Afghanistan, the costs of reconstruction to the U.S. taxpayer have been significant, with the Special Inspector General for Afghanistan Reconstruction reporting that these costs have exceeded $85.5 billion.[17] While some of these costs are directed toward establishing civil governance institutions and other elements essential to the building of a democratic society, some portion of this spending has been allocated to repair and rebuild property and infrastructure damaged or destroyed in the counterinsurgency.

In addition, monetary restitution to grieving family members when innocents are accidently killed and the costs of sheltering those whose property is destroyed in kinetic engagements could be minimized through the wider application of nonlethal means.

In short, the use of nonlethal weapons can have a strategic "multiplier effect" by avoiding collateral damage to property and infrastructure, minimizing unintended civilian casualties, overcoming negative perceptions of the United States, denying opportunities for enemy propaganda victories, and minimizing long-term reconstruction costs. Perhaps no other capability allows for a broader range of employment options across a wider spectrum of contingencies with the capacity to affect outcomes from the tactical level to the strategic.

The Afghanistan Experience

Nearly a decade after the start of Operation *Enduring Freedom*, noncombatant casualties continue to strain the U.S.-Afghan relationship, undermining efforts to develop the trust and confidence of the Afghan people. This strain was recognized by International Security Assistance Force Commander General John R. Allen, who noted in his 2011 Tactical Directive that "Every civilian casualty is a detriment to our interests and those of the Afghan government, even if insurgents are responsible. We must redouble our efforts to eliminate the loss of innocent civilian life. . . . We must never forget that the center of gravity in this campaign is the Afghan people; the citizens of Afghanistan will ultimately determine the future of their country."[18] Former Chairman of the Joint Chiefs of Staff Admiral Mike Mullen warned, "Lose the people's trust, and we lose the war."

Civilian casualties in Afghanistan rose 15 percent from 2009 to 2010 and another 8 percent from 2010 to 2011,[19] yet three out of four civilian casualties are caused by Taliban and insurgent forces.[20] Nevertheless, so-called escalation-of-force incidents are the primary cause of civilian casualties by coalition forces.[21] Many occur at entry control points, convoys, and other controlled access areas. As former International Security Assistance Force (ISAF) Commander General David Petraeus noted, "Counterinsurgents cannot succeed if they harm the people they are striving to protect."[22] Wider use of nonlethal capabilities in such scenarios could mitigate this risk, allowing U.S. forces who must make split-second decisions to "pull the bullet back" should they engage suspicious individuals later deemed to be noncombatants.

Although some U.S. forces in Afghanistan are equipped with nonlethal capabilities, their overall availability remains limited. As General Joseph Dunford, assistant commandant of the Marine Corps, has stated, the "demand for effective nonlethal weapons right now exceeds the inventory. . . . Squads and platoons that are interacting with people [in Afghanistan] want to take decisive action but limit the possibility of injuring civilians."[23]

U.S. combatant commands have sought to expand the availability of nonlethal weapons, though progress has been slow. Recent surveys of deployed units indicate significant shortfalls in nonlethal weapons education, knowledge, training, and availability. Accordingly, U.S. Central Command recently reemphasized predeployment training requirements for nonlethal weapons.

Without Service institutionalization of nonlethal weapons training and equipping, deployed forces will continue to be called upon to exercise what some have called "courageous restraint" to minimize unintended casualties and damage. While such restraint has contributed to a 26 percent drop in the number of coalition-caused civilian casualties, it has also been controversial, raising concerns that it limits the ability of troops to protect themselves and thus increases their risks. Some have noted that restraint in the application of lethal force on ethical grounds "transfers risk" from enemy combatants and noncombatants to U.S. forces and that this creates "a false dilemma where one must choose between non-combatant lives, which have value, and soldiers' lives, which do not."[24] Here, also, the greater availability of nonlethal weapons may help alleviate these concerns.

The effects of unintended civilian casualties reach beyond the local population. The accidental killing of innocents can have a traumatic effect as well on young troops who must forever live with the consequences of their actions. The United States must do all it can to provide its uniformed men and women in harm's way with the tools they need to complete the mission and avoid inadvertent death or injury to noncombatants.

Setting the Record Straight

Communicating effectively about nonlethal weapons and how they can assist the warfighter in achieving the objectives of U.S. military strategy is a critical prerequisite to gaining acceptability and support for these capabilities. This effort, however, will be handicapped without the more active engagement of senior-level military and civilian leaders.

Accepting nonlethal weapons as an integral element of the warfighter's toolkit requires a cultural shift that is counterintuitive to the military, which understandably emphasizes the use of lethal force. As former Army Vice Chief of Staff General Peter Chiarelli noted, "if we're really serious about fighting an insurgency, we have to change our culture and accept the importance, and sometimes preeminence, of non-lethal effects."[25] This is not the equivalent of "dumbing down" U.S. military capabilities. Nor is it a reflection of what some have called a "softer military."[26] As former USCENTCOM Commander General Anthony Zinni, USMC, noted, "Non-lethal weapons when properly applied . . . make the United States more formidable, not less so."[27]

Unfortunately, misunderstandings and mischaracterizations of the effects of nonlethal weapons are common. New technologies often raise ethical, cultural, and political concerns. The challenge of deploying a new technology is that it is not well understood and is easily subject to mischaracterization, especially in underdeveloped societies where cultural, ethnic, and religious differences may be exploited for political purposes by America's adversaries.

In response to a request from an operational commander, an Active Denial System was shipped outside of the continental United States—and was later ordered to return stateside, having never been used. Although the system has been demonstrated as safe in more than 11,000 tests on 700 human volunteers and does not cause any long-term or permanent health issues, the newness of the technology, coupled with concerns over its mischaracterization as a "microwave" weapon that "fries," "cooks," or sterilizes its targets, resulted in a lack of willingness to employ it. This experience highlights the power of perceptions to shape policy and reinforces the importance of ensuring they are based on fact rather than myth.

Shaping the information environment is just as important as shaping the military environment. Strategic communication is essential for generating understanding and advocacy of technological solutions to contemporary military/operational issues. A bottom-up approach, including at the unit level, is a necessary but not sufficient condition for success in achieving greater acceptance and integration of nonlethal weapons capabilities into current and future military planning and operations. The value of these capabilities must also be communicated from the top down.

restraint in the application of lethal force on ethical grounds "transfers risk" from enemy combatants and noncombatants to U.S. forces

Signs of Progress

Notwithstanding the limitations of current systems and the challenges noted above, there appears to be a broad-based foundation of support for greater investment in and employment of nonlethal weapons—from senior leadership to deployed units to policymakers and opinion leaders. Several combatant commanders have now included nonlethal weapons on their annual Integrated Priorities List. General Chiarelli has also noted that "In a counterinsurgency, non-lethal effects are as important as—and, at times, more important than—kinetic effects."[28] Then–Major General Richard Mills, commander of ISAF's Regional Command–Southwest, stated, "I am a supporter of non-lethal weapons. I would like to see some suite of those weapons provided to us over here."[29] At the unit level, one Army officer who served in Iraq and Afghanistan commented, "To back away from applying non-lethal weapons in irregular warfare risks sending the message that the United States is incapable of either developing [a nonlethal weapons] arsenal or determining how to employ [nonlethal weapons], or is reluctant to attempt a form of warfare that involves dealing with dissatisfied people as human beings and not simply as targets."[30]

Congress has also expressed bipartisan support for nonlethal weapons. The Ike Skelton National Defense Authorization Act for Fiscal Year 2011 called for the procurement and fielding of nonlethal capabilities to "improve military mission accomplishment and operational effectiveness" in counterinsurgency operations.[31]

The House Armed Services Committee (HASC) in particular has highlighted "the value of non-lethal weapons in reducing risks to the warfighter and to non-combatants in current and prospective contingency operations."[32] The committee urged DOD "to accelerate its effort to field such systems, including active denial technologies; to ensure adequate funding for the non-lethal weapons science and technology base; and to develop policy, doctrine, and tactics for their employment."[33] The HASC also expressed concern that DOD "does not fully appreciate the important role non-lethal capabilities can play in helping to ensure mission success," arguing that "budgetary trends do not reflect an urgent need for non-lethal capabilities."[34]

U.S. Army (Martin Greeson)

M5 Modular Crowd Control nonlethal munition used to incapacitate large groups with flash bang and impact of rubber balls

U.S. Army (Phillip Valentine)

Soldier loads 40mm nonlethal rounds into launching system during training in Iraq

In 2004, the Council on Foreign Relations called for "incorporating . . . nonlethal capabilities more broadly into the equipment, training, and doctrine of the U.S. armed services," concluding that doing so "could substantially improve the United States' ability to achieve its goals across the full spectrum of modern war."[35] In 2007, a RAND study highlighted the "inadequacy" of nonlethal capabilities and the negative political fallout from killing noncombatants.[36] In 2009, RAND called for a range of capabilities that are scalable for maximum effectiveness, concluding that "creating and mainstreaming this capability requires vision, initiative, commitment, and persistence on the part of those soldiers' civilian and military leaders."[37] And Brookings Institution scholar Michael O'Hanlon has argued, "Rather than ask our troops to make a choice between being at risk and taking actions that could kill innocent Afghans and set back the war effort, we should give them the [nonlethal] tools they need to do their job."[38]

More recently, a report by the Center for Strategic and Budgetary Assessments noted that nonlethal weapons—including directed-energy technologies—can play a valuable role in countering the antiaccess/area-denial strategies of adversaries.[39] It is precisely these kinds of threats that the new Defense Strategy Guidance argues the United States is increasingly likely to confront.[40] Moreover, the employment of nonlethal capabilities to support antiaccess/area-denial operations is recognized in the new Joint Operational Access Concept.

Conclusion

Many future conflicts are likely to be unconventional and irregular and take place in environments where it is difficult to distinguish between combatants and noncombatants. Conventional operations may also occur in urban environments within close proximity to civilians and critical infrastructure. In these circumstances, nonlethal weapons can play an increasingly useful role in support of U.S. military goals and objectives. Yet this transformation is unlikely to happen without a greater understanding of the tactical and strategic benefits of these weapons.

Nonlethal weapons are not a substitute for the application of lethal force. When employed, nonlethal weapons are always backed by lethal means. As an adjunct to lethal force, however, they can be a powerful addition to the warfighter's toolkit. For example, nonlethal weapons can:

- close the gaps in existing counterpersonnel and countermateriel capabilities
- create a more capable and versatile force without loss of lethality
- help determine intent and provide important deescalatory options for warfighters between shouting and shooting
- avoid negative consequences that could emerge as a result of the use of lethal force including to young troops where the costs of a wrong decision on the use of force can be psychologically devastating
- be applicable to anticipated contingencies and changes in the strategic environment
- conform to U.S. military strategy
- be consistent with the moral principles that guide U.S. military actions
- reflect an American approach to war that is compliant with international law and its requirement to use force judiciously, proportionately, and discriminately
- reduce unintended civilian casualties and inadvertent damage to property
- avoid expensive reconstruction costs associated with rebuilding infrastructure damaged as a result of traditional kinetic military operations
- help achieve mission success.

To accomplish these objectives, the value of nonlethal weapons must be better appreciated by everyone from the civilian and military leadership down to the operator on the battlefield. Because of their transformative strategic benefits across a range of military operations, the role nonlethal

weapons can play in likely future contingencies should be explicitly referenced in policy and strategy documents such as the Quadrennial Defense Review.[41] Persistent myths must be dispelled with dispassionate reasoning and reliance on facts.

nonlethal weapons provide capabilities with unique value that may offset their monetary cost

Nonlethal weapons must be affordable, reliable, and scalable to circumstances. They should be operationally effective, suitable to a variety of scenarios, adaptable to current weapons systems, and provide improved capabilities and increased range. Moreover, they must be available in sufficient quantities to make their investment worth the cost.

All of the Services must integrate nonlethal weapons more broadly into their doctrines, training, exercises, and deployments. Greater acceptability of nonlethal capabilities will not occur unless forces are properly trained and equipped to use them. They should be treated as an integral component of the warfighter's capabilities from the beginning, not a costly add-on down the road. Integration of nonlethal weapons can enable greater freedom of maneuver for the force and will enhance the array of fires available to facilitate the offense.

The capabilities provided by nonlethal weapons can help enable mission success across the full spectrum of conflict—from irregular warfare to more traditional contingencies—and the forces likely to benefit from their employment must take the lead in demonstrating their utility. In this regard, the importance of tracking and highlighting incidents where nonlethal weapons have avoided the consequences of using deadly force and successfully deescalated the potential for violence cannot be overestimated.

Most importantly, cost should not be confused with value. Nonlethal weapons provide capabilities with unique value that may well offset their monetary cost. Recognition of this fact is needed to develop the requisite levels of advocacy and sustained funding that allow them to be integrated more fully into the "rebalanced" force of the future.

Finally, there is no substitute for senior-level advocacy in shaping the environment within the defense bureaucracy, among key decisionmakers and leaders, and throughout the general public. Such advocacy is essential to highlight the growing relevance of nonlethal technologies and the ability of nonlethal weapons to help achieve the objectives of U.S. military strategy. Although the top military and civilian leadership of DOD has acknowledged the importance of avoiding noncombatant casualties to mission success, there has yet to be an explicit public articulation of the role nonlethal weapons can play in accomplishing this task. That would be an important step as DOD reconciles its military strategy, plans, and programs with fiscal realities.

Like our experiences with the Global Positioning System and the unmanned aerial vehicle, the transformation of nonlethal weapons from a niche capability to one with scalable effects useful across the spectrum of contingencies depends on those with the vision to see their broad-based, across-the-board utility in helping achieve mission success. And their effective integration into the warfighter's toolkit will not only help us achieve our strategic and tactical goals and objectives but will also help us remain true to our core values as a nation. **JFQ**

NOTES

[1] "Human Chains Guard NATO Targets," BBC News, April 9, 1999, available at <news.bbc.co.uk/2/hi/europe/314953.stm>.

[2] See, for example, George Will, "Futility in Afghanistan: An NCO Fires Off a Round of Illumination," *Jewish World Review*, June 20, 2010, available at <www.jewishworldreview.com/cols/will062010.php3>.

[3] Cheryl Pellerin, "Gates Cites Efforts to Avoid Civilian Casualties in Libya," American Forces Press Service, March 23, 2011, available at <www.army.mil/article/53647/Gates_cites_efforts_to_avoid_civilian_casualties_in_Libya/>.

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

[5] This updated definition appears in DOD Directive 5210.56, "Carrying of Firearms and the Use of Force by DOD Personnel Engaged in Security, Law and Order, or Counterintelligence Activities," available at <www.dtic.mil/whs/directives/corres/pdf/521056p.pdf>. Nonlethal weapons have also been referred to by some, including within the law enforcement community, as "less lethal" or "less than lethal" weapons. In 1996, the term "nonlethal weapons" was established in DOD lexicon and formally codified in DOD Directive 3000.3, "Policy for Non-Lethal Weapons," available at <www.dtic.mil/whs/directives/corres/pdf/300003p.pdf>. The term *non-lethal weapons* also appears in Joint Publication 1-02, *DOD Dictionary of Military and Associated Terms* (Washington, DC: The Joint Staff, November 8, 2010, as amended through March 15, 2012), available at <www.dtic.mil/doctrine/dod_dictionary/>. Admittedly, the term is not always a best fit in describing the capability and is arguably unappealing to the combat arms community. The continued expansion of the nonlethal weapons portfolio may require reconsideration of the term.

[6] The General Accounting Office was subsequently renamed the Government Accountability Office.

[7] Secretary of Defense Robert M. Gates, speech at the U.S. Air Force Academy, Colorado Springs, CO, March 4, 2011.

[8] E.R. Bedard, *Non-Lethal Capabilities: Realizing the Opportunities*, Defense Horizons 9 (Washington, DC: NDU Press, March 2002), 1.

[9] Cited by Paul R. Capstick, "Non-Lethal Weapons and Strategic Policy Implications for 21st Century Peace Operations" (Carlisle, PA: U.S. Army War College, February 26, 2001), 9.

[10] As a commanding officer of the U.S. peacekeeping contingent stated, "The non-lethal rounds achieved a tremendous effect: Everyone backed up immediately and settled down." See Lieutenant Colonel James Brown, commanding officer of the Army's 709th Military Police Battalion, quoted in Eric Adams, "Shoot to Not Kill," *Popular Science* (May 2003), 90.

[11] Colonel Douglas A. Tamilio, Project Manager for Soldier Weapons, cited in DOD Non-Lethal Weapons Program, *Non-Lethal Weapons for Today's Operations* (Quantico, VA: DOD, 2011), 11, available at <www.jnlwp.usmc.mil/misc/publications/AR2011.pdf>.

[12] Ibid., 9.

[13] *The National Military Strategy of the United States of America* (Washington, DC: Joint Chiefs of Staff, February 2011), 7.

[14] International Security Assistance Force News Release 2010-08-CA-004, "General Petraeus Issues Updated Tactical Directive: Emphasizes 'Disciplined Use of Force,'" August 1, 2010, available at <http://smallwarsjournal.com/documents/isafnewsrelease2.pdf>.

[15] Ibid.

[16] Special Inspector General for Iraq Reconstruction, *Quarterly Report to the United States Congress*, April 30, 2010, available at <www.sigir.mil/files/quarterlyreports/April2010/Report_-_April_2010.pdf>.

[17] Special Inspector General for Afghanistan Reconstruction, *Quarterly Report to the United*

States Congress, April 30, 2012, available at <www.sigar.mil/pdf/quarterlyreports/2012-04-30qr.pdf>.

[18] COMISAF's Tactical Directive, November 30, 2011, available at <www.isaf.nato.int/images/docs/20111105%20nuc%20tactical%20directive%20revision%204%20%28releaseable%20version%29%20r.pdf>.

[19] See Alissa J. Rubin, "Taliban Causes Most Civilian Deaths in Afghanistan, U.N. Says," *The New York Times*, March 9, 2011, A15, available at <www.nytimes.com/2011/03/10/world/asia/10afghanistan.html?_r=1&scp=3&sq=afghan&st=cse>. Also see United Nations (UN) Assistance Mission in Afghanistan and Afghanistan Independent Human Rights Commission, *Afghanistan: Annual Report 2010—Protection of Civilians in Armed Conflict*, March 2011, available at <http://unama.unmissions.org/Portals/UNAMA/human%20rights/March%20PoC%20Annual%20Report%20Final.pdf>; and UN Assistance Mission in Afghanistan Press Release, "Civilian Casualties Rise for Fifth Consecutive Year in Afghan Conflict," February 4, 2012, available at <http://unama.unmissions.org/Default.aspx?tabid=1741&ctl=Details&mid=1882&ItemID=16242>.

[20] UN Assistance Mission in Afghanistan Press Release.

[21] See Dan Fox, "Improving Capabilities for Joint Urban Operations," PowerPoint briefing, U.S. Joint Forces Command, 2007.

[22] Statement of General David H. Petraeus before the Senate Armed Services Committee, March 15, 2011, 9, available at <http://armed-services.senate.gov/statemnt/2011/03%20March/Petraeus%2003-15-11.pdf>.

[23] James K. Sanborn, "Dunford: Marines Will Continue to Be Needed," *Marine Corps Times*, April 14, 2011, available at <www.marinecorpstimes.com/news/2011/04/marine-dunford-conference-041411w/>.

[24] See, for example, Tony Pfaff, "Risk, Military Ethics, and Irregular Warfare," Foreign Policy Research Institute E-Notes, December 2011.

[25] Cited in Richard L. Scott, "Non-Lethal Weapons and the Common Operating Environment," *Army Magazine* (April 2010), 22.

[26] Bedard, 2.

[27] See Dennis B. Herbert, "Non-Lethal Weaponry: From Tactical to Strategic Applications," *Joint Force Quarterly* 21 (Spring 1999), 89.

[28] Scott, 22.

[29] Dan Lamothe, "2-Star Supports More Use of Non-Lethal Weapons," *Marine Corps Times*, February 2, 2011, available at <www.marinecorpstimes.com/news/2011/02/marine-corps-afghanistan-tasers-nonlethal-weapons-020110/>.

[30] Scott, 21.

[31] See Section 1078 of the Ike Skelton National Defense Authorization Act for Fiscal Year 2011 (Public Law 111-383), January 7, 2011, available at <www.gpo.gov/fdsys/pkg/PLAW-111publ383/pdf/PLAW-111publ383.pdf>.

[32] *Report of the Committee on Armed Services, House of Representatives, on H.R. 2647, National Defense Authorization Act for Fiscal Year 2010*, Report 111-166, June 18, 2009, 235.

[33] Ibid.

[34] *Report of the Committee on Armed Services, House of Representatives, on H.R. 5136, National Defense Authorization Act for Fiscal Year 2011*, Report 111-491, May 21, 2010, 228.

[35] Graham T. Allison et al., *Non-Lethal Weapons and Capabilities*, Report of an Independent Task Force (New York: Council on Foreign Relations, 2004), v.

[36] See David C. Gompert et al., *War by Other Means: Building Complete and Balanced Capabilities for Counterinsurgency*, RAND Counterinsurgency Study, Final Report, MG-595/2-OSD (Santa Monica, CA: RAND, 2008).

[37] See David C. Gompert et al., *Underkill—Scalable Capabilities for Military Operations and Populations* (Santa Monica, CA: RAND, 2009), 133.

[38] Michael E. O'Hanlon, "Troops Need Not Shoot in Afghanistan," The Brookings Institution, Washington, DC, April 23, 2010, available at <www.brookings.edu/opinions/2010/0423_afghanistan_ohanlon.aspx>.

[39] Mark Gunzinger with Chris Dougherty, *Outside in: Operating from Range to Defeat Iran's Anti-Access and Area-Denial Threats* (Washington, DC: Center for Strategic and Budgetary Assessments, January 2011).

[40] DOD, *Sustaining U.S. Global Leadership*.

[41] Some progress has been made in integrating nonlethal weapons into a number of DOD guidance documents. For example, the Joint Operating Concept for Countering Irregular Threats published in 2011 declared, "Most activities to counter irregular threats will not be primarily combat operations led by joint task forces but rather nonlethal activities conducted with other partners." See DOD, *Irregular Warfare: Countering Irregular Threats Joint Operating Concept*, version 2.0 (Washington, DC: DOD, May 17, 2010), 27, available at <www.dtic.mil/futurejointwarfare/concepts/iw_joc2_0.pdf>.

U.S. Navy (Julio Rivera)

MV-22 Osprey takes off from USS *Bataan* in Mediterranean

The V-22 Osprey

FROM TROUBLED PAST TO VIABLE AND FLEXIBLE OPTION

By ERIC BRAGANCA

After a few years of staying out of the limelight, the V-22 is back in the news because of a recent crash in Morocco that claimed the lives of two Marines and as the object of press and congressional inquiries for possible budget cuts.[1] After 10 years of expanding defense spending, military programs are again challenged to justify their funding and existence. American involvement in Iraq is over, Osama bin Laden is dead, and the President has vowed to begin withdrawing from Afghanistan soon. Does America still need the V-22? Yes. The American people deserve the best value for their dollar on any program during any time period despite any budget realities, and the V-22 has slowly and quietly become a solid, efficient performer. But there are still critics who do not know the quiet truths about the V-22.[2] It has an enviable safety record (despite the most recent crash), is cost-efficient, and has the flexibility to take on new roles and missions to handle our continued global security demands. No single aircraft is the answer to all of America's needs, but the V-22 offers the best troop-transport capability now and through the next decade.

Surprising Safety Record

Many who are familiar with the history of the V-22 recall the early years of its development when a series of high-profile crashes nearly caused the Department of Defense (DOD) to cancel the program. Richard Whittle, in *The Dream Machine*,[3] gives an excellent accounting of those days and the terrible impact they had on the people involved. The new tilt-rotor design and challenging military requirements demanded numerous compromises to save weight and increase speed as well as survivability in combat environments. A series of crashes and the tragic

Lieutenant Colonel Eric Braganca, USAF (Ret.), is a Consultant on Joint Operations with Whitney Bradley and Brown. His last military assignment was as Chief Systems Engineer for the CV-22 in the Joint Program Office.

loss of lives as the program rushed to meet military timelines caused a redesign of critical components. The "new" V-22 began flying again in 2001 and has slowly become one of the safest combat aircraft in the Marine Corps inventory. The redesign of some key areas of the aircraft in 2000 and 2001 made a dramatic improvement in the safety of the aircraft. These improvements made an immediate, although unheralded, improvement in its safety. The V-22 went from near extinction to becoming one of the safest aircraft in the Marine vertical-lift inventory. The Marine Corps accident rate for all of its aircraft since 2001 (the last 10 years) is just under 2.5 mishaps for every 100,000 flight hours.

Before Morocco, the Osprey's crash rate was half that and slightly better than the venerable CH-46, which it is replacing in Marine squadrons. To have a new aircraft with a radically new design sustain a 10-year safety record better than other aircraft that are much better understood is exceptional. Even with the Morocco fatalities, the V-22 accounts for only 6 deaths out of the 600+ that have occurred in rotary-wing mishaps since 2001. Rotary-wing operations remain highly dangerous, and the V-22 is no exception. Ospreys have flown over 100,000 flight hours with over half of that coming in the last 3 years. During that time, V-22s have completed numerous deployments to Iraq, Africa, and Afghanistan, and also have performed exceptionally well in high-profile missions such as the rescue of an American pilot in Libya and supporting the bin Laden raid in Pakistan.

In the last few years, the V-22 experienced fires around the engines due to leaking hydraulic fluid dripping onto hot metal. Because the V-22 has an engine and rotor system that tilts during every takeoff and landing, there are larger and different stresses put on components in those areas than in other aircraft. In response to those problems, government and aircraft manufacturers implemented hardware and software changes to detect and prevent the leaks. Initially, the fixes just notified the crew that the hydraulic system was about to leak and shut down that part of the system. Follow-on improvements installed better hydraulic lines in key areas, which prevented the leaks. After a series of tests, engineers learned that a blower, driven by the hydraulics, was causing extreme pressure changes in the hydraulic system. This blower is soon to be replaced throughout the fleet even though the aircraft has not experienced an engine fire since the improved hydraulic lines have been installed. While the improved lines are good, the new blower will prevent the hydraulic pressure changes and is an even better solution. The crews and passengers who fly in the V-22 deserve this level of safety and protection, and they are now getting it. Furthermore, improving safety continues to be a part of the V-22 program.

Before the Marine crash, which is still under investigation, the Air Force lost a CV-22 in April 2010 during a combat mission in Afghanistan supporting special operations forces. This crash was terrible for the families who lost loved ones, but it did highlight how far the V-22 has come in openness and trust in the aircraft by the people who fly it and fly in it. Sadly, 4 people died, but 16 survived even though the aircraft broke apart during the catastrophic impact with the ground. The joint command responsible for the mission launched the CV-22 that night into a challenging weather environment in a remote mountainous target area against a hostile force. They were confident that the V-22 was capable and safe. Two Air Force safety boards reviewed the crash circumstances and found that the extreme environment—high altitude, darkness, and featureless terrain—was the most likely cause of the crash. While one of the boards suggested an engine failure might have contributed, the board lacked evidence. A joint government and industry technical investigation of one of the engines indicated no failure; the other engine was not recovered. A government review of the crash data (speed, altitude, fuel status) showed that an engine failure was highly unlikely and would not have caused the crash. Based on that technical review, Air Force Special Operations Command publicly discounted an engine failure as the cause.[4] The CV-22 returned to combat missions a few days after the crash and continued operating in the extreme Afghanistan environment without incident—the commanders, crews, and passengers did not lose faith in the aircraft. The V-22 community did not shy away from open and public scrutiny of the safety or usefulness of the aircraft.

Numerous other claims about the V-22 have proven untrue. Some claims seemed superficially credible until examined more closely. One completely false claim was that the V-22 would not be supportable on Navy ships such as the CH-46s it was replacing. However, Marines have deployed more than three squadrons on ships in the last 2 years, including a Marine air element on the USS *Kearsarge* that used its V-22s to rescue an F-15 pilot who ejected over Libya in March 2011. Another claim that falls into the "half-truth" category is that V-22s cannot autorotate (the method helicopters use to land when all engines fail[5]). It is true, but irrelevant, that the V-22 cannot autorotate. The whole truth is that the V-22 has a larger flight envelope where it can survive a dual-engine failure than the flight envelope of any comparable aircraft. If both engines fail while it is flying fast (called "airplane mode"), the V-22 can glide like any fixed-wing aircraft, obviating the need for autorotation. So the only risk is when both engines fail while the V-22 is in "helicopter mode" (with the prop-rotors/engines pointed upward). V-22s spend the vast majority of their time operating in airplane mode and use helicopter mode only when taking off and landing. Every aircraft ever made has some combination of low speeds and altitudes that should be avoided because a loss of engine power will not allow a safe landing. Even helicopters have speed-altitude combinations that do not allow a successful autorotation landing. Because of its power and speed, the V-22 spends less time in these "avoid" regions than helicopters, making the V-22 less likely to experience a crash from a dual-engine failure—meaning safer operations for crew and passengers.

the V-22 went from near extinction to becoming one of the safest aircraft in the Marine vertical-lift inventory

V-22s started with a questionable safety record as the manufacturers and military testers learned about the new, unique tiltrotor machine. But since the redesign of the aircraft, the 1990s record of crashes has been replaced by 10 years of exceptional safety and a continued focus on making the aircraft safer. Despite the poor reputation earned by those early years, the V-22 community developed and maintained an openness to accepting scrutiny even when the worst happened.

U.S. Air Force (Andy M. Kin)

Navy SEALs hoisted onto Air Force Special Operations CV-22 Osprey at Hurlburt Field

Affordable Transportation

Recent congressional inquiries have focused on the cost of the V-22.[6] This is not surprising given the current financial climate. When V-22 costs are evaluated against what the military would need as an alternative, it proves an effective and efficient aircraft for DOD and the Nation. To make a fair comparison, the V-22 must be examined using initial purchase costs for a comparable fleet of replacements, but also including operating and maintenance costs as well as personnel costs needed to support operations—what the military calls *life-cycle cost*.

Each new Marine MV-22 costs approximately $74 million. The Air Force's CV-22 variant costs more—approximately $84 million each—because it has added avionics such as a terrain-following radar and advanced defensive systems to protect it against radar and infrared missiles. This seems high compared to the $16 million price tag for each Army basic H-60M. But a more advanced H-60, with defensive equipment and networked global communications for tomorrow's combat operations, costs much more. And when a basic H-60 is modified for a combat role, the price grows dramatically. Egypt bought four such H-60s in 2008 for $44 million each,[7] and the Air Force's combat replacement program is buying 10 H-60s that are expected to cost $40 million each after modifications to make them combat effective.[8] That is almost half as much as a single V-22, but an H-60 can hold only 7 to 10 troops while a V-22 can hold 24; in combat, V-22s have carried as many as 35 troops when the seats were removed and the troops were secured using tie-downs on the floor. A Marine squadron on a ship would need more than two-and-a-half times as many H-60s to carry the same number of troops as a single V-22. A V-22 can also fly twice as fast, which means it can go twice as far in the same time. A squadron equipped with H-60s would need more than twice as many aircraft to go half as far. To extend the range of the H-60, the military would need air refueling support (such as C-130s) or additional ground refueling assets (tanker trucks/personnel and security). When factoring in these additional costs for the same warfighting capabilities, the V-22 life-cycle cost is cheaper than an H-60 or other comparable options. This comparison is why the military stuck with the V-22 even when it had its early problems.

The civilian transport world uses different measures of efficiency than the military does. The government focuses on the overall cost, while the for-profit world focuses on the comparative advantage of the available options. The airline industry measures the efficiency of an aircraft using a formula that takes into account the cost to fly a specified mission, the number of passengers it can carry, and the distance flown—cost per available seat-mile. Employing a similar formula using the maximum range of different aircraft, it is possible to compare the cost-efficiency of the different options.

The Marine Corps did this analysis and found that while the V-22 costs more to fly per hour than other options, it is more efficient because it can carry more passengers a greater distance. The CH-46 costs $4,600 per hour to operate, but carries half as many passengers as the V-22 and travels slower and not as far. The CH-46 costs $3.17 per passenger-mile. The CH-53E, the Marines' heavy-lift helicopter, can carry extremely heavy loads on its cargo hooks (sling-loaded below the aircraft) but carries the same number of passengers as the V-22 (like the V-22, the CH-53E can carry more troops when loaded without seats, but this analysis uses troops-in-seats for comparison since this is the officially approved measure). The CH-53E costs the same to operate hourly as the V-22 but travels slower and therefore not as far, so it costs $3.12 per passenger-mile. The Navy's newest H-60 version—the MH-60S—costs much less per hour (just over $2,500), but it can carry only seven passengers and also has a shorter range. The MH-60S costs $2.84 per passenger-mile. The V-22 costs almost $11,500 per hour and can carry 24 passengers at speeds over 250 knots—nearly twice that of fully-loaded helicopters. The V-22 costs $1.75 per passenger-mile.

These cost numbers do not include the V-22 program office's recent cost-reduction initiatives, which garnered DOD's 2011 David Packard Excellence in Acquisition Award for exemplary innovations and best practices in the defense acquisition process by decreasing the cost per flying hour over 15 percent.[9] In 2010, the Osprey flight-hour cost was reduced to $10,400 per hour and as low as $9,400 per hour for the first half of 2011. Using the 2011 rate, the Osprey cost-per-hour drops to $1.43—half of the H-46 and H-60 rates. And these rates do not include the costs of additional support assets that alternative solutions would require, such as additional air refueling, fuel trucks, personnel, and so forth. The H-53s can carry heavier external loads, so the Osprey cannot assume the Marines heavy-lift role for moving artillery, vehicles, or other large equipment. But in the passenger-moving role, the V-22 is far cheaper than the alternatives currently in the military inventory. If the military only needs to move small numbers of troops short distances, the H-60 is more efficient. But the Marines, Army, and special operations forces routinely need to move larger forces and prefer to base as far from the enemy as possible.

Recent criticisms have focused on the cost of the V-22 but have failed to account for

the expense of its rivals. The cost of each V-22 is higher than alternative aircraft, but this ignores the fact that DOD needs fewer V-22s to accomplish the same mission. The V-22 is cheaper than other options using both a life-cycle cost and a cost-per-available-seat-mile analysis. It is quantifiably safer and cheaper than alternative vertical-lift options, and it also provides the desired qualitative advantages for today's and tomorrow's military needs.

U.S. Air Force (Markus Maier)

Air Force CV-22 Ospreys take off from Kirtland Air Force Base

Future Operations

Combat operations are complete in Iraq and should be winding down in Afghanistan in the next year or two. Already the United States is focusing on other areas of the world both for counterterrorism and for the potential of larger operations against more developed threats. As America transitions to these tasks, the V-22 becomes an even greater asset. With its ability to operate from Navy ships, it improves the country's ability to defend shipping lanes, conduct small counterterrorism missions, and participate in larger operations against larger forces where greater connectivity and defensive capabilities are needed.

In 2008, Colonel Glenn Walter, USMC, wrote that the V-22 would enhance military operations by exploring all nine principles of war.[10] His analysis stands today and is reinforced by the last 4 years of V-22 combat operations. The Air Force Osprey variant can avoid detection to surprise an enemy with advanced detection systems such as integrated defense networks found in China, Iran, and North Korea. Since V-22s can be based farther away from their targets than alternative systems, troops will be safer from enemy attack—that is, ships launching V-22s can remain farther away from antiship missile launchers. The improved defensive systems of the CV-22 also provide greater security by protecting the troops from ground and air threats as they transit to and from targets. We have learned that access to bases is increasingly difficult and frequently requires political and military sacrifices to secure the basing rights necessary to conduct certain operations. As we face a future of more counterterrorist missions such as the one that killed bin Laden, the United States may not have readily available bases next door such as Afghanistan provided. Should the United States lack that advantage for future high-priority missions in areas such as the Pacific Rim or Africa, the V-22 becomes invaluable. The political advantage of decreased reliance on sometimes questionable allies is incalculable.

DOD is looking at aircraft for a number of missions that have traditionally been seen as needing helicopters. Each Service is looking for replacements to existing aircraft because current options have reached the end of their service-life or need greater capabilities. The V-22 offers a highly competitive option for each of these demands, but many within DOD have shied away from considering it because of misperceptions shaped by the colored history of the aircraft. With the safety and cost advantages easy to see, the V-22 should move to the front of the line for all the Services in some key areas.

The Air Force has been looking for a combat search and rescue (CSAR) replacement to its HH-60. The Service has a small fleet of highly modified H-60s with aerial refueling probes, internal fuel tanks, advanced navigation systems, improved defensive systems, rescue hoists, and long-range communication capabilities. As already described, the V-22 is superior to the H-60 in all these areas. And since the Air Force has already paid for the development and test costs of these upgrades on the V-22, it could start buying combat-ready aircraft rapidly (although that is not an easy prospect in the current fiscal environment). The increased speed of the V-22 also improves the CSAR force's chance of arriving within the *golden hour*—that first hour when the opportunity to save a life is greatest. A CSAR V-22 has more cabin room than an H-60 so a medical team could perform lifesaving actions with more medical equipment while the aircrew moves the patient directly from the battlefield to the trauma center faster and without the need for a transfer to a longer-range aircraft. The V-22 is tailor-made for this lifesaving combat mission.

The Navy is looking for a replacement for its small fixed-wing aircraft carrier resupply aircraft, the C-2. The V-22 can do this mission as well. Although not a complete replacement for the C-2, the V-22 can add new mission areas that the C-2 cannot do, such as resupplying noncarriers ships (with helicopter pads) and long-range overwater rescue. Despite having only a handful of aircraft, the C-2 achieved a logistics advantage because it shared many common parts with the Navy's early warning and command aircraft, the E-2. This meant that the C-2 shared space for people and parts aboard an aircraft carrier and achieved some economies of scale with logistics and training. Because the Marine Corps and Air Force are already using V-22s, these economies of scale will exist if V-22s take over this mission area, too. V-22s have established worldwide logistics chains ashore and afloat. The Marines operate a jointly manned training center in North Carolina training Marine and Air Force aircrew and maintainers. The loss of commonality with the E-2 will be balanced by commonality with a larger fleet of Marine and Air Force V-22s.

The Army is beginning to focus on developing a new, faster helicopter.[11] According to Major General Anthony Crutchfield, director of the U.S. Army Aviation Center of

Excellence, the Army wants an aircraft that "flies faster, longer, carries more payload, requires a smaller logistical footprint and is more survivable."[12] The current development has focused on an aircraft much like the cancelled RAH-66 Comanche, a helicopter-type aircraft with a small rear-facing propeller that pushes the aircraft to faster speeds than current helicopters. One prototype is already flying, but it has no troop-carrying capability. And while this development offers new opportunities and capabilities, it is not slated to be ready until 2030, leaving the Army with a 20-year capability gap. In the interim, the Army could use the V-22 to expand the mission set of faster vertical-lift aircraft by integrating more weapons and electronic systems to meet its needs while it continues to develop its next-generation helicopter. For example, the Army could immediately begin using V-22s for its medical evacuation mission. In a role that is similar to the Air Force's CSAR mission, the advantages are compelling. Once introduced to the aviation inventory, the Army could then expand the V-22 role into other areas planned for future developmental aircraft. This would allow the Army to conduct risk-reduction development and evaluation of Army-unique equipment, which will decrease the time to integrate them on new aircraft. This will mitigate the problems experienced with the Littoral Combat Ship (where the Navy has experienced delays fielding the ship, which has further delayed the planned subsystems). Since a next-generation helicopter requires years of development and testing before beginning to develop the advanced avionics, using V-22s now can accelerate some of those capabilities while decreasing the follow-on integration time for the next aircraft.

The V-22 offers the military many options for many different missions. When it was first developed, some saw it as the future of all aviation, both military and commercial. That utopian vision has not come to pass, but the V-22 does offer some concrete advantages right now for each of the Services' pressing aviation needs. In these fiscally challenged times, the V-22 offers safe capabilities at reasonable costs without having to wait years for new development.

Conclusion

The V-22 has a troubled past that includes crashes, development problems, and high costs. But the improvements incorporated into the modern V-22 have resulted in an unparalleled and enviable safety record for a combat aircraft. The V-22 community has continued to strive for safer airplanes and has demonstrated a level of openness that is refreshing and indicates confidence in its usefulness. After years of criticism for being expensive, the V-22 is showing that it is cheaper to buy and operate than other vertical lift aircraft for the long-range troop-carrying role. It rapidly became a high-demand asset in Iraq and Afghanistan. However, the V-22's advantages go far beyond our current conflicts. It can succeed in missions around the world from discrete counterterrorist raids to small-scale conflicts to major fights against technologically advanced nations. It offers benefits to all of these missions with enhancements to the military principles of mass, maneuver, surprise, security, and simplicity. As DOD and Congress look to manage a burgeoning budget while maintaining the world's best military force, the V-22 should rise to the top of the list of systems needed for today and tomorrow.

with the safety and cost advantages easy to see, the V-22 should move to the front of the line for all the Services

Tilt-rotor aircraft are not ready to transform aviation, as some have claimed. But this first-generation V-22 is ready for more missions while helping to keep the military budget from bankrupting the country. It proves itself every day for the Marines and special operations troops who have come to rely on it and are developing new ways to integrate it into their daily missions. It can be adapted and produced for even more military uses without the need for the lengthy development and testing of basic aircraft that delay all new programs and cost billions of dollars. All new types of aircraft have experienced development problems as the builders and users tried to learn how to fly and use them. Early fixed-wing aircraft took years to develop into useful machines, as did jets, spacecraft, and helicopters. The V-22, with its radical tilt-rotor concept, was no exception. More lessons can be learned, but with over 100,000 flight hours (half of those in the last 2 years), the V-22 has become safer, cheaper, and more capable than other options for America's troop-carrying role. **JFQ**

NOTES

[1] Marcus Weisberger, "Where Will Budget Ax Fall?" *Defense News*, January 16, 2012; Jennifer Rubin, "Obama Needs a Defense Budget to Match His Vision," *The Washington Post*, March 29, 2011; John Feffer, "One Creature That Deserves Extinction: The V-22 Osprey," *Foreign Policy in Focus*, February 25, 2011, available at <www.fpif.org/blog/one_creature_that_deserves_extinction_the_v-22_osprey>; William Hartung, "Libya Makes the Case for Lower Military Spending," *HuffingtonPost.com*, March 22, 2011, available at <www.huffingtonpost.com/william-hartung/libya-makes-case-for-lowe_b_839168.html>.

[2] "Assessment of Impacts of Budget Cuts," letter from House Armed Service Committee Republican Staff to Chairman Howard "Buck" McKeon, September 22, 2011.

[3] Richard Whittle, *The Dream Machine: The Untold History of the Notorious V-22 Osprey* (New York: Simon and Schuster, 2010).

[4] Bruce Rolfson, "USAF Generals Clash over CV-22 Crash," *Defense News*, January 10, 2011.

[5] Mark Thompson, "V-22 Osprey: A Flying Shame," *Time*, September 26, 2007.

[6] Jeremiah Gertler, *V-22 Osprey Tilt-Rotor Aircraft: Background and Issues for Congress*, RL31384 (Washington, DC: Congressional Research Service, March 10, 2011); Michael J. Sullivan, *V-22 Osprey Aircraft: Assessment Needed to Address Operational and Cost Concerns to Define Future Investment*, GAO-09-692T (Washington, DC: Government Accountability Office, June 23, 2009).

[7] "Egypt—UH-60M Black Hawk Helicopters," *Aerospace and Defense News*, available at <www.asdnews.com/news/17587/Egypt_-_UH-60M_BLACK_HAWK_Helicopters .htm>.

[8] Marcus Weisberger, "USAF Nears OK for $40M Rescue Helos," *Defense News*, September 26, 2011.

[9] 2011 Defense Acquisition Workforce Awards, available at <www.dau.mil/pubscats/ATL%20Docs/Jan_Feb_2012/2011%20DAW-awards.pdf>.

[10] Glenn Walters, "MV-22B Osprey: A Strategic Leap Forward," *Joint Force Quarterly* 49 (2nd Quarter 2008), 16–19.

[11] Michael Hoffman, "US Army Outlines Next Vert-Lift Aircraft," *Defense News*, April 25, 2011.

[12] Ibid.

U.S. Navy (Tommy Lamkin)

Crewman directs BF-04, a Marine Corps F-35B Lightning II, after vertical landing on USS *Wasp*, as second F-35 approaches

THE F-35 AND THE Future of Power Projection

By ROBBIN F. LAIRD *and* EDWARD T. TIMPERLAKE

Dr. Robbin F. Laird is a Military and Security Analyst, the co-founder of Second Line of Defense, and a Member of the Editorial Board of Contributors, AOL Defense. The Honorable Edward T. Timperlake is the Editor of Second Line of Defense Forum and former Director of Technology Assessment, International Technology Security, Office of the Secretary of Defense.

The F-35 is called a joint strike fighter (JSF), and its ability to work with, leverage, and enhance the capability of power projection forces is at the heart of the next 20 years of rebuilding U.S. and allied forces. The "geriatric condition" of U.S. forces and the past 10 years of ground combat in faraway areas make it clear that a fundamental reconstruction is required. Yet much of the discussion inside the Beltway treats the F-35 as if it were simply a tactical aircraft replacement for the Air Force, Navy, and Marine Corps fleets. It is really a "flying combat system" rather than a tactical aircraft, which allows the United States and its allies to look at power projection in a very different way.[1] It also allows the United States and its allies to get the best value out of their forces.

The F-35 will replace multiple aircraft in the fleet, and by so doing, it will create significant economies of scale and savings. The aircraft is 80 percent common across the fleet, and savings come from software commonality, new approaches to digital maintenance, and flight-line enhancements and improvements. Possibly the F-35's most important capability is its ability to combine information with Aegis systems and other command and control systems operated by allies worldwide. This sharing capability will not only enhance combat capability but also dramatically change the way the United States can work with its allies. This article discusses several aspects of the change, which is disruptive in nature. If the culture of thinking about combat does not change, and we think of this as the next iteration of what the Services will have for combat aircraft, the entire revolution will be missed.

Anticipating the "Re-Norming" Revolution

The F-22 has been deployed for several years, and its evolution is having a significant impact on rethinking air operations. The decade or more of deployment prior to the F-35 will provide a significant impact on the F-35 and its concept of operations.[2] The primary task of the F-22 is air-to-air dominance followed by core competence in counterair defense missions. It also provides a key gap-filler capability between the now retired F-117 and the exceptional capabilities of the F-35 against increasingly lethal mobile air defense systems. For example, SA-10s and SA-20s can be dismantled, moved, and ready for action in a short time. The trend line is toward rapid mobility in the adversary's air defenses, and mobility in this domain means that the incoming strike aircraft must be able to execute target identification, target acquisition, and strike missions virtually simultaneously. A key aspect of the new fifth-generation aircraft is its onboard machine processing capability, which allows the pilot to perform operations simultaneously that historically required several platforms operating sequentially. But the limited number of F-22s ensures that the F-35 will be the dominant fifth-generation aircraft both in terms of numbers and in its availability in a coalition environment. From the standpoint of thinking through 21st-century air operations, the ability of the F-22 and F-35 to work together and to lead a strike force will be central to U.S. core capabilities for projecting power and will be a crucial role of the 21st-century Air Force.

fourth-generation aircraft join the fray as areas of the battlefield are cleared of the most lethal threat systems

For the Air Force, the largest stakeholder in the F-35, the challenge and opportunity is to blend the F-22s with the F-35s in creating a "re-normed" concept of air operations. For example, the F-22 and F-35 will work together in supporting air dominance—to "kick in the door" to open the enemy's battlespace—for the insertion of a joint power projection force. Here the F-22 largely provides the initial strike and guides the initial air dominance operations; the F-35 supports the effort with stealth and sensor capabilities able to operate in a distributed network, providing strike; intelligence, surveillance, and reconnaissance (ISR); and capabilities to suppress enemy air defenses as well as attack shore defenses against maritime projection forces. Fourth-generation aircraft join the fray as areas of the battlefield are cleared of the most lethal threat systems, expediting participation and increasing survivability by linking into the fifth-generation networked situational awareness. An excellent insight into the role of the F-22 in anticipating the F-35 was provided by a Marine Corps F-22 pilot. Lieutenant Colonel Dave Berke is becoming a key F-35 squadron commander, but he provided an interview while at Nellis Air Force Base (AFB) regarding his experience with the F-22 and how he saw the plane as part of the ongoing revolution in re-norming air operations.

In response to a question about what the fused sensor experience is all about in fifth-generation aircraft and how the whole capability of an aircraft is not really an F series but a flying combat system, Berke provided the following explanation:

I think you're hitting the nail on the head with what the JSF is going to do, but it's also what the Raptor missions have already morphed into. The concept of Raptor employment covers two basic concepts. You've got an antiaccess/global strike mission; and you have the integration mission as well. And the bottom line is that the integration mission is our bread and butter. When I say "us," I'm talking about the Air Force and the F-22. Most of our expected operating environments are going to be integrated.[3]

As a pilot with significant operational experience across the legacy fleet, Berke provided insight into how the fifth-generation solution was different:

It's a major evolution. There's no question about it. My career has been in F-18s, but I also flew F-16s for 3 years. I was dual operational in the Hornet and the Viper when I was a TOPGUN instructor. I am now coming up on 3 years flying Raptors. I was also on carriers for 4 years, so I've done a lot of integration with the Navy and a lot of integration with the Air Force. Three years flying with the Air Force has been pretty broadening.

For me, it's a great experience to see the similarities and difference between the Services. Navy and Marine aviation is very similar. USAF aviation is very different in some ways. I actually was with the Army for a year as FAC [forward air controller] *in Iraq as well. So from a tactical level, I've got a lot of tactical operator experience with all three Services—Navy, Army, and the Air Force. This has been really illuminating for me having the experience with all of the Services in tactical operations. Obviously I will draw upon that experience when I fully engage with the JSF. But flying a Raptor, the left, right, up, down, is just flying; flying is flying. So getting in an airplane and flying around really is not that cosmic no matter what type of airplane you're sitting in.*

But the difference between a Hornet or a Viper and the Raptor isn't just the way you turn or which way you move the jet or what is the best way to attack a particular problem. The difference is how you think. You work totally differently to garner situational awareness [SA] *and make decisions; it's all different in the F-22. With the F-22 and certainly it will be the case with the F-35, you're operating at a level where you perform several functions of classic air battle management and that's a whole different experience and a different kind of training. . . .*

In the Raptor, the data is already fused into information thereby providing the situational awareness. SA is extremely high in the F-22 and obviously will be in the JSF; and it's very easy for the pilot to process the SA. Indeed, the processing of data is the key to having high SA and the key to making smart decisions. There's virtually no data in the F-22 that you have to process; it's almost all information.[4]

Air Force pilots have underscored some of the changes articulated by Berke and have reinforced the need for culture change to get a different air combat and overall combat capability into the Nation's 21st-century force structure. An interview with three senior Air Force pilots at Langley AFB in late 2010 underscored the significance of the change. The pilots—Lieutenant Colonel Damon Anthony, Major James Akers, and Lieutenant Colonel Steve Pieper—provided an understanding of how classic combat operations built around the use of Airborne Warning and Control Systems and the Combined Air Operation Center (CAOC) will be modified as new aircraft reshape operational capabilities. As Lieutenant Colonel Pieper put it:

I think the most difficult and the most painful set of shifts will be organizational. They will relate to the people who are now forced to relinquish operational strategic decisions to folks like us in the room, which has always been the case.

So tactical decisions have always had operational strategic and national impact. The difference is that organizationally, we'll be forced to reconcile that notion, and understand that the individual who's charged with those tactical decisions will now have the kind of information that was previously only available nearly fused but far more imperfectly fused in the CAOC. That information will now be distributed in the battlespace.

So that speaks to an entirely different not just physical architecture, also personnel architecture, but more importantly leadership paradigm and approach to solving a problem. You now are far more able to remove fat layers of intermediate data processing and you're able to sic a force of very capable assets on an objective.

We're able dynamically to adapt in the middle of that process and make appropriate decisions in support of your objective far more effectively than if you had just sent planes out on a specific task.[5]

In other words, the F-22 has paved the way for the F-35, and integrating the F-22 with the F-35 will be a core contribution of the Air Force in shaping innovative combat capabilities for the United States and its allies in the decade ahead. Both planes are shapers of an entirely new approach to combat capabilities across the joint and coalition force.

The F-35 Is More Than Stealth, More Than a Weapons System

The F-35 joint strike fighter is often defined by its stealth characteristics, and the debate revolves around whether one needs "a high-end aircraft" or, if one is pessimistic, whether "stealth is really stealthy." Although interesting, such discussions miss the point. Stealth is an enabler for this aircraft, not its central definition. As a Marine F-18 pilot put it:

I would say low observability is a capability set or is an asset to the platform, but the platform as a whole brings a lot by itself. There are situations where low observability will be very important to the mission set that you're operating in. And then there will be situations where the ISR package or the imaging package that comes with that aircraft, the ability to see things, will be more important; that will change based on the mission set and how you define the mission.[6]

Moreover, one of the challenges facing the F-35 is that it is often described using historical aviation words, generally obscuring the technological advance of stealth itself. As Lieutenant General David Deptula, USAF (Ret.), constantly reminded his Service and others, the "F" before the F-22 and the F-35 is somewhat of a misnomer. There are significant generational changes in the way individual combat aircraft and fleets of aircraft handle data and can make decisions.[7]

Stealth on this aircraft is a function of the manufacturing process; it is not hand built into the aircraft and maintained as such. It is a *characteristic* of high-tolerance manufacturing, and as such, stealth will be maintained in the field, not in the factory or depot. This is revolutionary in character.

At the heart of the F-35 is a new comprehensive combat systems enterprise.[8] The F-35 is the first combat aircraft that sees completely around itself. The Electro Optical Distributed Aperture System (DAS) makes this happen, and it allows the operator or the fleet managers to see hundreds of miles away on a 360-degree basis. The combat system enterprise allows the aircraft to manage the battlespace within this seamless 360-degree space. Unlike legacy aircraft, which add systems that have to be managed by the pilot, the F-35 creates a synergy workspace where the core combat systems work interactively to create functional outcomes; for example, jamming can be performed by the overall systems, not just by a dedicated electronic warfare system.

integrating the F-22 with the F-35 will be a core contribution of the Air Force in shaping innovative combat capabilities for the United States and its allies

The F-35 is a flying combat system integrator and in a different historical epoch than the F-15s, F-18s, and F-16s. The 360-degree capability, coupled with the combat system enterprise, explains these historic differences on a per plane basis. The ability of the new aircraft to shape distributed air operations collectively is another historic change that the United States and its allies need to make, especially with the growing missile, air defense, and offensive air capabilities in the global market space and battlespace. The legacy combat aircraft have added new combat subsystems over a 30-year period. These evolved aircraft and their new subsystems are additive, iterative, and sequential. The resulting configurations are built over the core foundational

Courtesy (Paul Weatherman)

F-35A Lightning II over Rogers Dry Lakebed, Edwards Air Force Base

aircraft. All of the legacy U.S. aircraft with the latest modifications, when offered for foreign sale, were rejected in India's fighter competition for the much newer European fighters, the Eurofighter and Rafale.

The F-35 was built with a foundation that allows interactivity across the combat systems, permitting the forging of a combat system enterprise managed by the computer on the aircraft. Said another way, F-35 core combat systems are interactive with one another, creating a synergistic outcome and capability rather than providing an additive-segmented tool. The aircraft's systems are built on a physical link, namely, a high-speed data bus built on high-speed fiber optical systems. To provide a rough comparison, legacy aircraft are communicating over a dial-up modem compared to the F-35 system, which is equivalent to a high-speed broadband system. The new data bus and high-speed broadband are the facilitators of this fully integrated data-sharing environment on the aircraft. While legacy aircraft have had similar subsystems, integration was far less mature.

Connected to the other combat systems via the high-speed data bus is the CNI system (communications, navigation, and identification). This is a flexible radio frequency system that enables the aircraft to operate against a variety of threats. The other core combat systems, which interact to create the combat systems enterprise, are the Active Electronically Scanned Array (AESA) radar, DAS, Electrical Optical Targeting System (EOTS), and electronic warfare (EW) system. As Pete Bartos, a former Strike Eagle Pilot now with Northrop Grumman, put it:

When this plane was designed, the avionics suite from the ground up, the designers looked at the different elements that can be mutually supporting as one of the integration tenets. For example, the radar didn't have to do everything; the Electrical Optical Targeting System didn't have to do everything. And they were designed together.

Fusion is the way to leverage the other sensors' strengths. To make up for any weaknesses, perhaps in the field of regard or a certain mode, a certain spectrum, with each of the sensor building blocks, they were all designed to be multifunction avionics.

For example, the AESA is an MFA—a multifunction array. It has, of course, the standard air-to-air modes, the standard air-to-ground modes. But in addition, it's really built from the ground up to be an EW aperture for electronic protection, electronic support, which is sensing, passive ops, and electronic attack.[9]

A way to look at the cross-functionality of the combat systems is to think past the narrow focus of additive systems. A system is added to do a task. The pilot needs to use that system to manage the task. With the F-35 interactive systems, the pilot will perform a function without caring which system is actually executing the mission. For example, for electronic warfare, including cyber, he could be using the EOTS, EW system, or AESA radar. The pilot really does not care, and the interactivity among the systems creates a future evolution whereby synergy among the systems creates new options and possibilities. Furthermore, the system rests on an upgradable computer with chip replacement, allowing generational leaps in computational power.

The F-35 provides a flexible architecture similar to a smart phone. With the F-35, we define a synergy space to draw on the menu of applications. And the F-35 combat systems are built to permit open-ended growing capability. In mathematical analogies, we are describing something that can create battlespace

"fractals," notably with a joint force able to execute distributed operations. The aircraft is a facilitator of a more robust combat environment than was available with legacy aircraft and command and control. This change requires pilots to rethink how to operate. F-35 performance and its pilot allow a revolution along the information axis of combat, or what might be identified as the "z-axis."

Operating on the Z-axis: Shaping a New Pilot Culture

The design characteristics blended together prior to the F-35 have been constantly improving range, payload (improved by system and weapons carried), maneuverability (measured by "P Sub s"), useful speed, and range (modified by VSTOL [vertical short takeoff and landing]—a plus factor). The F-35 is also designed with inherent survivability factors; first, redundancy and hardening, and then stealth. Stealth is usually seen as the fifth-generation improvement. Nevertheless, reducing the F-35 to a linear x-y axis improvement or to stealth misses the point. The F-35 is taking technology into a revolutionary three-dimensional situational awareness capability. This capability establishes a new vector for TacAir (tactical air) aircraft design. This can be measured on a z-axis.

Traditionally, the two dimensional depiction is that the x-axis is time and the y-axis is performance and captures individual airplanes that tend to cluster in generation improvement. Each aircraft clustered in a "generation" is a combination of improvements. Essentially, the aeronautical design "art" of blending together ever improving and evolving technology eventually creates improvements in a linear fashion. The F-35 is not a linear performance enhancement over legacy or fourth-generation fighter aircraft. When we consider information and the speed at which it can be collected, fused, presented, and acted on in the combat environment, those who possess this advanced decision capability will have a clear advantage.

While this is not a new concept, having been originally conceived in John Boyd's famous OODA (observe, orient, decide, and act) loop, the information dimension of combat aircraft design now is so important that it forces us to gauge the value of such a weapons system along the z-axis, which is the pilot's cockpit OODA loop axis. This OODA loop ability is measured as the combined capability the pilot gains from integrated command, control, communications, computers, ISR, and his resultant decisionmaking (C^4ISR-D) and employment or action. From Boyd's theory, we know that victory in the air or, for that matter, anywhere in combat is dependent on the speed and accuracy of the combatant in making a decision. The better support the pilot in a combat aircraft receives from his information systems, the better the combat engagement outcome. The advantage goes to the better information enabled. Pilots have always known this, but the revolutionary fifth generation, designed in C^4ISR-D, requires a similar advancement in how pilots approach their work.

In addition, today's industrial learning curve to improve sensors, system capability, and weapons carried is likely flatter than that required to build another airframe, and it may be a new American way of industrial surging.[10] The U.S. arsenal of democracy may be shifting from an industrial production line to a clean room and a computer lab as key shapers of competitive advantage. This progress can be best seen in movement out the z-axis. The Air Force F-22 pilot community has been experiencing this revolution for some time, and their lessons learned are being incorporated into a pilot's F-35 training. Learning from those experiences as well as those of the legacy fleet, the Marine Corps recognizes that a new pilot culture will emerge because of operating on the z-axis. General Jon Davis, 2nd Marine Aircraft Wing commander, underscored that three pilot cultures are being rolled into a very new one. The commander linked this to generational change:

The F-35B is going to provide the USMC aviator cultures in our Harriers, Hornets and Prowlers to coalesce and I think to shape an innovative new launch point for the USMC aviation community. We are going to blend three outstanding communities. Each community has a slightly different approach to problem-solving. You've got the expeditionary basing that the Harrier guys are bringing to you. You have the electronic warfare side of the equation and the high-end fight that the Prowler guys think about and the [communications] *and jamming side of the equation, which the Prowler guys think about. And you have the multi-role approach of the F-18 guys.*[11]

What General Davis discussed concerning the new pilot culture is shaped in large part by bringing EW into the cockpit. The Marine Aviation Weapons and Tactics Squadron 1 (MAWTS-1) is currently working to shape that new pilot culture. MAWTS-1 pilots and trainers are looking at the impact of the V-22 and F-35 on the changes in tactics and training generated by the new aircraft. MAWTS-1 is taking a much older curriculum and adjusting it to the realities of the impact of the V-22 and the anticipated impact of the F-35.

MAWTS-1 is highly interactive with the various centers of excellence such as Nellis AFB, Eglin AFB, and the Navy/Marine test community at Pax River, as well as the United Kingdom, in shaping F-35 transition. In fact, the advantage of having a common fleet will be to provide for significant advances in cross-Service training and evolutions in concepts of operations. Additionally, the fact that MAWTS-1 is studying the way the Air Force trains combat pilots to fly the F-16 in shaping the Marine F-35B Training and Readiness Manual is a testimony to a joint-Service approach. This is extremely important in how MAWTS-1 addresses the future. An emerging approach may well be to take functions and then to redesign the curriculum around those functions. For example, the inherent capabilities of the emerging F-35 C^4ISR-D cockpit with 360-degree SA may turn out with appropriately designed data links to be a force multiplier in the tactical employment of the MV-22 Osprey and the helicopter community, and reach back to Navy combat forces afloat.[12]

the better support the pilot in a combat aircraft receives from his information systems, the better the combat engagement outcome

Northern Edge 2011

The F-35 can be understood as a combat aircraft that can operate and manage combat space within a 360-degree radius for more than 800 miles. A recent operational test of the F-35 radar and the DAS occurred in Northern Edge 2011, a joint and combined exercise that serves as a focal point for the restructuring of U.S. power projection forces.

As the results from the exercise are evaluated, military leadership and program managers should be able to make a definitive judgment on the way ahead for the program *now*, not in some distant future. In both Northern Edge 2009 and 2011, the air combat baseline was being re-normed and the limitations of legacy aircraft were well highlighted when compared to newer systems. Northern Edge validated, in real time, the ability of American and soon allied TacAir fleets to give total concurrent SA to each combat pilot. In a robust jamming operating environment, the F-35 radar and DAS separated themselves from the pack and have initiated a new era in thinking about combat operations.

As an F-35 joint program office release underscores, this is not only about the ability of airpower to operate in a robust EW environment in which cyber conflict is a key dimension, but it is also about the ability of an airborne capability to support maritime operations:

This year provided an opportunity to observe the performance of the F-35 JSF systems in multiple robust electronic warfare scenarios. The AN/APG-81 active electronically scanned array radar and AN/AAQ-37 distributed aperture system were mounted aboard Northrop Grumman's BAC 1-11 test aircraft. Making its debut, the AN/AAQ-37 DAS demonstrated spherical situational awareness and target tracking capabilities. The DAS is designed to simultaneously track multiple aircraft in every direction, which has never been seen in an air combat environment.

A return participant, the AN/APG-81 AESA, demonstrated robust electronic protection, electronic attack, passive maritime and experimental modes, and data-linked air and surface tracks to improve legacy fighter situational awareness. It also searched the entire 50,000 square-mile Gulf of Alaska operating area for surface vessels, and accurately detected and tracked them in minimal time.[13]

The C[4]ISR-D capability in each cockpit takes the F-35 out of the linear fifth-generation development path. The F-35 radar was validated in a tactically relevant environment. Until proven otherwise, America still has the most capable EW and, to use an older phrase, ECCM (electronic counter-countermeasures) fighting force in the world. So being tactically "validated" in an American-designed exercise is the gold standard. Northern Edge exercises provide operational—not test—environments. Block 2 is ready for Marine F-35B initial operational capability. In 2009, Block 2 was the first improvement up the z-axis, and pilots from MAWTS (the Marine equivalent of TOPGUN) are paying close attention. Block 3—the next step up the z-axis—demonstrated that the radar worked effectively in sea surface search and ship target track. If American TacAir forces afloat can see an enemy, they will kill that enemy. Block 4 is the next step up for "Three Dimensional Warriors" and a z-axis cockpit. A fighter pilot knowledgeable about Northern Edge, when asked about DAS, stated that it had a feature of "passive ranging." When asked what that meant, he casually remarked, "Shooting people off your tail and all that stuff."[14]

the use of the Osprey underscored the game-changing possibilities of the ARG in littoral operations

Operating Differently: A Peek into the Future

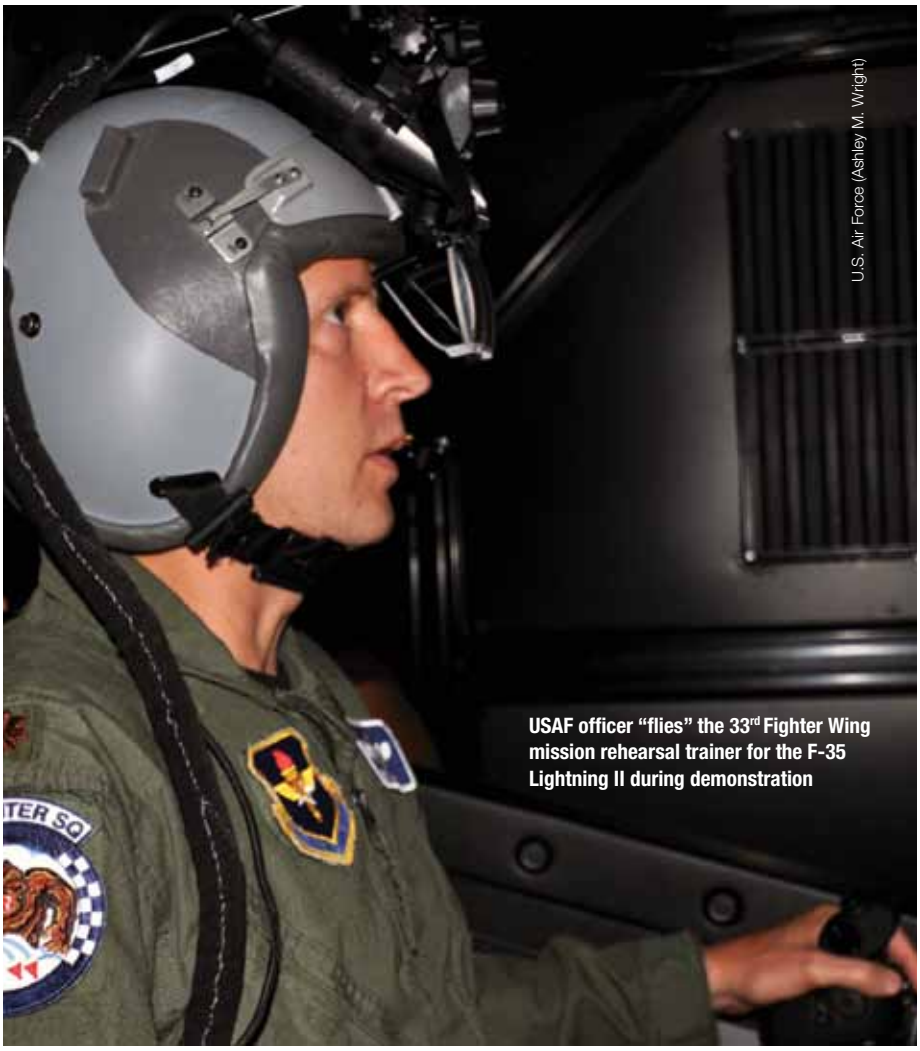
Rediscovered operationally during recent maneuvers off the shores of Libya is what the Amphibious Ready Group (ARG)—what we prefer to call the "agile response group"—can do with transformational aircraft. The aircraft in this case was the Osprey, but the Osprey paired with the F-35B will make the Gator Navy not just a troop carrier but a capital ship. It is harder to find a greater value proposition than adding the F-35B to the fleet and turning amphibious "tigers" into air combat "lions." The ARG is experiencing fundamental change, with new ships and new planes providing new capabilities, and these new capabilities are congruent with recent Libyan operational experiences. Given the Marines' battle hymn, it seems that "the shores of Tripoli" can have a whole new meaning for the evolution of the U.S. force structure.

The ARG was used in several unprecedented ways in the Libyan operation. First, the V-22 Osprey was a key element of changing how U.S. forces operated. The Osprey provided a logistical linchpin that allowed the ARG to stay on station and the Harriers to create greater sortie generation rates and quicker operations tempo. The use of the Osprey in the operation underscored the game-changing possibilities of the ARG in littoral operations in the future. The key point is that the sea base, which in effect is represented by the ARG, can provide a very flexible strike package. Given their proximity to shore, the Harriers could operate with significant sortie rates against enemy forces. Not only could they come and go rapidly, but the information they obtained with their LITENING pods could be delivered to their ship and be processed and used to inform the next strike package. Commanders did not need a long command and control or C[4]ISR chain to inform combat. This meant that Muammar Qadhafi's ground forces would not have moved far from the last positions Harriers noted before the new Harriers moved into attack positions.[15]

This combination of compressed C[4]ISR and sortie rates created a deadly combination for enemy forces and underscored that using sea bases in a compressed strike package had clear advantages over land-based aircraft still several hours from the fight and dependent on C[4]ISR coming from hundreds or even thousands of miles away. One more point about the ARG's operations is that the Osprey and Harrier worked together closely to enhance combat capabilities. One aspect of this was the ability of the Ospreys to bring parts and support elements to the Harriers. Instead of waiting for ships to bring parts, or for much slower legacy rotorcraft to fly them out, the Osprey, traveling at 300 miles per hour, could bring parts from land bases to keep up with the Harrier's operations tempo.[16]

The highly visible pilot rescue mission certainly underscored how a vertically launched aircraft working with the Osprey off of the ARG can create new capabilities. The elapsed time of authorization to the recovery of a pilot and his return to the USS *Kearsarge* was 43 minutes. This rescue took place even though the Air Force had a rescue helicopter aboard USS *Ponce*. It was not used for two reasons: It would have gotten to the pilot much later than an Osprey team, and the command and control would have been much slower than what the Marines could deliver.[17]

The key to the Marines' command and control was that the pilots of the Ospreys and Harriers planned the operation together in



USAF officer "flies" the 33rd Fighter Wing mission rehearsal trainer for the F-35 Lightning II during demonstration

the ready room of USS *Kearsarge*. They did not meet in virtual space. They exchanged information in real time and were in the same room. They could look at the briefing materials together. The Harriers were informed by fresh intelligence aboard the *Kearsarge*. The sea base brought together the assets and intelligence to execute the mission. The Marines used their land base largely to supply the sea-based air operations via Ospreys. Second, having the C4ISR forward-deployed with the pilot as the key decisionmaker is crucial to mission success.

The Navy–Marine Corps team has a number of new capabilities being deployed or acquired that will enhance its ability to perform such operations. The F-35B will give the Marines an integrated electronic warfare and C4ISR capability. The new landing platform docks have significant command and control capabilities. The new Littoral Combat Ship could provide—along with the Osprey—significant combat insertion capability for ground forces along with rapid withdrawal capability.

Honeycombing the Pacific: Crafting Scalable Forces

A new Pacific strategy can be built in part around the cultural revolution that the new F-35 engenders in interconnecting capabilities through the C4ISR-D enablement strategy. No platform fights alone, and shaping a honeycomb approach where force structure is shaped appropriately to the local problem but can reach back to provide capabilities beyond a particular area of interest within the honeycomb is key. The strategy is founded on having platform presence. By deploying such assets as those of the U.S. Coast Guard (for example, the National Security Cutter—or Navy surface platforms such as Aegis, LCS, or other surface assets) and by deploying sub-Service assets and having bases forward-deployed, the Nation has core assets that, if networked together, are capable of making significant gains possible. Scalability is the crucial glue to making a honeycomb force possible. That is why a Navy, Marine Corps, and Air Force common fleet is the crucial glue. And when "Aegis becomes my wingman" or "the SSGN [guided missile submarines] becomes the ARG fire support" through the F-35 C4ISR-D systems, a combat and cultural revolution is both possible and necessary. Basing becomes transformed as allied and U.S. capabilities become blended into a scalable presence and engagement capability. Presence is rooted in basing; scalability is inherently doable because of C4ISR enablement, deployed decisionmaking, and honeycomb robustness.

The reach from Japan to South Korea to Singapore to Australia is about how allies are reshaping their forces and working toward greater reach and capabilities. For example, by shaping a defense strategy, which is not simply a modern variant of *Sitzkreig* in South Korea and Japan, more mobile assets such as the F-35 allow states in the region to reach out, back, and up to craft coalition capabilities. In the case of South Korea, instead of strengthening relatively static ground capabilities, shaping a mobile engagement force allows for better South Korean defense as well as better regional capabilities to deal with myriad challenges likely to unfold in the decades ahead.

The introduction of F-35As into the Air Force and Republic of Korea (ROK) wings deployed to South Korea can set innovations in motion that can help U.S. and ROK forces redesign and improve defense capability within the Korean Peninsula while allowing ROK capabilities to play a greater role within the region. South Korea could be an ideal area to shape a new concept-of-operations approach. North Korea has a large but linear force. By basing F-35As in South Korea, a nonlinear combat system is inserted. And the United States can bring F-22s from Guam. It would then have multiple vectors to confuse enemies about its military planning and disrupt any kind of attempted linear attack.

Introducing the F-35As into South Korea will generate a whole new approach to linking C4ISR into a more effective deployable force. As former Secretary of the Air Force Michael Wynne emphasized:

The gains are really if you have a distributed shooter set, it's chaos to start with because the

North Koreans have a very linear plan. In the artillery exchange, it was a very linear plan. In the points of crossings on the borders, it's a very linear plan. The placement of their artillery pieces in the mountains depicts a very linear thinking on their part. And what they can't stand and I don't think they have the citizenry support to actually stand [is] *a nonlinear solution set. So it will cause us to essentially rethink our whole game plan because it has to involve the surrounding terrain, the surrounding military where frankly we have to show the Chinese that we're not planning on invading them and we will stop at the North Korean border. Korea is after all the last vestige of Yalta.*[18]

Lockheed Martin

F-35C Joint Strike Fighter test launches from steam catapult for carrier suitability at NAS Patuxent River

The recent decision by Japan to buy the F-35A is a significant move forward in shaping a new Pacific approach and capability. The Japanese understand the opportunity to leverage the F-35 combat systems enterprise, and that is a key reason why the Japanese down-selected the aircraft. The Japanese—a key Aegis partner—also understand the significant opportunity provided by integrating the Aegis with the F-35. Combining the Aegis with the F-35 means joining their sensors for wide-area coverage. Because of a new generation of weapons on the F-35 and the ability to operate a broad wolf pack of air and sea capabilities, the JSF can perform as the directing point for combat action. With the Aegis and its new SM-3 missiles, the F-35 can leverage a sea-based missile to expand its strike area. Together, the F-35 and Aegis significantly expand the defense of land and sea bases.

The commonality across the combat systems of the F-35's three variants provides a notable advantage. Aegis is a pilot's wingman whether he is flying an F-35A, B, or C. Eighty percent of the F-35s in the Pacific are likely to be F-35As, many of them coalition aircraft. Therefore, building an F-35 and Aegis global enterprise provides coverage and capability across the Pacific, which is essential for the defense of Japan.

Moreover, the commonality of the fleet allows hubs to be built in the region supporting common operations, shaping convergent capabilities. The distributed character of allied forces in the region as well as the connectivity which the F-35 allows as an interdependent flying combat system diversifies capabilities with which a core adversary would have to cope. Reducing concentration of forces and targets is a significant enhancer of deterrence.

During President Barack Obama's recent visit to Darwin, Australia, the opportunity provided by commonality across the F-35 fleet was highlighted by the possibility of building a hub in Darwin for sustainment of an allied fleet as well as ISR sharing for common decisionmaking. Darwin's strategic location could become a hub of Pacific operations for Australia and a place to visit for its core allies. Singapore, South Korea, Japan, and the United States could all become key members of an Australia-based and Australian-run F-35 hub.

Australia rightly wishes to preserve its independence in being a partner in flying the F-35. The Royal Australian Air Force (RAAF) is joining a fleet of aircraft—F-35 As, Bs, and Cs—that can be deployed to Australia for training, from bases in Singapore, South Korea, and Japan, and off U.S. ships and U.S. Air Force air bases in the Pacific. The entire allied team can draw upon Australian air modernization to shape new capabilities for Australia and diversify support for the F-35 multinational fleet. The RAAF can go from being on its forward deployed airfield to becoming a hub for the F-35 fleet in several ways.

First, given the significant commonality among the three types of F-35s, a logistics and support hub can be based in the Northern Territories. The differences among naval air and air force air are significantly blurred by the commonality of the F-35s. This means that specific support for the As, Bs, and Cs could be generated. Based on the earnings from a logistics hub, Australia will be able to pay for a significant part of its own fleet modernization. And a hub is not a permanent base. As an on-call service facility, it enables allies to draw on its support when they work with Australia on regional security missions.

Second, Australia has the large territory necessary for Asian F-35 fleets to train. The F-35 is not a replacement tactical aircraft; it is new flying combat system that will need significant training territory for pilots to learn how to use all of its capabilities. As an aircraft that has EW built in, training to do cyber and EW ops is important. As a fifth-generation aircraft, its ability to engage "aggressors" and to "defeat" air defense assets requires enough space to operate as well. Instrumented training ranges over Australia and the contiguous ocean are invaluable for building the necessary skills to deter any aggressor. As an added benefit, Australia will gain substantial revenue from allies when its training facilities are used. With the logistics facilities and the training facilities, the F-35 could gain significant cash for Australia's military modernization efforts.

Third, the F-35 is a significant ISR asset. The Aussies can build ISR collection facilities that can leverage the entire allied fleet of F-35s operating in a regional security setting. They can use such facilities to shape an approach to link other allied ISR assets to establish a honeycomb network or grid along the Pacific Rim.

If each element of the deployed honeycomb can reach out, up, and back for weapons, which can be directed by the z-axis of the F-35, a significant jump in capability, survivability, flexibility, and lethality can be achieved. A scalable structure allows for an economy of force. Presence and engagement in various local cells of the honeycomb may well be able to deal with whatever the problem in that vector might be. Moreover,

remembering that in the era of Black Swans, one is not certain where the next "crisis" or "engagement" might be. By being part of a honeycomb, the U.S. or allied force can be part of a greater whole.

Singapore, South Korea, Japan, and the United States could all become key members of an Australia-based and Australian-run F-35 hub

This means that the goal is *not* to deploy more than we need to perform to the task. Vulnerability is reduced, risk management is enhanced, and the logistics and sustainment cost of an operation is significantly reduced. We do not have to deploy a Carrier Battle Group or multiple air wings when an ARG is enough. By leveraging the new platforms, which are C[4]ISR enabled and linked by the F-35 across the Navy, Marine Corps, Air Force, and allied fleets, a new Pacific strategy can be built. This strategy meets the needs of *this* century and the centrality of allied capabilities, unlike the last decade when the United States dealt largely with asymmetric adversaries with limited power projection tools.

The Way Ahead

By building on the F-35 and leveraging its capabilities, the United States and its allies can build the next phase of power projection within affordable limits. U.S. forces need to become more agile, flexible, and global in order to work with allies and partners to deal with evolving global realities. Protecting access points (the global conveyer of goods and services), ensuring an ability to work with global partners in having access to commodities, shaping insertion forces that can pursue terrorist elements wherever necessary, and partnering with global players all require a reinforced maritime and air capability. This is thus a priority for all Services in the reconfiguring effort. Balanced force structure reduction makes no sense because the force structure was redesigned for land wars that the Nation will not take on in the decade ahead. The U.S. Army can be recast by the overall effort to shape new power projection capabilities and competencies.

Retiring older Service systems, which are logistical money hogs and high maintenance, can shape affordability. Core new systems can be leveraged to shape a pull rather than a push transition strategy. Fortunately, the country is already building these new systems and is in a position to shape an effective transition to a more affordable power projection capability. At the heart of the approach is to move from the platform-centric focus, where the cost of a new product is considered the debate point, to the inherent value of new systems and their ability to be conjoined. "No platform fights alone" is the mantra, and core recognition of how the new platforms work with one another to shape the collaborative concept of operations and capabilities is central to a strategic redesign of U.S. forces. **JFQ**

NOTES

[1] Robbin F. Laird, "Embrace the Airpower Revolution," *Defense News*, February 21, 2011, 61; and Robbin F. Laird, "Recovering the Strategic Context for JSF," *Defense News*, September 4, 2006, 21.

[2] Robbin F. Laird, *A 21st-Century Concept of Air and Military Operations*, Defense Horizons 66 (Washington, DC: NDU Press, March 2009).

[3] "Fifth Generation Aircraft: A View from the Cockpit: An Interview with Dave Berke," in *"Re-Norming" Air Operations* (Arlington, VA: Second Line of Defense [SLD], 2010), 42.

[4] Ibid., 42–43.

[5] "Culture Change in Shaping a New Con-ops: An Interview with Damon Anthony et al.," in *"Re-Norming" Air Operations*, 48–49.

[6] "Shaping an Economy of Force," in *The F-35 Maintenance Revolution* (Arlington, VA: SLD, 2010), 14.

[7] "A New Paradigm for Manned and Unmanned Systems," in *"Re-Norming" Air Operations*, 79–82.

[8] See Robbin F. Laird et al., "Enabling Three Dimensional Warriors," in *Three Dimensional Warriors* (Arlington, VA: SLD, 2009), 36–49; and Robbin F. Laird, "A Key Foundational Element for 'Re-Norming': The F-35 Combat System Enterprise," in *"Re-Norming" Air Operations*, 60–62.

[9] "Shaping the F-35 Combat System Enterprise," *SLD.com*, March 22, 2011, available at <www.sldinfo.com/shaping-the-f-35-combat-system-enterprise/>.

[10] Edward T. Timperlake, "The United States vs. USSR: TacAir Lessons Learned from a 'Hot' Cold War," in *"Re-Norming" Air Operations*, 8–17; and Edward T. Timperlake, "The F-35B in the Perspective of Aviation History," in *Three Dimensional Warriors*, 2–3.

[11] "'The Future Is Now': Clearing the Decks for the 'iPad-Generation Pilots': An Interview with Jon M. Davis," in *The F-35 Maintenance Revolution*, 11.

[12] For a look at the thinking of Marines at Marine Aviation Weapons and Tactics Squadron 1 (MAWTS-1) on the new opportunities inherent in the aircraft and new concepts of operations, see "Preparing for the F-35B Transition: MAWTS Re-Shapes its Curriculum," *SLD.com*, October 20, 2011, available at <www.sldinfo.com/preparing-for-the-f-35b-transition-mawts-re-shapes-its-curriculum/>.

[13] Tracey Saiki, "Continued Testing of F-35 JSF Sensors a Success at Northern Edge 2011," F-35 Lightning II Press Release, June 27, 2011.

[14] Edward T. Timperlake, "The Northern Edge Difference: Re-Structuring the Strategic Debate," *SLD.com*, August 31, 2011, available at <www.sldinfo.com/the-northern-edge-difference-re-structuring-the-strategic-debate/>.

[15] "The Role of the Osprey in Operation *Odyssey Dawn*," *SLD.com*, September 22, 2011, available at <www.sldinfo.com/the-role-of-the-osprey-in-operation-odyssey-dawn/>.

[16] "The Amphibious Ready Group (ARG) and Libya: Shrinking 'The Average Commute': An Interview With Colonel Mark Desens, Commander of the 26th MEU," *SLD.com*, September 5, 2011, available at <www.sldinfo.com/the-amphibious-ready-group-arg-and-libya/>.

[17] "The Execution of the TRAP Mission over Libya: An Interview with Major Debardeleben," *SLD.com*, September 27, 2011, available at <www.sldinfo.com/the-execution-of-the-trap-mission-over-libya/>.

[18] Michael W. Wynne, "F-35As to Korea: Shaping a Defense Transition," *SLD.com*, November 22, 2011, available at <www.sldinfo.com/f-35as-to-korea-shaping-a-defense-transition-to-deal-with-real-threats/>.

Keep From All Thoughtful Men:
How U.S. Economists Won World War II
By James G. Lacey
Naval Institute Press, 2011
280 pp. $34.95
ISBN: 978-1-59114-491-5

Reviewed by
DAVID A. ANDERSON

James Lacey, a scholar of strategy and national security studies, writes a fascinating book detailing the evolution of the munitions plan (victory program) in support of the U.S. war effort to defeat the Axis powers during World War II. The author asserts that the magnitude of this undertaking, necessitating extensive industrial mobilization of the U.S. economy, made World War II the "economist's war." Lacey supports his thesis by chronologically covering the major events and activities that led to the plan's acceptance and execution.

The author first dispels the widely held belief that Major Albert Wedemeyer, USA (later, Lieutenant General), was the originator of the victory program. Lacey carefully discredits historians, and Wedemeyer himself, through credible scholarly forensics. He does note that Wedemeyer proposed a plan, as he claimed; however, it was not the one embraced by his superiors, let alone the Franklin D. Roosevelt administration. In fact, Lacey shows the plan to be outright wrong anyway.

Lacey subsequently describes the trials and tribulations of military and civilian leaders as they organized and prepared the Nation for war—progressing from a humble ad hoc working group into the powerful War Production Board (WPB). He includes in this discussion the complex dialogue that took place among these eventual planning power brokers (for example, Kuznets, Hopkins, Nelson, Knox, Knudsen, Nathan, and General Somervell), which was complicated by the number of their diverging personalities and agendas, all working toward a common endstate but often visualizing different ways and means to achieve it. Interwoven throughout are the philosophical debates that took place, such as those addressing funding, sourcing, and mobilization requirements, and how much of the U.S. economy would have to be directly committed to support the war effort. Also included are the conversations addressing assistance requirements in support of Great Britain's and the Soviet Union's war efforts.

The industry-by-industry assessment of U.S. production capacity, led by statistician Stacy May, and the mobilization analysis, led by Simon Kuznets, was instrumental to the fruitfulness of these discussions. They came to several notable conclusions. They determined that the military had underestimated its budgetary needs by some 50 percent. The country would run out of production capacity long before it ran out of money to finance munitions production. America needed to shift large segments of the labor force from one geographical location to another to meet military output objectives. President Roosevelt's "must have" munitions were in direct conflict with the Nation's production capacity. Diverting/creating added production capacity to meet the President's requirement would adversely affect overall force capabilities and delay any possible landing on European soil to defeat Germany. The country could commit up to half of its economic capacity in support of the war effort without adversely affecting the short- and/or long-term well-being of the economy. This would be necessary to avert a protracted war. (The author further dispels the notion that the American public had to make great sacrifices in support of the war.) Finally, the United States would be incapable of sustaining a European landing force able to defeat Germany before May 1944. History proved them astonishingly accurate.

What is most amazing is that the analysts determined the most plausible landing date 3 days before the United States entered the war. In the end, Lacey professes that it was economists supporting the WPB, led by economic mastermind Simon Kuznets, supported by statistical work led by Stacy May, who ultimately determined the victory program and when the Normandy landing would take place.

The work involved in gaining industry's collective and collaborative support for the war effort is another of the many interesting insights provided. Memories of being forced to expand production capacity in support of World War I, only to have to subsequently and significantly scale back at great expense after the war, made industry very apprehensive and fearful of a similar fate.

A unique feature of the book is its appendices, which contain all the historical documents that support the author's argument. These documents include Wedemeyer's victory program, Kuznets first feasibility study, and General Somervell's written comments regarding the recommendations in the feasibility study. The book's short title derives from one of the many derogatory comments made by Somervell toward Kuznets's feasibility study results. The reader will find these documents valuable throughout his reading of the book.

Lacey has meticulously researched an inherently complex topic and crafted it in a concise and engaging way. This book is a must-read for 20th-century military historians, strategists, national security studies academics, and students. Also valuable is the author's chapter in *The Shaping of Grand Strategy* (Cambridge University Press, 2011), which he coedited. It directly complements this noteworthy body of work. **JFQ**

Lieutenant Colonel David A. Anderson, USMC (Ret.), DBA, is a Professor of Strategic Studies and the Odom Chair of Joint, Interagency, and Multinational Operations at the U.S. Army Command and General Staff College.

The Shaping of Grand Strategy: Policy, Diplomacy, and War
Edited by Williamson Murray, Richard Hart Sinnreich, and James Lacey
Cambridge University Press, 2011
283 pp. $27.99
ISBN: 978-0-521-15633-2

Reviewed by
FRANCIS P. SEMPA

Great powers pursue national objectives and promote and protect national security interests by means of grand strategy. This sounds obvious and simple enough, but as Carl von Clausewitz wrote of war, in selecting and implementing grand strategies, even the most simple things are difficult. That is the common thread that links the nine insightful essays collected by Williamson Murray, Richard Hart Sinnreich, and James Lacey in *The Shaping of Grand Strategy: Policy, Diplomacy, and War.*

As Williamson Murray notes in the opening essay, there is no neat, precise definition of grand strategy. "The closer one comes to understanding what it entails, the more one sees how complex and uncertain in historical terms are the aspects that encompass its making and use" (p. 5). Grand strategy is affected by a nation's geographical position, historical context, the nature of its government, and the character and capabilities of its leaders, and it encompasses political, social, economic, and military realities. "No theoretical construct, no set of abstract principles, no political science model," Murray writes, "can capture its essence" (p. 11).

The essence of grand strategy can only be understood by historical examples, which is why seven of the nine essays are case studies of successes and failures of grand strategies at different periods of history. "It is the understanding of the ambiguities and uncertainties that political and military leaders have confronted in the past and will confront in the future," writes Murray, "that is the basis of any successful grand strategy" (p. 33).

The contributors to *The Shaping of Grand Strategy* examine Louis XIV's France; Britain during the Seven Years' War; Otto von Bismarck's Prussia and Germany; Britain in the late 19th and early 20th centuries; Britain in the 1930s and the early years of World War II; the United States in World War II; and the United States in the early Cold War years. As Richard Hart Sinnreich points out in his concluding essay, these case studies reveal no "patterns" of grand strategy—no precise theories to explain why some strategies succeed and others fail. There are simply too many variables and too much plain luck involved. Sinnreich quotes Bismarck on this subject: "Man cannot create the current of events. He can only float with it and steer" (p. 254).

Louis XIV succeeded in making France the predominant power in Europe in the late 17th and early 18th centuries, explains John A. Lynn II, but his quest for absolute security and his unilateral foreign policies produced concerted opposition among other European powers and nearly bankrupted France. Louis's grand strategy embroiled his country in wars for 51 of the 72 years he occupied the throne. France increased its continental possessions, but at far too high a cost.

Louis's grand strategy stands in stark contrast to that of Otto von Bismarck, who skillfully steered the Prussian/German ship of state during the mid to late 19th century. "No statesman ever adjusted war to policy with a nicer judgment than Bismarck," wrote Halford Mackinder. As Marcus Jones notes in his essay, Bismarck waged three short and successful wars, attained Prussian predominance through a united German Empire in the center of Europe, and then formed alliances with other great powers that maintained general peace. Bismarck, unlike Louis, did not seek absolute security nor act unilaterally on the international stage. Instead, after 1871, Bismarck "was at pains to demonstrate that Germany was a satiated state, without ambitions or intentions against her neighbors or territories abroad" (p. 105). Jones attributes Bismarck's success as a strategist to his "nuanced grasp" of political realities, his "Machiavellian flexibility" in pursuing Prussia's interests, and his moderation and prudence in conducting both war and diplomacy (p. 83).

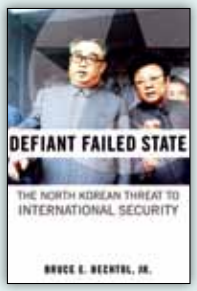
Essays by Jeremy Black, Sinnreich, and Murray about British grand strategies during the Seven Years' War, the decades preceding World War I, and the prewar and early World War II years demonstrate the dynamic nature of "strategic culture," the impact of domestic politics on strategy, and the importance of individual leadership to the success or failure of grand strategy.

Britain's strategic focus shifted to imperial issues as a result of the Seven Years' War and the struggle with France for control of North America. Its grand strategy in the years immediately before World War I changed from the "splendid isolation" of an offshore balancer to a strategic commitment to continental allies in the face of a growing German geopolitical threat. Later, the horrors of World War I produced British leaders in the 1930s who sought to avoid war at almost any cost. When appeasement of Hitler failed, Britain turned to Winston Churchill, whose grasp of history and understanding of the nature of Adolf Hitler's totalitarian challenge helped him formulate and implement a grand strategy—husbanding British resources, seeking aid from and an alliance with the United States, and allying with Joseph Stalin's Russia—that saved Britain and defeated the German threat, but alas, could not save the British Empire.

The final case studies, by James Lacey and Colin Gray, examine how Franklin D. Roosevelt and his military chiefs devised a successful grand strategy for global war by prioritizing the defeat of Germany, invading North Africa, Sicily, then Italy, delaying the invasion of France until 1944, conducting a two-pronged war against Japan in the Pacific, and insisting on the unconditional surrender of the Axis powers while, after the war, Harry S. Truman and his talented advisors repeatedly made the right decisions to contain the Soviet geopolitical threat by "the purposeful building, in succession, of the economic . . . political, and . . . military tiers of Western Security between 1945 and 1953" (pp. 233–234).

When all is said and done, these case studies show that a successful grand strategy depends on the wisdom and character of military and political leaders and their understanding of history as a useful but imperfect guide to navigate the ship of state. **JFQ**

Francis P. Sempa is the author of *Somewhere in France, Somewhere in Germany: A Combat Soldier's Journey Through the Second World War; Geopolitics: From the Cold War to the 21st Century;* and *America's Global Role: Essays and Reviews on National Security, Geopolitics, and War.* He 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.*



Defiant Failed State: The North Korean Threat to International Security

By Bruce E. Bechtol, Jr.

Potomac Books, Inc., 2010
288 pp. $29.95
ISBN: 978-1-59797-531-5

Reviewed by
ROBERT DANIEL WALLACE

Bruce Bechtol, a retired military officer and former Defense Intelligence Agency analyst, is a well-known security studies academic and an associate professor at Angelo State University's Center for Security Studies. His previous works deal almost exclusively with the security dilemma that North Korea poses to the United States, its allies, and the international community. This book is a continuation of Bechtol's efforts to describe and explain the seemingly unpredictable nature of the Kim regime, North Korea's military capabilities, and the future of the Korean Peninsula. This is Bechtol's response to those who would discount North Korea as a threat to the United States and its allies.

Bechtol's goal in this book is to "discuss the main threats that North Korea presents to the national security of the United States and its allies" (p. ix). He notes that after the Cold War, North Korea became a "multi-faceted" threat through its arms supply industry, nuclear capabilities, and uncertainty surrounding leadership succession (p. 2). Moreover, Bechtol supports continued "hard line" foreign policy efforts (containment and deterrence) when dealing with Kim Jong-Il and the North Korean government.

The preface states that Bechtol's intention is not to "produce an analysis that is overly focused on political science or international relations jargon, or a work that is built on theory" (p. x). Thus, the text has the tone of both a historical narrative and a current intelligence report on North Korea's actions and capabilities. The main portion of the book explores familiar territory for those who study North Korea. This includes discussions of military capabilities, weapons proliferation, the Six-Party Talks on North Korea's nuclear program, issues surrounding Kim Jong-Il's successor, and the Republic of Korea (ROK)-U.S. military alliance. Bechtol concludes with a treatment of North Korean capabilities viewed through a U.S. Department of Defense lens (using the "diplomatic, informational, military, and economic" construct) and recommendations for both a firm U.S. foreign policy and a strong U.S.-ROK alliance to counter North Korea's threat. These areas are important for any analysis of North Korea and its foreign policy activities, which often have repercussions not only for East Asia, but for the entire world. While three of the main chapters are expanded or rewritten articles that have been previously published by Bechtol, their inclusion within a single text allows readers to gain a more comprehensive view of the Democratic People's Republic of Korea (DPRK) within a single volume.

Although Bechtol intentionally limits his text to a discussion of the threats posed by the Kim regime, this narrow scope is the most significant weakness of the book. This text contains a detailed and scrupulously notated study of recent DPRK threat activity (down to the grid coordinates of long-range missile danger areas on p. 33), but lacks a much-needed wider scope of analysis. For example, although he does briefly discuss the ascension of Kim Jong-Il to power (pp. 101–102), the inclusion of a more detailed comparison between the first transition between "the Kims" (Kim Il-Sung to Kim Jong-Il) and current efforts by the North Korean regime to establish Kim Jong-Un (Kim Jong-Il's son) could help to clarify events surrounding succession. In describing North Korea's military threat, Bechtol correctly notes that its asymmetric threat is credible, but omits mentioning how the current threat compares to the DPRK's long history of unconventional activities. Additionally, North Korea's actions have significant repercussions within the region, and the inclusion of an international relations perspective would help bolster Bechtol's arguments. Finally, comparisons to other Communist regimes (past or present) might allow for a better understanding of DPRK activities.

North Korea continues to exist as a recalcitrant and isolated Cold War country, and remains, at its very core, a sovereign nation focused on state survival. Surrounded by perceived threats (from Japan, South Korea, and the United States), North Korea continues to look to China for support while attempting to ensure that it can survive (at any cost) without outside assistance. North Korea's threatening foreign policy activity might be similar to other state-level patterns observed throughout history. Examination and comparison of North Korean activity to Japan's efforts at autarky prior to World War II, Cuba's long history of Communist rule and isolation, or China's modernist approach to communism and economic expansion all might help readers to understand the choices made by the Kim regime. Contrasting North Korea with other "rogue" nations could help support Bechtol's arguments that the North Korean threat remains both unique and dangerous to U.S. interests.

There are a number of other minor areas in which the book might have been improved. The text assumes readers have an understanding of regional U.S. interests and military contingencies in the region—a phrase such as "designated ROK forces chop to the CFC commander" (p. 169) might be confusing to some readers. Additionally, a number of Bechtol's graphics fared poorly in the publishing process, although this might have been out of his control. Finally, although Bechtol provides a detailed discussion of successors to Kim Jong-Il and presents two figures that describe the Kim family (p. 105) and its "Power Circle" (p. 118), the argument is difficult to follow and could be clarified with the inclusion of another figure showing the hierarchy of other key (nonfamily) individuals.

Bechtol makes a credible argument that North Korea remains a threat, but readers would benefit from a more complete discussion of the historical, regional, and theoretical issues that surround the Kim regime. Nevertheless, Bechtol has done an admirable job of describing actions taken by North Korea that pose a security risk for East Asia, providing noteworthy information for policy analysts. The hardest part in writing about North Korea is how to research and analyze its closed society and political system in a credible manner. Bechtol's book clearly demonstrates that examining the complicated nature of the DPRK's leaders and government remains a difficult task for any scholar. **JFQ**

Lieutenant Colonel Robert Daniel Wallace, USA, is a faculty member at the U.S. Army Command and General Staff College and a Ph.D. student in Kansas State University's Security Studies Program.

The United Nations and Intergovernmental Organization Command Relationships: Part III of III

By GEORGE E. KATSOS

Previously in *Joint Force Quarterly*, we provided command relationship overviews as they occur in both U.S. and multinational doctrine.[1] In this last installment, we take a broad look at command relationships as they exist under normal conditions within intergovernmental organizations such as the United Nations (UN). Commanders must use caution not to exchange U.S. with UN or any other organization's terminology.

The United Nations

Founded in 1945, the UN is an international organization of countries committed to maintaining peace and security around the world.[2] Its charter is the foundational document that provides the UN Security Council (UNSC) with responsibilities such as establishing peacekeeping operations (PKOs).[3] Currently with 193 member states and no standing army, the UN approaches member states for military force contributions. Member states that contribute forces to PKOs are called troop contributing countries (TCCs).[4] Even though TCC forces operate under a UN command[5] with blue berets or helmets with UN insignia, TCCs always retain full command[6] of their national forces and may withdraw them at any time.[7]

Established by a UNSC resolution (UNSCR) with the agreement between warring parties, a UN PKO contains binding mandates with tasks such as supporting a cease-fire, peace agreement, or protection of civilians.[8] Within the spectrum of UN PKOs, five activities are carried out by UN forces: peacekeeping (create conditions for peace, consent needed); peace enforcement (practices ensuring peace, consent not needed); peacemaking (establish equal power relationships among actors); peace-building (civilian infrastructure); and conflict prevention (action taken in advance of a crisis). Although the terms *peacekeeping* and *peace enforcement* do not appear in the UN Charter, their legal basis is found in chapters VI ("Pacific Settlement of Disputes") and VII ("Action with Respect to Threats to the Peace, Breaches of Peace and Acts of Aggression").[9]

Within the UN mission structure, three levels of command and control exist. At the strategic level, the UNSC provides overall political direction. At the operational level, the UN Secretary-General provides executive direction assisted by the Department of Peacekeeping Operations (DPKO). At the tactical level where the military component resides and appointed by the Secretary-General via submissions by member states to DPKO is the highest ranking military individual on the UN force, the UN Force Commander (UNFC) or head of military component. The UNFC reports to the special representative of the Secretary-General, also known as the chief of mission, and exercises UN operational control (UN OPCON)[10] over all military personnel including military observers. Commanders of different contingents report to the UNFC on all operational matters and must not be given or accept instructions from their own national authorities that are contrary to the mission's mandate.[11] To reflect participation of TCCs in UN PKOs, an integrated command structure is normally adopted. Even though collaboration between TCC personnel is a strength in UN PKOs, common concerns are the capability of headquarters staff and its integration with a firm understanding of TCC military capabilities.

U.S. Support and Doctrine

The current U.S. position regarding command over American forces engaged in a multinational contingency operation is rooted in Article II of the U.S. Constitution, Title 10 of U.S. Code,[12] and further refined by a group of Presidential directives. As Commander in Chief, the President of the United States always retains command authority over U.S. forces. Any large-scale participation of American forces likely to involve combat is ordinarily conducted under U.S. command[13] or through a competent regional organization.[14] Normally, the President will keep units formed in support of a UN mission under a U.S. chain of command; however, he will make the exception of placing units under UN OPCON/UN tactical control of a U.S. officer in a UN deputy commander position. Within the limits of UN OPCON, a foreign commander cannot change the mission or deploy U.S. forces outside the operational area agreed to by the President; separate units or divide their supplies; administer discipline; or promote anyone or change the internal organization of U.S. forces.

In 1950, the UNSC established a UN command to stop Communist aggression in Korea. Through the years, international military presence in the Republic of Korea (ROK) declined from worldwide to bilateral. Eventually, UN member states called for the dissolution of the UN command in Korea and for the establishment of a ROK-U.S. combined command system. As a result, in 1978 remaining ROK-U.S. forces transferred from UN command to the ROK-U.S. Combined Forces Command (CFC).[15] If conflict arises, the CFC commander will act in the defense of the ROK and technically could act as the commander of UN forces in Korea. When conflict occurs, U.S. forces will be either under "combined OPCON" and even possibly UN OPCON. *Combined OPCON* is a more restrictive term than *U.S. OPCON*, strictly referring to the employment of warfighting missions.[16]

Following military operations in Panama and Kuwait/Iraq in 1992, the President authorized National Security Directive (NSD) 74, "Peacekeeping and Emergency Humanitarian Relief Policy," outlining U.S. support for UN peacekeeping. In 1993, Policy

George E. Katsos is a Joint Doctrine Planner in the Joint Chiefs of Staff J7, Joint Education and Doctrine Division. This article is the last of three on command relationships.

Review Document (PRD) 13, "Peacekeeping Operations," was drafted. It aimed to improve UN peacekeeping. However, PRD 13 did not come to fruition due to political pressures resulting from U.S. casualties in the UN operation in Somalia, which was commanded by a Turkish general and a dual-hatted U.S. deputy who was as the commander of U.S. Forces Somalia. Even though thousands of American troops were placed under UN OPCON for this mission,[17] the UNFC in reality had little or no control over these forces since the arrangement of these attached forces was intended for utilization under the U.S. deputy.[18]

While Presidential directives in the 1990s articulated policies on peacekeeping, existing joint doctrine provided limited guidance. The first step toward filling that gap was joint publication (JP) development conducted by the joint doctrine development community led by the Joint Chiefs of Staff J7. The increase of JP development began in 1993 with the creation of JP 3-07.3, *Peace Operations*, and JP 3-07.5 (now JP 3-68), *Noncombatant Evacuation Operations*. In 1994, Presidential Decision Directive (PDD) 25, "U.S. Policy on Reforming Multilateral Peace Operations," established instructions and clarified command relationship terminology for U.S. participation in peace operations. It also focused attention on the need for improved dialogue and decisionmaking among governmental agencies. Less than 24 months after the release of PDD 25, joint publications on stability operations, interorganizational coordination during joint operations, and foreign humanitarian assistance entered U.S. military doctrine.[19] PDD 25 also laid the basis for PDD 56, "Managing Complex Contingency Operations," in 1997, which institutionalized policies and procedures on managing complex crises.[20]

When the UN released the *Report of the Panel on UN Peace Operations* in 2000, it exposed additional shortfalls in the execution of UN PKOs.[21] In 2004, the President's Global Peace Operations Initiative (GPOI) was created to assist in filling those gaps by training peacekeepers and regionally building sustainable indigenous peacekeeping training capacity as primary objectives. Implemented through a close partnership between the U.S. Department of State and Department of Defense (DOD), with State in the lead, GPOI is now another mechanism like troop contribution or financial assistance led by State and other congressional means of the U.S. Government supporting UN and regional peace operations.[22] Under a new development in U.S. policy last year, the President issued Presidential Study Directive 10, "Creation of Interagency Atrocities Prevention Board and Corresponding Interagency Review."[23] This directive identified the prevention of mass atrocities and genocide as a core national security interest of the United States and directed the creation of an atrocities prevention board to coordinate a whole-of-government approach to preventing and responding to mass atrocities and genocide. As a result, military doctrine on the protection of civilians and mass atrocity response operations is being further developed and incorporated into joint doctrine and publications such as JP 3-07.3. In support of this doctrine, GPOI will play a key role in implementing the recommendations of the board when it comes to training peacekeepers who are often the first line of defense in preventing mass atrocities.

Other Organizations and Force Structures

When the UNSC determines that an operation exceeds the capabilities of the United Nations, the Security Council under chapter VIII ("Regional Arrangements") of the charter can authorize a lead nation operation such as the UN-sponsored operations in Korea (U.S. led) and East Timor (Australian led). In January 1991, the *Desert Storm* coalition ejected Iraqi forces from Kuwait under the authority of a UNSCR. Led by an officer now called the U.S. Central Command commander, the United States and its Western allies operated under a parallel command that was separate from the Arab forces commanded by a Saudi commander.

When an operation exceeds UN capabilities and is regional, again under chapter VIII, the United Nations can authorize an organization to lead it. Two such regional organizations are the North Atlantic Treaty Organization (NATO) and African Union (AU). Operating under a UN-sanctioned mission in 2001, NATO took over the UN-mandated International Security Assistance Force in Afghanistan, which provides security in and around the capital. Soon after, the UN Assistance Mission in Afghanistan was established as a peacekeeping mission that focused on recovery and reconstruction. While acting under a UNSCR, few would argue the legality of a NATO military presence; however, when NATO acts under its own mandate as in Yugoslavia in 1999, undoubtedly the question of legality arises.[24] UN forces do require a status of forces agreement with the host nation to be present in the country.

Established in 2002, the AU adopted UN doctrine as a framework for its own doctrine, which informs the development of the African Standby Force (ASF). The ASF is made up of five military brigades from the continent's five economic regional communities and is intended for rapid deployment for a multiplicity of peace operations including the right to intervene in a member state in circumstances of war crimes, genocide, or crimes against humanity.[25] Forces under an AU command[26] are AU OPCON[27] to the regional organization's force commander. Recently, the AU cooperated in military operations with the United Nations by deploying in advance of a UN force in Sudan's Darfur region in 2006, which was later replaced by a UN-led UN-AU hybrid operation in 2007.[28] A concern of the ASF is that AU forces are largely underfunded and poorly equipped. The AU currently leads the peace operation in Somalia.

In addition to formed units, UN missions function with individual UN military observers (MILOBS). UN MILOBS are unarmed and observe, record, and report on the status of formal agreements. If a UN military force is present, MILOBS work in conjunction with the force but under a separate chain of command. Even though the United States has not recently provided formed units under the command of foreign commanders, it has provided individual MILOBS to UN missions. For US MILOBS, the Secretary of the Army is executive agent for DOD support to UN missions, and the responsibility for administrative control is with the U.S. Military Observer Group in Washington.

Conclusion

The U.S. military will continue to operate as a joint force and will likely participate in multinational environments addressing conflict and human suffering around the world. Command relationships at all levels will continue to challenge U.S. forces involved in all types of operations. Recently in Operations *Odyssey Dawn* and *Unified Protector* (Libya), command relationships and employment of air and maritime assets impacted five U.S. combatant commands and four Services as well as the mission's transfer of authority to the multinational community. Commanders must understand the realities of different

levels of command relationships within U.S. chains of command and how American command relationships are impacted when those commanders or forces are assigned or attached to multinational coalition positions or operations. **JFQ**

NOTES

[1] See George E. Katsos, "Command Relationships," *Joint Force Quarterly* 63 (4th Quarter 2011), 153–155, available at <www.ndu.edu/press/lib/images/jfq-63/JFQ-63.pdf>; and "Multinational Command Relationships, Part II of III," *Joint Force Quarterly* 65 (2d Quarter 2011), 102–104, available at <www.ndu.edu/press/lib/pdf/jfq-65/JFQ-65.pdf>.

[2] See "UN at a Glance," *UN.org*, available at <www.un.org/en/aboutun/index.shtml>.

[3] Per other nations and organizations, *peacekeeping operations* are also known as *peace support operations*.

[4] Per the North Atlantic Treaty Organization (NATO) "NATO Glossary of Abbreviations Used in NATO Documents and Publications," AAP-15 (2010), *troop contributing countries* are known as *troop contributing nations*.

[5] *United Nations* [UN] *command* is the authority vested in a military leader for the direction, coordination, and control of military forces; also known as UN operational command. UN command has a legal status and denotes functional and knowledgeable exercise of authority to attain objectives or goals. See UN Department of Peacekeeping Operations (UNPKO), "Authority, Command and Control in United Nations Peacekeeping Operations Policy," Ref. 2008.4 (February 2008); and *Peacekeeping Operations, Principles and Guidelines* (New York: UNPKO, January 2008), 4.

[6] *Full command* is equivalent to U.S. combatant command (command authority), also known as COCOM, for internal matters only and NATO full command; a UN Force Commander (UNFC) will not have full command over another nation's forces. See "Authority, Command and Control in United Nations Peacekeeping Operations Policy," 4.

[7] *Handbook on United Nations Multidimensional Peacekeeping Operations* (New York: UNPKO, December 2003), 67.

[8] UN Security Council Resolution 1674 (2006).

[9] *Peacekeeping Operations, Principles and Guidelines*, 17–18.

[10] *UN operational control* (UN OPCON) is similar to U.S., African Union (AU), and NATO OPCON: the authority granted to a UNFC in a UN peacekeeping operation (PKO) to direct forces assigned so that the commander may accomplish specific missions or tasks that are usually limited by function, time, or location (or a combination); to deploy units concerned and/or military personnel; and to retain or assign tactical command (TACOM) or tactical control (TACON) of those units/personnel. *OPCON* includes the authority to assign separate tasks to subunits of a contingent, in consultation with the contingent commander and as approved by the UN headquarters. Other relevant UN command relationship terms include *UN TACOM* (equivalent to NATO TACOM), which is the authority delegated to a military or police commander in a UN PKO to assign tasks to forces under his command for the accomplishment of the mission assigned by higher authority; *UN TACON* (equivalent to U.S., AU, and NATO TACON), which is the detailed and local direction and control of movement, or maneuver, necessary to accomplish missions or tasks assigned (moreover, as required by operational necessities, the UNFC may delegate the TACON of assigned military forces/police personnel to the subordinate sector and/or unit commanders); and *UN administrative control* (ADCON), which is similar to U.S. and NATO ADCON as well as AU administrative control (ADMCON) and is the authority over subordinate or other organizations within national contingents for administrative matters such as personnel management, supply, services, and other nonoperational missions of the subordinate or other organizations. ADCON is a national responsibility given to the National Contingent Commander in PKOs. Ibid., 4.

[11] *Handbook on United Nations Multidimensional Peacekeeping Operations*, 68.

[12] Michael Canna, *Command and Control of Multinational Operations Involving U.S. Military Forces*, Occasional Paper (Washington, DC: The Atlantic Council, August 2004), 3.

[13] *U.S. OPCON* is the authority to perform those functions of command over subordinate forces involving organizing and employing commands and forces, assigning tasks, designating objectives, and giving authoritative direction necessary to accomplish the mission. See Joint Publication (JP) 1, *Doctrine for the Armed Forces of the United States* (Washington, DC: The Joint Staff, 2012), GL-11. Other U.S. command relationship terms include *U.S. combatant command* (command authority) (COCOM), which is the nontransferable command authority, which cannot be delegated, of a combatant commander to perform those functions of command over assigned forces involving organizing and employing commands and forces; assigning tasks; designating objectives; and giving authoritative direction over all aspects of military operations, joint training, and logistics necessary to accomplish the missions assigned to the command (GL-5). *U.S. TACON* is the authority over forces that is limited to the detailed direction and control of movements or maneuvers within the operational area necessary to accomplish missions or tasks assigned (GL-12). *U.S. ADCON* is the direction or exercise of authority over subordinate or other organizations in respect to administration and support (GL-5).

[14] Canna, 7.

[15] Kyung Young Chung, "An Analysis of ROK-US Military Command Relationship from the Korean War to the Present" (Master's thesis, U.S. Army Command and General Staff College, 1989), 73–91, available at <www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA211800>.

[16] Ibid.

[17] Canna, 12.

[18] Ibid.

[19] Entering into U.S. military doctrine were JP 3-07, *Missions Other Than War* (now known as *Stability Operations*); JP 3-08, which was renamed *Interorganizational Coordination During Joint Operations*; and JP 3-07.6 (now JP 3-29), *Foreign Humanitarian Assistance*.

[20] William P. Hamblet and Jerry G. Kline, "Interagency Cooperation: PDD 56 and Complex Contingency Operations," *Joint Force Quarterly* 24 (Spring 2000), 93.

[21] UN General Assembly and Security Council, *Report on the Panel on United Nations Peace Operations*, A/55/305-S/2000/809, August 21, 2000.

[22] The U.S. assessment level of the overall UN budget is around 27.3 percent, or $2,126,382,000. See Marjorie Ann Browne, *United Nations Peacekeeping: Issues for Congress*, RL33700 (Washington, DC: Congressional Research Service, February 11, 2011).

[23] This interagency effort was led by Special Assistant to President Barack Obama and Senior Director of Multilateral Affairs on the National Security Council Samantha Power, along with assistance from Deputy Assistant Secretary of State of the Bureau of International Organization Affairs Victoria Holt, Deputy Assistant Secretary of Defense/Special Coordinator for Rule of Law and Humanitarian Policy Rosa Brooks, and Deputy Assistant Secretary of Defense for Plans Janine Davidson.

[24] Janka Oertel, "The United Nations and NATO," paper prepared for the Academic Council on the United Nations System 21st Annual Meeting, Bonn, Germany, June 5–7, 2008, 4.

[25] Jakkie Cilliers, *The African Standby Force: An Update on Progress*, Institute for Security Studies (ISS) Paper 160 (Pretoria: ISS, March 2008), 1.

[26] *AU command* is the authority to issues operational directives only within the limits of the regional operational authority. See *African Union Peace Support Operations Standing Operating Procedures* (Addis Ababa: AU, 2008), 1.

[27] *AU OPCON* is the authority granted to military commanders in a peace support operation to direct forces assigned so the commander may accomplish specific missions or tasks that are usually limited by function, time, location, or a combination of these elements. Another relevant command relationship is *AU TACON*, which is the detailed and local direction and control of movement or maneuvers necessary to accomplish missions or tasks; it is delegable to subordinate commanders. Ibid., 3.

[28] Cilliers, 7.

Joint Publications (JP) Under Revision

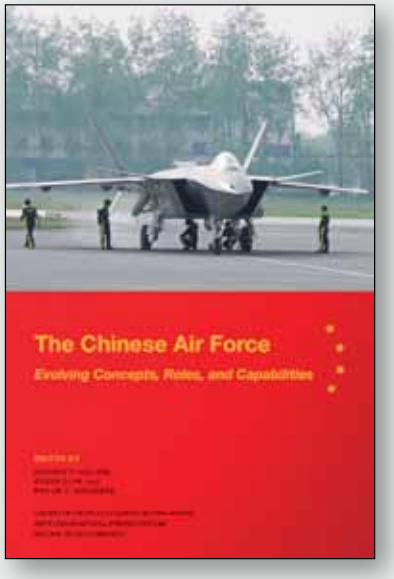
JP 1-05, *Religious Affairs*
JP 2-0, *Joint Intelligence*
JP 2-01.3, *Joint Intelligence Preparation of the Operational Environment*
JP 2-03, *Geospatial Intelligence Support to Joint Operations*
JP 3-00.1, *Strategic Communication and Communications Strategy*
JP 3-02, *Amphibious Operations*
JP 3-04, *Joint Shipboard Helicopter Operations*
JP 3-05, *Special Operations*
JP 3-05.1, *Joint Special Operations Task Force Operations*
JP 3-06, *Joint Urban Operations*
JP 3-07.3, *Peace Operations*
JP 3-07.4, *Counterdrug Operations*
JP 3-09.3, *Close Air Support*
JP 3-11, *Operations in Chemical, Biological, Radiological, and Nuclear Environments*
JP 3-12, *Cyberspace Operations*
JP 3-13, *Information Operations*
JP 3-14, *Space Operations*
JP 3-16, *Multinational Operations*
JP 3-17, *Air Mobility Operations*
JP 3-18, *Joint Forcible Entry Operations*
JP 3-24, *Counterinsurgency Operations*
JP 3-26, *Counterterrorism*
JP 3-27, *Homeland Defense*
JP 3-28, *Defense Support of Civil Authorities*
JP 3-29, *Foreign Humanitarian Assistance*
JP 3-32, *Command and Control for Joint Maritime Operations*
JP 3-33, *Joint Task Force Headquarters*
JP 3-35, *Deployment and Redeployment Operations*
JP 3-40, *Combating Weapons of Mass Destruction*
JP 3-41, *Chemical, Biological, Radiological, or Nuclear Consequence Management*
JP 3-57, *Civil-Military Operations*
JP 3-59, *Meteorological and Oceanographic Operations*
JP 3-60, *Joint Targeting*
JP 3-63, *Detainee Operations*
JP 3-72, *Nuclear Operations*
JP 4-0, *Joint Logistics*
JP 4-01, *The Defense Transportation System*
JP 4-01.2, *Sealift Support to Joint Operations*
JP 4-01.6, *Joint Logistics Over-the-Shore*
JP 4-02, *Health Service Support*
JP 4-08, *Logistics in Support of Multinational Operations*
JP 4-10, *Operational Contract Support*

JPs Revised (within last 6 months)

JP 1, *Doctrine for the Armed Forces of the United States*
JP 1-06, *Financial Management Support in Joint Operations*
JP 2-01, *Joint and National Intelligence Support to Military Operations*
JP 3-01, *Countering Air and Missile Threats*
JP 3-13.1, *Electronic Warfare*
JP 3-13.3, *Operations Security*
JP 3-13.4, *Military Deception*
JP 3-15.1, *Counter-Improvised Explosive Device Operations*
JP 4-01.5, *Joint Terminal Operations*
JP 6-01, *Joint Electromagnetic Spectrum Management Operations*

NEW from *NDU Press*

FORTHCOMING from NDU Press



INSS
INSTITUTE FOR NATIONAL STRATEGIC STUDIES

The People's Liberation Army Air Force: Evolving Concepts, Roles, and Capabilities

Edited by Richard P. Hallion, Roger Cliff, and Phillip C. Saunders

The People's Liberation Army Air Force has undergone a rapid transformation since the 1990s into a formidable, modern air force that could present major challenges to Taiwanese and U.S. forces in a conflict. To examine the present state and future prospects of China's air force, a distinguished group of scholars and experts on Chinese airpower and military affairs gathered in Taipei, Taiwan, in October 2010. This volume is a compilation of the edited papers presented at the conference, rooted in Chinese sources and reflecting comments and additions stimulated by the dialogue and discussions among the participants. Contributing authors include Kenneth W. Allen, Roger Cliff, David Frelinger, His-hua Cheng, Richard P. Hallion, Jessica Hart, Kevin Lanzit, Forrest E. Morgan, Kevin Pollpeter, Shen Pin-Luen, Phillip C. Saunders, David Shlapak, Mark A. Stokes, Murray Scot Tanner, Joshua K. Wiseman, Xiaoming Zhang, and You Ji.

INSS
INSTITUTE FOR NATIONAL STRATEGIC STUDIES

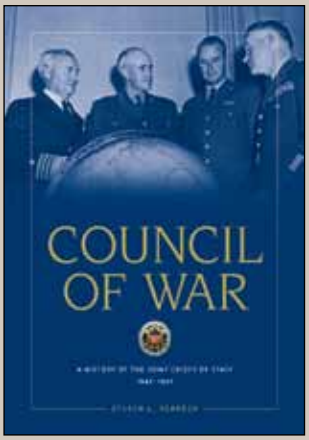
Transatlantic Perspectives, No. 2
The United States, Russia, Europe, and Security: How to Address the "Unfinished Business" of the Post–Cold War Era

Isabelle François

Isabelle François provides concrete ideas for the United States, Russia, and Europe to take with them to the NATO summit in Chicago in May 2012. This is a chance for the three actors to refine their relationships toward the goal of partnership and the ultimate emergence of an inclusive European security community. François provides an assessment of the NATO-Russia cooperation of the past 20 years, concluding that the relationship has yet to deliver a strategic partnership in line with each nation's current rhetoric, documents, and political declarations. François points to a significant level of unfinished business from the post–Cold War, which will have to be addressed if there is any hope of building a whole Europe that is free, undivided, and at peace. The second part of the paper reviews the current challenges facing the NATO Allies and Russia in three main areas: reduction of nonstrategic nuclear weapons in Europe, stalemate regarding conventional forces in Europe, and limits of cooperation in missile defense.

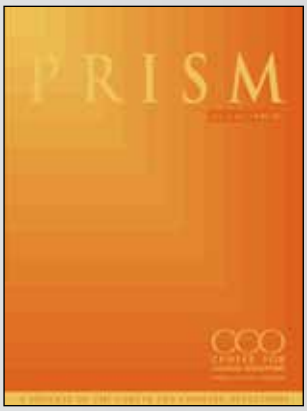
NDU Press

Visit the NDU Press Web site for more information on publications at ndupress.ndu.edu



Council of War: A History of the Joint Chiefs of Staff, 1942–1991

Steven L. Rearden's *Council of War: A History of the Joint Chiefs of Staff, 1942–1991* surveys the role and contributions of the Joint Chiefs of Staff (JCS) from the early days of World War II through the end of the Cold War. The JCS, an organization of military advisors and planners established early in World War II, first advised the President on the strategic direction of U.S. Armed Forces in that war and continued afterward to play a significant role in the development of national policy. Because of their relations with the President, the Secretary of Defense, and the National Security Council, a history of their activities, both in war and in peacetime, provides insights into the military history of the United States. The importance of their activities led the JCS to direct that an official history of their actions be kept for future generations to study. Dr. Rearden's *Council of War* follows in the tradition of volumes previously published about JCS involvement in national policy, the Korean War, and the Vietnam War. Using a combination of primary and secondary sources, and adopting a broader view of previous volumes, this fresh work of scholarship examines the military implications of problems from 1942 to 1991. Although focused strongly on the JCS, Rearden's well-researched treatise deals too with the wider effect of crucial decisions and their ensuing policies.



PRISM

A Journal of the Center for Complex Operations

PRISM 3, no. 3 (June 2012), opens "Features" with Dennis Blair proposing ways in which developed democracies can use their military-military relations to assist democratic development around the world; Colin Gray brings strategic theory to the discussion of rival doctrines about counterinsurgency; Andrea Barbara Baumann focuses on coordination of civilian and military organizations within a whole-of-government approach; Mark Sedra critiques current state-building policy and practice; Lant Pritchett, Michael Woolcock, and Matt Andrews discuss how some developing countries are stuck in a "capability trap"; Nadia Gerspacher and Adrian Shtuni offer initial lessons learned from MoDA in which civilians are building institutional capacity and helping demilitarize security institutions; William Upshur, Jonathan Roginski, and David Kilcullen outline a simplified yet descriptive method of assessing counterinsurgency campaigns; Lesley Anne Warner provides context for Kenya's October 2011 invasion of Somalia; and Dov Zakheim offers five observations on the do's and don'ts of state-building. In "From the Field," Robert Hulslander and Jake Spivey examine Village Stability Operations and Afghan Local Police, while the "Lessons Learned" section features Geoffrey Lambert, Larry Lewis, and Sarah Sewall weighing in about military support provided by U.S. Joint Special Operations Task Force–Philippines to Philippine military operations. Closing out the issue is an interview with Álvaro Uribe Vélez, the 58th president of Colombia (2002–2010).

CCO
CENTER FOR
COMPLEX OPERATIONS
DIPLOMACY • DEFENSE • DEVELOPMENT

PRISM explores, promotes, and debates emerging thought and best practices as civilian capacity increases in order to address challenges in stability, reconstruction, security, counterinsurgency, and irregular warfare. Published by NDU Press for the Center for Complex Operations, *PRISM* welcomes articles on a broad range of complex operations issues, especially civil-military integration. Manuscript submissions should be between 2,500 and 6,000 words and sent via email to prism@ndu.edu.

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