

JFQ

Issue 61, 2^d Quarter 2011

Operational Cyber

Expeditionary Economics

An Islamic Way of War?



Inside

Issue 61, 2^d Quarter 2011

Editor **Col William T. Eliason, USAF (Ret.), Ph.D.**
Executive Editor **Jeffrey D. Smotherman, Ph.D.**
Supervisory Editor **George C. Maerz**
Production Supervisor **Martin J. Peters, Jr.**
Senior Copy Editor **Calvin B. Kelley**
Book Review Editor **Lisa M. Yambrick**
Visual Design Editor **Tara J. Parekh**
Copy Editor/Office Manager **John J. Church, D.M.A.**
Internet Publications Editor **Joanna E. Seich**
Design **Amy Ellis, John Mitrione, Jessica Reynolds,**
U.S. Government Printing Office

Printed in St. Louis, Missouri



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.

This is the official U.S. Department of Defense edition of *JFQ*. Any copyrighted portions of this journal may not be reproduced or extracted without permission of the copyright proprietors. *Joint Force Quarterly* should be acknowledged whenever material is quoted from or based on its content.

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

2^d Quarter, April 2011
ISSN 1070-0692



JFQ Dialogue

- 2 From the Chairman
- 6 Letters to the Editor

Forum

- 8 Executive Summary
- 10 Ten Propositions Regarding Cyberspace Operations
By Brett T. Williams
- 18 Cyber War: Issues in Attack and Defense
By Robert A. Miller, Daniel T. Kuehl, and Irving Lachow
- 24 Digital Gunnery: It's About Time
By John A. Macdonald and Martin K. Schlacter
- 27 Principles of (Information?) War
By Francis Hsu

Special Feature

- 32 Institutionalizing Economic Analysis in the U.S. Military:
The Basis for Preventive Defense *By Carl J. Schramm*
- 39 Expeditionary Business in the 21st Century
By Robert E. Love and Steve R. Geary
- 43 Savings and the Defense Logistics Enterprise
By C.V. Christianson

Commentary

- 47 Rethinking Foreign Area Officer Management
By William E. Ward
- 53 A Smarter Force for Less Time and Money
By Stephen D. Pomper
- 56 Building Credible Voices: Traditional Communication in Afghanistan
By Robert M. Hill
- 64 The Future of National Security, By the Numbers
By P.W. Singer

Features

- 72 Transformation Achieved? Revisiting the 1997 National Defense Panel
By Ricardo A. Marquez
- 81 An Islamic Way of War? *By Adam Oler*
- 89 Why Unmanned *By Paul Scharre*



JFQ

Features

94 Security Cooperation, Security Assistance, and Building Partner Capacity: Enhancing Interagency Collaboration
By Sharif Calfee, Joseph Lee, Peter Crandall, and Young Rock An

100 Preventing War in the Middle East: A Role for NATO?
By Kenneth Weisbrode

Recall

103 Decisiveness in War *By Phillip S. Meilinger*

Book Reviews

109 The Gulf Wars and the United States
Reviewed by Stephen A. Bourque

110 Deciphering the Rising Sun
Reviewed by Robert J. Hanyok

111 Better Safe than Sorry
Reviewed by Francesco N. Moro

112 War
Reviewed by James P. Terry

113 Death by Moderation
Reviewed by David M. Oaks

Joint Doctrine

114 Joint Chiefs of Staff J7, Joint Education and Doctrine Division
By George E. Katsos

115 Defining Asymmetric Warfare: A Losing Proposition
By Jesse G. Chace

PUBLISHER

ADM Michael G. Mullen, USN

PRESIDENT, NDU

VADM Ann E. Rondeau, USN

ADVISORY COMMITTEE

Maj Gen Joseph D. Brown IV, USAF *Industrial College of the Armed Forces*

Gen James E. Cartwright, USMC *The Joint Staff*

LTG Robert L. Caslen, USA *U.S. Army Command and General Staff College*

LtGen George J. Flynn, USMC *USMC Combat Development Command*

VADM William E. Gortney, USN *The Joint Staff*

Maj Gen Robert C. Kane, USAF *Air War College*

RADM Douglas J. McAneny *National War College*

John A. Nagl *Center for a New American Security*

Maj Gen Robert B. Neller, USMC *Marine Corps War College*

VADM Daniel T. Oliver, USN (Ret.) *Naval Postgraduate School*

LtGen John M. Paxton, Jr., USMC *The Joint Staff*

Brig Gen Anthony J. Rock, Jr., USAF *Air Command and Staff College*

Brig Gen Marvin T. Smoot, USAF *Joint Forces Staff College*

ADM James G. Stavridis, USN *U.S. European Command*

RADM James P. Wisecup, USN *Naval War College*

EDITORIAL BOARD

Richard K. Betts *Columbia University*

Stephen D. Chiabotti *School of Advanced Air and Space Studies*

Eliot A. Cohen *The Johns Hopkins University*

COL Joseph J. Collins, USA (Ret.) *National War College*

Col Mark J. Conversino, USAF (Ret.) *Air War College*

Aaron L. Friedberg *Princeton University*

Col Thomas C. Greenwood, USMC (Ret.) *Institute for Defense Analyses*

Alan L. Gropman *Industrial College of the Armed Forces*

Douglas N. Hime *Naval War College*

Mark H. Jacobsen *Marine Corps Command and Staff College*

CAPT John F. Kirby, USN *The Joint Staff*

Daniel T. Kuehl *Information Resources Management College*

Thomas L. McNaughter *The RAND Corporation*

Kathleen Mahoney-Norris *Air Command and Staff College*

Col Mark Pizzo USMC (Ret.) *National War College*

James A. Schear *Office of the Secretary of Defense*

LtGen Bernard E. Trainor, USMC (Ret.)

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.

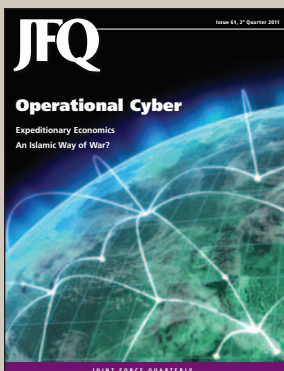
Joint Force Quarterly is published by the National Defense University Press for the Chairman of the Joint Chiefs of Staff. *JFQ* is the Chairman's flagship joint military and security studies journal designed to inform members of the U.S. Armed Forces, allies, and other partners on joint and integrated 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.

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

ndupress.ndu.edu

ABOUT THE COVERS

Table of contents (left to right): MQ-1 Predator crewmembers inspect sensor (U.S. Air Force/Larry E. Reid, Jr.); Sailors and Afghan contractors build helicopter landing pads at Forward Operating Base Khilaguy, Afghanistan (U.S. Navy/Michael B. Watkins); Navy demonstrates autonomous unmanned surface vehicle (U.S. Navy/Joshua Adam Nuzzo); and team unloads CH-53E on flight line (Fleet Readiness Center-East/Dykie Whitfield).

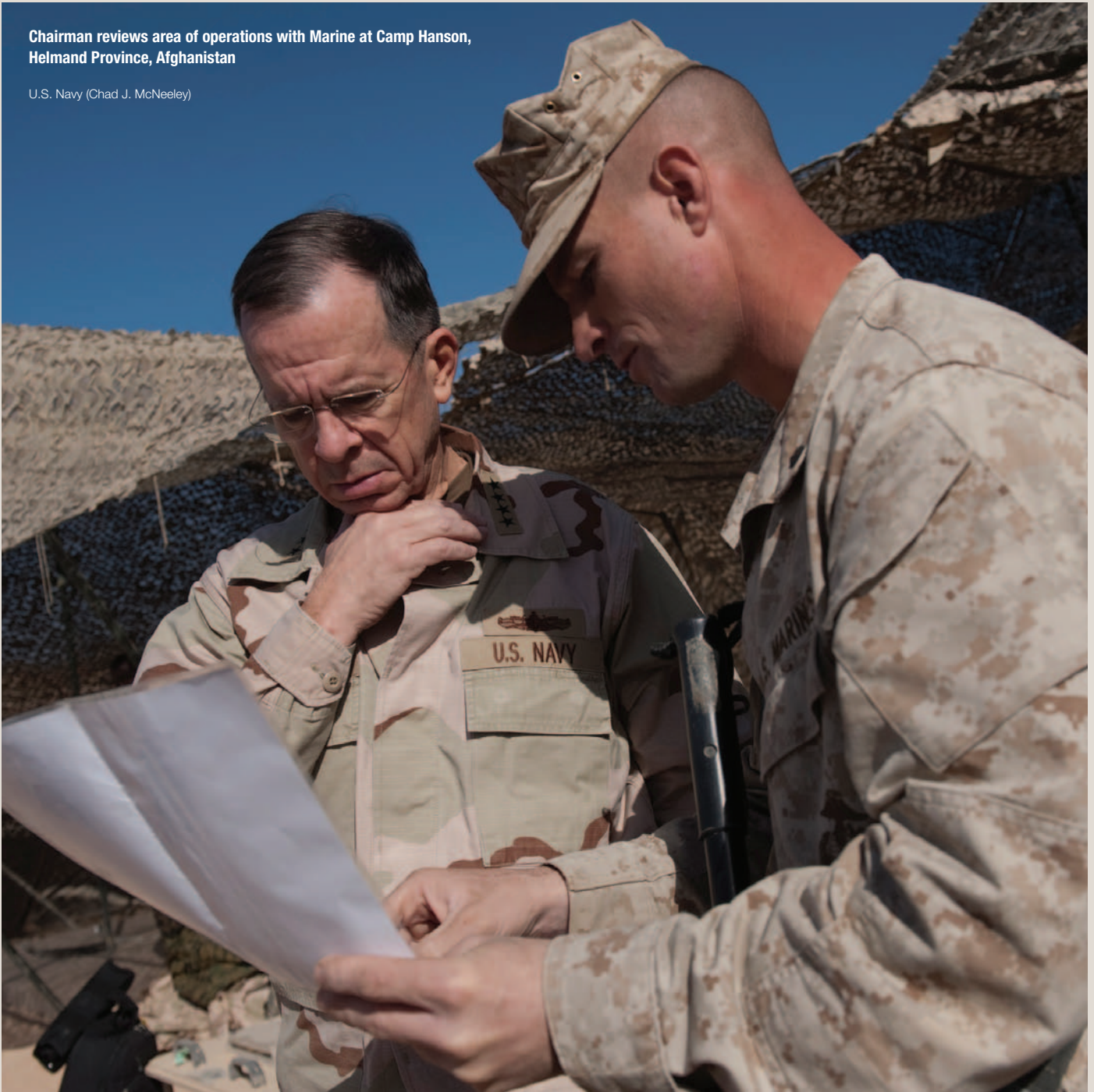


From the Chairman

Leadership and the 2011 National Military Strategy

Chairman reviews area of operations with Marine at Camp Hanson, Helmand Province, Afghanistan

U.S. Navy (Chad J. McNeeley)



The Nation is at a strategic inflection point and must continue to adjust to a redistribution of power in the international order. The United States and its allies and partners will find themselves competing for influence in an environment in which persistent tension is the norm. We—the joint force—seek to prevent this tension from escalating into conflict. Above all, however, we must remain capable of fighting and winning the Nation's wars.

Earlier this year, I published *The National Military Strategy of the United States of America 2011: Redefining America's Military Leadership*. In consultation with the combatant commanders and Joint Chiefs of Staff, I prepared this document to articulate the ways and means by which the joint force will advance the Nation's enduring interests and support its strategic objectives.

the emerging security environment demands that we pursue wider and more constructive partnerships

Guided by the National Security Strategy and Quadrennial Defense Review, the U.S. military strategy advances three broad themes. First, in defending and advancing the Nation's interests, the joint force leadership approach will often be as important



Marines with IED detector dog patrol in Kajaki, Afghanistan

U.S. Marine Corps (Matthew P. Troyer)

as the military capabilities we provide. Second, the emerging security environment demands that we pursue wider and more constructive partnerships—public and private, bilateral, trilateral, and multilateral. And third, we must adapt full-spectrum joint force capabilities and attributes to the emerging threat environment to ensure that we can continue to deter and defeat aggression.

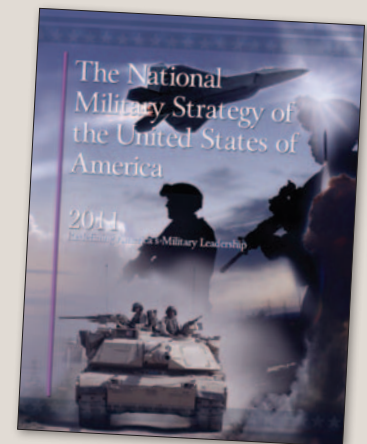
As much as ever, there is a profound need and desire for America's continued military leadership. At the same time, changes in the global environment suggest that we must redefine *how* we lead. Leadership is about more than power; it is about our approach to exercising power. Our strategy calls for employing a spectrum of leadership roles—facilitator, enabler, convener, and guarantor—sometimes simultaneously. And in all these roles, we will emphasize mutual responsibility and respect.

In many ways, this has been the key to our success over the last 9 years of sustained combat operations. In Iraq, for example, the military supported whole-of-nation efforts to



Soldiers support Iraqi army during cordon and search outside Joint Security Station Basra Operations Command

U.S. Army (Joshua E. Powell)





F-22 Raptor drops back from KC-135 after refueling

create conditions for a sustainable and stable political environment. In turn, we are creating an unprecedented partnership to enable Iraq's fledgling security forces to partner in combating extremism and contribute to greater security in the Middle East. Our approach is similar in Afghanistan, and we are starting to see progress there.

leadership is about more than power; it is about our approach to exercising power

As an institution with profound convening power, from the halls of our war colleges to the largest multinational exercises in the world, our values, relationships, and military capabilities are bringing others together to help deepen security relationships and address common security challenges. Lastly, our unmatched core military capabilities to deter and defeat acts of aggression allow us to act as a guarantor that can underwrite security

when our interests or those of our allies and partners are threatened.

While this strategy is informed by institutional lessons and constraints from nearly a decade of conflict, it also focuses on areas of forward and innovative thinking. First, we must embrace our role in developing a strategic, whole-of-nation approach to combating violent extremism. Second, we must provide deterrence against a full spectrum of threats—strategic, conventional, and 21st-century threats such as cyber aggression and violent extremism.

Third, we must employ a comprehensive approach to defeating aggression. Since warfighting domains are becoming increasingly interdependent, assured access for the joint force to the global commons will remain critical to defeating aggression and countering emerging antiaccess and area-denial strategies. In turn, the joint force must develop new capabilities to fight through degraded domain environments and place increased emphasis on our enabling capabilities—from cyber and space, to intelligence, surveillance, and reconnaissance, and logis-

tics. Cyber and space, which are simultaneously enabling and warfighting domains, deserve special attention to ensure that we can operate effectively.

Finally, we must reconcile U.S. national interests with the emerging strategic environment to help inform global force posture decisions. The National Military Strategy points to an increased geographic emphasis on Asia, delineates the capabilities required to succeed in this theater, and argues that we need to leverage expanded and more effective

we must embrace our role in developing a strategic, whole-of-nation approach to combating violent extremism

relationships to enhance regional stability. It is my hope that these topics will inspire new and creative thinking that will fill the pages of this journal and others in the months and years ahead. The need is certainly there.

The key to implementing this strategy will remain, as it has in the past, our people and their families. The all-volunteer force will remain the military's greatest strategic asset. We must continue to recruit, train, grow, and nurture leaders who can truly out-think and out-innovate our adversaries while gaining the trust, understanding, and cooperation of an expanding set of partners.

the all-volunteer force will remain the military's greatest strategic asset

In addition, we must think about our civil-military continuum more broadly to ensure that we are not only retaining the highest quality joint force possible, but also setting the conditions for our veterans' success as they make the difficult transitions from war to back home and then eventually to civilian life. Successful veterans are powerful advocates in our communities for the military and critical enablers to sustaining the all-volunteer force through the inspirational model of their example.

Our mission set has evolved, but our core objectives have not. The National Military Strategy provides a road map for the way the military will deter, fight, and win the Nation's wars in a dynamic and uncertain world. If the past is prologue, there will be challenges in this century that we have yet to imagine, but I am confident that they will be met by the leadership, partnership, and creativity of the men and women of the U.S. military. This strategy aims to provide them a way ahead that is every bit as good as they are, and I encourage every leader to read it, discuss it, debate it, and if needed, refine it.

I look forward to hearing from all of you as we implement this strategy together. **JFQ**

MICHAEL G. MULLEN
Admiral, U.S. Navy
Chairman of the Joint Chiefs of Staff



U.S. Navy (Jat lon A. Rhinehart)

Sailors and Coastguardsmen stop skiff suspected of participating in pirate activity in Gulf of Aden



NEW
from **NDU Press**

for the
Africa Center for Strategic Studies



The Africa Security Briefs series presents research and analysis by Africa Center for Strategic Studies (ACSS) experts and outside scholars with the aim of advancing understanding of African security issues. Published for ACSS by National Defense University Press, each issue is produced in English, French, and Portuguese editions (Portuguese edition available only online).

Africa Security Brief 11

West Africa's Growing Terrorist Threat: Confronting AQIM's Sahelian Strategy

Africa Security Brief 10

Investing in Science and Technology to Meet Africa's Maritime Security Challenges



Forging Partnerships for Africa's Future

The Africa Center offers a variety of resources that keep readers abreast of the Africa-related news and research published on this site.

<http://africacenter.org/>

To subscribe to Africa Center's Daily Media Review and/or Africa Security Briefs, go to <http://africacenter.org/subscribe/>, enter email address, check the box next to the name of the newsletter(s) desired, and click the "Submit" button.

Visit the NDU Press Web site
for more information on publications
at ndupress.ndu.edu

LETTERS

To the Editor—I was confused by part of Sebastian Gorka and David Kilcullen’s article “An Actor-centric Theory of War: Understanding the Difference Between *COIN* and *Counterinsurgency*” (*JFQ* 60, 1st Quarter 2011). The authors “propose that a theory of war based on who is using violence against us makes much more sense today than theories based on putative generational changes in warfare or the asymmetry of combatants” (p. 15).

First, this seems to be a theory of *warfare* and not *war*, a distinction I think we can all agree is critical. It certainly was to Carl von Clausewitz. I further observe that what is being proposed is not *theory* but rather *taxonomy*. I again submit that the distinction is critical.

Moreover, are not “actor-centric” taxonomies the norm in describing warfare? *Irregular warfare* is warfare conducted by or against irregulars. There is no really useful or definable “irregular” or even “guerrilla” style of warfare, despite what some may claim. *Guerrilla warfare* is that conducted by guerrillas, a word that has its origin in the Spanish diminutive of *war*—thus, *small war*. The popular and useful description *small wars* refers to warfare conducted by “irregulars.” Indeed, this was the definition that C.E. Callwell, author of *Small Wars*, used. Insurgencies are, after all, conflicts conducted by insurgents. I submit that this is common, enduring, and useful.

Thus, when the authors state that “irregular warfare is, therefore, more regular or conventional than our strategic lenses would propose” (p. 17), they completely miss both the original and the useful meaning of the term *irregular warfare*. Frequency is not a qualifier and never has been. At the risk of pushing this to an absurd degree, I would even go so far as to point out that “armored warfare” is that conducted by armored forces.

All in all, I am struggling to think of any useful description of warfare “based on putative generational changes in warfare or the asymmetry of combatants” that is in common use. The descriptions that employed “fourth generation” and “asymmetry” were never widely used and are very much in an extreme minority. AirLand Battle was never a description of warfare; it was an operational concept or doctrine associated with Field Manual 100–5, *Operations*, during the 1980s.

For some years, many writers, and notably Professor Colin Gray, have been using the enduring description of regular and irregular warfare based on the actors involved—thus, my contention that what Gorka and

Kilcullen are proposing is arguably already in place and has been for some considerable time.

I agree with the authors that the nature of the entire discussion has been woeful, but I would add that this has been somewhat obvious for the past 7 years, and many people have remarked on it. To that end, I cannot see how an “actor-centric theory of war” in any way advances us past the point where we have been for some time, even if it were an original idea. The same level of debate is likely to continue regardless of a supposedly new taxonomy of warfare.

The problem with the debate as a whole is the lack of any intellectual rigor, which leads some to think that irregular warfare is defined by something other than one of the participants. I do agree that “war is war” (“and not popularity seeking,” to complete the passage), which I think most of us would have attributed to William Tecumseh Sherman, rather than Carlos Ospina.

—William F. Owen
Tel Aviv

To the Editor—I am pleased to see *JFQ* publish an article on private contractors (T.X. Hammes, “Private Contractors in Conflict Zones: The Good, the Bad, and the Strategic Impact,” *JFQ* 60, 1st Quarter 2011). Having recently completed a book manuscript on the topic of private security contractors (*Patriots for Profit: Contractors and the Military in U.S. National Security* [Stanford University Press, forthcoming]), I am not optimistic that Dr. Hammes’s recommendations for reform could be implemented or, if they were, that they would make much difference in remedying the many bad aspects he accurately identifies arising from the U.S. Government’s use of contractors in conflict zones.

When Dr. Hammes writes about the “[George W. Bush] administration’s faith in the efficiency and effectiveness of private business compared to governmental organization” (p. 27), an uninformed reader might think he is suggesting that the use of contractors began with that administration. In fact, the emphasis on contracting goes back at least to the Presidency of Ronald Reagan and took on extra momentum during the 8 years of the Clinton administration.

Federal contracting policy is governed by the Federal Acquisition Regulation and the Federal Activities Inventory Reform

Act of 1998. The Office of Management and Budget (OMB) in Circular A–76 provides specific guidance for competitive sourcing. In the United States, there is a huge emphasis on contracting, including in conflict zones, and I see few indications that the reliance on contractors will diminish during the current administration. The emphasis on contracting, including national security and defense, is ingrained in American political culture and supported in extensive legislation.

The emphasis on improving or reforming the bad aspects that Dr. Hammes identifies has come mainly from Congress, which has conducted extensive hearings on private contracting, directed the Government Accountability Office (GAO) to investigate all aspects of contracting, created the Special Inspector General for Iraq Reconstruction (SIGIR) in 2003 and the Special Inspector General for Afghanistan Reconstruction (SIGAR) in 2008, and provided guidance in the National Defense Authorization Act for fiscal year 2008 to the Department of Defense regarding “contractors performing private security functions in areas of combat operations.” Although Dr. Hammes notes the existence of the Commission on Wartime Contracting, which was created by Congress in 2008, he neither acknowledges the role of Congress nor cites SIGIR or SIGAR, although both have Web sites rich in reports and audits. Virtually all of the bad aspects identified in the article have been extensively documented in GAO, SIGIR, and SIGAR reports and audits. The fact that serious reform has yet to be implemented is not due to a lack of information, but rather to political and bureaucratic realities.

Two of these realities must be noted if only to put some perspective on the difficulty of implementing reforms. First, private contractors, including private security contractors, constitute a profit-making industry. Thus, while Dr. Hammes apparently puts some faith in the Commission on Wartime Contracting to reform “inherently governmental functions,” congressional guidance to OMB to define “inherently governmental functions” by October 2009 did not result in much. The interim definition by OMB on March 31, 2010, is still vague enough to allow private security contractors to engage in what most objective outsiders would consider inherently governmental functions.

Second, contractors in conflict zones will only be under control and effective if there are U.S. Government employees, in

uniform or not, in sufficient numbers with adequate training and guidance to oversee them. Dr. Hammes acknowledges this point, which is extensively documented in the Gansler Report (“Urgent Reform Required: Army Expeditionary Contracting,” Report of the Commission on Army Acquisition and Program Management in Expeditionary Operations, October 31, 2007). From what I can determine by meeting with faculty and students in the Contracting Management curriculum here at the Naval Postgraduate School, the Services are slow to respond. And the temptations to leave the Services and join industry, with its higher salaries and fewer bureaucratic headaches, are hard to resist.

Based on my research with secondary literature and government documents that finally entailed six 1-week-long research trips to Washington, DC, I am not at all confident that we will soon see any significant improvement in the stark picture that Hammes so accurately describes.

—Thomas C. Bruneau
Distinguished Professor of
National Security Affairs
Naval Postgraduate School

To the Editor—Lieutenant Colonel Eric A. Hollister’s article, “Ike Warned Us About This: The MICC Stranglehold on Responsible Procurement” (*JFQ* 59, 4th Quarter 2010), portrays a rather misleading and incomplete analysis of widespread open source information, while missing key studies that a thorough literature review would have uncovered. The article has critical errors and leaves out vital information. Additionally, it conveys a one-sided critique of major weapons system acquisitions, focusing almost exclusively on Air Force programs. As a result, his analysis largely reflects an emotional and parochial view. An objective review of the military-industrial-congressional complex (MICC) literature leaves no Service, and no part of the MICC, unscathed from acquisition scandals or major criticism.

The author should have interviewed several knowledgeable tanker, acquisition, or congressional experts to verify and critically analyze his information. Also, he should have looked beyond the easy open source information. That lack of due diligence could lead readers to a number of erroneous conclusions. For example, there is a clear misunderstanding of the different tanker models: “Repeated studies . . . have determined that KC-135Es were ‘structurally viable until 2040,’ and the KC-135R variants could be flown until 2030” (p. 91).

Fact: KC-135Es have never been predicted to be more structurally viable than KC-135Rs, and all the KC-135Es were retired by 2009.

An example of missing information includes a spring 2001 Air Force letter to Congress requesting an analysis of alternatives (AoA) for a KC-135 replacement—Congress did not approve. Had the Air Force conducted an AoA in 2001 or after the fiscal year 2002 appropriations bill, the tanker imbroglio most likely would not have emerged. Additionally, it seems incredible that Colonel Hollister only casually mentioned Senator John McCain, the driving force behind most of the tanker investigations; when Senator McCain was mentioned, it was only related to the “split buy” issue that is peripheral to the overall saga. Several critical issues missed were Senator McCain’s concern of how the congressional appropriations process usurped the defense authorizing committees’ authority, and the cost-benefit analysis of the lease—illustrating a very bad deal for taxpayers.

The author addressed two defense industry practices: front-loading and political engineering. What he missed, however, were Air Force recommendations during the 2001 Quadrennial Defense Review to modify commercial-off-the-shelf (COTS) aircraft as tankers (a significant change in acquisition strategy) largely from the commercial industrial base that would substantially mitigate concerns of front-loading and political engineering (with significant savings). Additionally, modified COTS aircraft move us closer to the Packard Commission Acquisition Reform (1986) recommendations: “fly-before-you-buy” acquisition instead of building from “rivet one” with multiple billions of research and development dollars before anything flies or is tested. Building from rivet one is an acquisition strategy that fosters much more front-loading and political engineering pathologies.

The topics covered by Colonel Hollister are extremely important and worthy of thorough and comprehensive study. Tragically, the need for and importance of tankers are even more critical to national security than the author conveyed—especially in light of recent emerging threats. The uncertainty surrounding the service life of KC-135s (and problems with the KC-10s), the associated cost growth and availability of tankers of the future, and the time to recapitalize these aircraft drive unacceptable strategic risk that is exacerbated by extended efforts to identify its replacement.

—Dr. Carl D. Rehberg
(Colonel, USAF, Ret.)
Chief, Air Force Long Range Plans
(2004–2008)



NEW
from **NDU Press**

for the
Institute for National Strategic Studies

Strategic Forum 265

Finland, Sweden, and NATO: From “Virtual” to Formal Allies?

Leo Michel examines the possibility of Finland and Sweden formally joining NATO. Since the early 1990s, the two countries have transformed their security policies and defense structures in ways that improve their ability to work closely with America. Both favor close cooperation with the Alliance, despite their official stance of “military non-alignment.” The author discusses the pros and cons of possible accession, noting that Finland is better positioned politically than Sweden to seek membership. He advises NATO to be patient, to stay the course chartered by its Strategic Concept, and to demonstrate solidarity and effectiveness—thereby remaining the essential force for Euro-Atlantic stability and security that has attracted countries to join its ranks.



Strategic Forum 264

European Energy Security: Reducing Volatility of Ukraine-Russia Gas Pricing Disputes

Despite recent agreements between Russia and Ukraine over natural gas pricing, the basic issues that caused a gas shutdown in 2009 remain unresolved. Why should the United States be concerned about the annual gas-pricing brinkmanship played by the two countries? Richard B. Andres and Michael Kofman explain why, noting that when such talks break down, our European allies suffer; and, equally important, the problem’s resolution will have important implications for power politics in the region. As Russia positions itself for a takeover of Ukrainian pipeline infrastructure, the authors urge the European Union to consider a serious investment in Ukraine to prevent complete Russian control over its energy security.



Visit the **NDU Press** Web site
for more information on publications
at ndupress.ndu.edu

Executive Summary

As an Airman, I have long heeded the words of Giulio Douhet on anticipating the changes in war, even in the battle of everyday life. Each of us has experienced the impact of a dramatic moment and often wondered why we did so little to anticipate it and then turned to thoughts of what we could have done. A series of such events is unfolding in the Middle East as this issue goes to press. While we cannot quite make out how the strategic landscape will evolve, we all will make adjustments in how to think and operate in the new reality that emerges. This is what Douhet had in mind. Toward that end, this issue of *Joint Force Quarterly* focuses on two topics that will figure prominently in that future strategic landscape: cyber and economics.

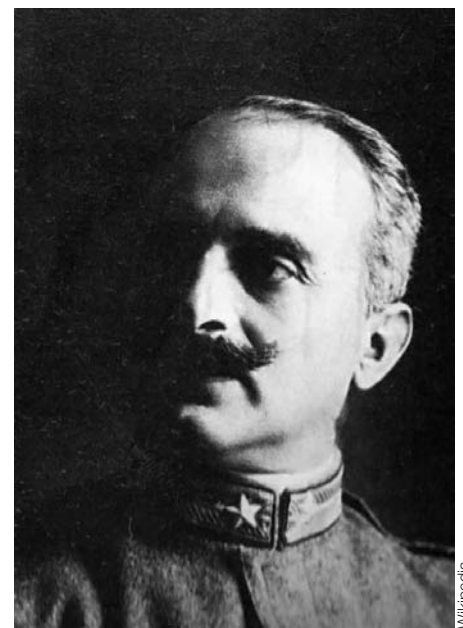
In the Forum, thinking about cyber takes center stage. Major General Brett Williams, a career Air Force fighter pilot who recently completed a tour as U.S. Pacific Command's communications director, leads off with an interesting and important update to Colonel Phil Meilinger's *10 Propositions Regarding Air Power*, with the general's insights on how to operationalize cyber for the joint fight. Independently from the General's work, three well-known cyber experts, Professors Robert Miller and Dan Kuehl of National Defense University's (NDU's) iCollege and Dr. Irving Lachow of MITRE offer 10 requirements the Nation must accomplish to prepare to defend and, if necessary, go on the offense in a cyber war. Given the constant requirement for readiness and vigilance of our combined force on the Korean Peninsula, Major General John MacDonald, Assistant Chief of Staff, C3/J3, United Nations Command/Combined Forces Command (CFC)/United States Forces Korea (USFK), and Lieutenant Colonel Martin Schlacter, Chief of Combined Data Network Operations for CFC and USFK,

report on the successful achievement of a decades-long effort to achieve fully integrated, combined digital exercises. As has been the case in every new area of warfare, figuring out how it fit into existing concepts, doctrine, and operations required a great deal of prevailing thought to be "rethink." Toward this end, we add Francis Hsu's very challenging thinker's article that asks you to consider just where cyber fits into our view of the principles of war.

Long a part of any strategic considerations in dealing with the aftermath of conflict, economics is too often left for others to sort out when military planners look at future operations. Warfighters normally are not business school graduates, but as our experiences in Iraq and Afghanistan have played out, creating markets in a war zone has become a part of the Provincial Reconstruction Team or infantry company commander's task list. This shift in military operations has given rise to discussion of "Expeditionary Economics," and our Special Feature section adds to the conversation on this emerging theme. Carl Schramm calls for the military to institutionalize economic analysis as an essential process to better prepare the Nation for success in future operations. Operationalizing business engagement on the ground in a conflict area is the theme of Robert Love and Steven Geary's article. On the support side of the military, Lieutenant General C.V. Christianson suggests a framework of improvements to our approach to the Defense Logistics Enterprise, including education for logistics professionals.

In Commentary, authors explore a range of ideas. Reflecting on his experiences as the first commander of U.S. Africa Command, General Kip Ward offers recommendations for revamping Foreign Area Officer management policies in all Services to better serve individual officers' career paths while significantly improving their contributions

to national security and regional objectives. Lieutenant Colonel Steven Pomper suggests changing public law to allow Reserve Officer Training Corps Cadets and Midshipmen to take part in 5-year advanced degree programs, which would provide a superior quality of junior officer to the Services. In recommending *traditional communication*, a local culture-based means of sending strategic messages, Dr. Robert Hill leverages his recent experience in Afghanistan, where he served as a public affairs officer and advisor to the International Security Assistance Force Deputy Chief of Staff for Communication. Dr. Hill believes using a local population's normal means of passing messages seems an obvious method but was one that had not been well used prior to his tour. As the final Commentary article tees up some interesting views on the need for serious adjustments in the Federal budget,



General Giulio Douhet, the Father of Airpower, advocated strategic bombing and military superiority of air forces

Wikipedia



U.S. Air Force (Adrian Cadiz)

Airman tears down panels used to mark landing zone for C-130 at Forward Operating Base Lagman, Afghanistan

Dr. Peter Singer takes us through his review of the “new math” confronting the Defense Department and the Government. Given the continuing global economic situation, Dr. Singer underscores the need to make realistic assessments of what *should* be done balanced with what *can* be done.

The Features section delivers on the Chairman’s tasking to me to seek out good writing and thinking from Professional Military Education students. The first article, an individual effort from National War College student Lieutenant Colonel Adam Oler, offers an important historical view, if one counter to popular opinion, of the relationship of Islam to war. The second student paper is an excellent group project from four Joint Forces Staff College students with a new take on enhancing interagency partnership in three important precrisis missions. Other selections look back at the 1997 Quadrennial Defense Review as it plays out today; discuss the requirement for unmanned military vehicles of all kinds; and take a new view of how the North Atlantic Treaty Organization can be used to keep the peace in the Middle East. The Recall section

features Dr. Phil Meilinger’s latest work on military decisionmaking in war. The issue is rounded out with four excellent book reviews and a challenge to efforts to doctrinally define asymmetric warfare, along with the Joint Doctrine Update.

On a more personal note, the reality of stepping up to a new challenge as the Editor of *JFQ* requires a different kind of strategic foresight, planning the content of forthcoming issues at least 3 months in advance. Whether in print or online, *JFQ* continues to gain readers each month, which keeps the NDU Press team focused on producing a quality product. As Editor, I need three things from our readers to make sure we succeed. First, I look forward to a constant stream of high-quality contributions from every corner of the joint force that will serve to engage and educate our readers. If your contribution passes this simple test, then I will work hard to find room for you to be published. Second, I need you to pass the word to your “battle buddies,” no matter where you are. If you can access the Internet or a mailbox, you can receive *JFQ* and send it to others. If knowledge

is power and *JFQ* has knowledge that you believe is worth passing on, take up the challenge to pass it on. I am absolutely convinced the key strength of our modern military is our willingness to learn and adapt. *JFQ* should be a part of that process. Finally, I seek the same type of honest and well-considered feedback that I expected in the classroom, the mission debrief, or on the line. Whether you are in uniform or not, have served in combat or not, we will provide you with a platform for open and informed debate on the issues related to the Joint Force.

Found something you liked (or something you didn’t) or have a valuable contribution to make? By all means, connect with us at JFQ1@ndu.edu, and together we can better prepare ourselves to anticipate the changes in the world ahead. **JFQ**

—William T. Eliason
Editor

Soldier checks functionality of GPS units for Afghan National Police training



TEN PROPOSITIONS *Regarding* CYBERSPACE OPERATIONS

By BRETT T. WILLIAMS

In trying to defend everything, he defended nothing.

—Frederick the Great

I have been the Director for Command, Control, Communications, and Computers (J6) at U.S. Pacific Command for almost 2 years. I came into this position with 28 years of warfighting experience as a fighter pilot and operational commander. The commander charged me with “operationalizing” the J6. I have focused most of my effort on cyberspace operations and have been challenged by the general unwillingness to apply accepted concepts of operational art to the cyber domain. The Prussian’s axiom in the epigraph on defense is a perfect example. In cyberspace, we attempt to defend everything. We attempt to protect the entire Department of Defense (DOD) Global Information Grid (GIG) against thousands of intrusion attempts every day. While there are many successes, we tolerate the fact that even a single failure could have significant impact. We need to stop trying to defend everything and instead find ways to compartmentalize risk and prioritize efforts against those components of cyberspace most critical for operational warfighting.

Our approach to cyberspace operations must change. Currently, the focus is primarily global with secondary regard for the specific priorities of combatant commanders. Cyber “experts” argue for the global approach because they see a direct analogy between the cyber domain and space. As I consider the ever-increasing scale, scope, and tempo of cyber activity compared to the warfighting

needs of the joint force commander (JFC), it is obvious that treating cyber like space is a mistake. This thinking produces a global command and control model that is acceptable for peacetime “enterprise” efficiency but is suboptimal for wartime. Global control does not provide the integration, responsiveness, and agility necessary for cyberspace operations at the theater level.

*if the discussion is focused
at the operational level of
war, we find that cyberspace
operations are actually quite
similar to those in other
domains*

This article acknowledges the global nature of the virtual domain, but argues for equal emphasis at the regional level. The challenge is making the cognitive connection between the virtual and physical worlds. Warfighters who have already made that connection understand that cyber operations at the operational level of war are actually quite similar to air, land, and maritime operations. This article explains that connection and allows us to apply the time-tested maxims of Frederick the Great and other warriors to cyberspace operations.

In 1995, Phillip Meilinger published a short book entitled *10 Propositions Regarding Airpower*, in which he offered 10 simple statements, each describing a characteristic of airpower. A short, persuasive narrative provided context to each proposition. The 10 propositions affected how we taught, thought about, and developed airpower doctrine. In a

similar way, the following 10 cyber propositions are intended to stimulate debate and discussion concerning command and control of cyberspace operations.¹

A note on terms. *Domain* refers to the five warfighting domains of land, maritime, air, space, and cyber. *Physical domains* are the four that exist in the physical world, and the *virtual domain* is cyberspace. *Terrestrial domains* are land, maritime, and air.

1. *Cyberspace is a warfighting domain. At the operational level of war, cyberspace operations are most similar to those in land, maritime, and air.*

In 2008, DOD defined *cyberspace* as a warfighting domain. This declaration was an acknowledgment of cyberspace’s critical role in national security. A prevailing argument is that as a domain, cyber is unique and therefore requires an entirely new warfighting approach. Cyber is indeed unique, but it is not any “more unique” than land, maritime, air, and space. Each of the four physical domains has distinctive characteristics that require application of specialized doctrine, policy, resourcing, and expertise for mission success. In this regard, cyberspace is no different. Cyber appears to be “more unique” due to the complex technology that defines the domain compounded by our inability to understand a virtual environment. In fact, cyberspace is hard to understand, but if the discussion is focused at the operational level of war, we find that cyberspace operations are actually quite similar to those in other domains.

In *Analogies at War*, Yuen Foong Khong argues there are compelling cognitive reasons for using analogies to aid in comprehension. The danger is that the analogy process is subject to systematic biases that may lead

Major General Brett T. Williams, USAF, is Director, Operations, Deputy Chief of Staff for Operations, Plans, and Requirements, Headquarters U.S. Air Force. He previously served as the Director, Command, Control, Communications, and Computer Systems, U.S. Pacific Command.

to simplistic and mistaken interpretations. Selecting the best comparison and using a sound analytic framework can help overcome these pitfalls. Many in the defense community find space an effective analogy for cyber because both have a global dimension. At the operational level of war, however, the global nature of the two domains is the only, and arguably the least important, similarity, as there are technical solutions available to mitigate the warfighting limitations that arise from the lack of boundaries in cyberspace. On the other hand, the terrestrial domains share several key characteristics with cyberspace. The existence of these shared attributes suggests that the best analogy for understanding cyberspace operations is not space. Instead, we should use our experience in the terrestrial domains as the basis for advancing an understanding of cyber as a warfighting domain.

The first characteristic shared between cyberspace operations and terrestrial ones is in the area of effects. In cyberspace, the potential exists to achieve tactical, operational, and strategic effects with cyber alone. This is rarely, if ever, true in space. The second shared component is constant and direct human interaction with the cyber domain, which is absent in space. Domestic and international actors from the civilian, commercial, and governmental sectors routinely and directly influence DOD operations in cyberspace. Concurrently, those actors are vulnerable to the effects of military cyber operations. So just like the terrestrial domains, we must be concerned with issues such as fratricide, the role of noncombatants,

cyberspace to provide the JFC with the ability to make decisions, direct actions, and manage risk in cyber. This dynamic will never exist for space operations.

Given just this short list of similarities, it is clear that starting from scratch is not required. We should apply existing capstone doctrinal tenets regarding strategy, operational art, and C² relationships to cyberspace operations, and our analogy should be the terrestrial domains.

2. The JFC must have C² of cyberspace, just as he does of the terrestrial domains.

JFCs are charged with exercising C² over the terrestrial domains. The JFC should exercise the same level of C² over cyberspace. In the terrestrial domains, JFCs organize the battlespace and implement control measures. They sense the environment, develop plans, make decisions, and direct actions. They understand the operational characteristics of forces that operate in each domain and are charged with managing risk within the context of achieving mission objectives. The JFC has all of these responsibilities in the terrestrial domains, and he should have the same authority and accountability in cyberspace.

The major challenge in giving the JFC C² of cyberspace operations is the GIG structure. Its global nature has led to C² relationships that give all cyberspace authority to U.S. Strategic Command, U.S. Cyber Command (USCYBERCOM), and the military Services. This paradigm must change so there is a balance between global and regional responsibilities in cyber. Doctrine, policy, and resources must be

Cyberspace is a manmade domain, and with existing technology cyberspace can be altered so commanders can choose from a variety of C² options tailored to the mission objectives and forces assigned.

In an effort to capitalize on proven operational tenets, we should consider applying existing C² models to cyberspace operations. The goal is to provide the JFC with direct operational C² for theater-specific missions and at the same time allow for global execution of other missions. The Theater Special Operations Command (TSOC) construct does this and provides an excellent model for developing the Theater Cyber Operations Command (TCOC). The TCOC would provide the geographic combatant commander with cyber capabilities in much the same way that TSOCs deliver special operations capability today. The TCOC would be under the combatant command of the geographic combatant commander, and forces would be assigned or attached as appropriate.

On a daily basis, the TCOC would be responsible for providing, operating, and defending the regional cyberspace architecture and would be capable of planning and integrating full-spectrum cyberspace operations in support of contingency planning and crisis response. When required, the TCOC would accept additional forces and provide functional component command support to subordinate joint task forces. At the same time, the TCOC would respond to USCYBERCOM direction as the combatant command responsible for planning, synchronizing, and executing global cyber operations. In addition, there would be an administrative command relationship with USCYBERCOM for synchronization and standardization. Depending on future decisions, there may be a funding relationship between the TCOCs and USCYBERCOM. TCOCs could be established now with personnel already assigned to the theaters. The most challenging aspect of establishing TCOCs would be determining the C² relationship among the TCOC and Service components.

A final concern is that today's JFC is not adequately prepared to assume C² of cyberspace operations. Years of practical experience and military education have made joint commanders comfortable with and competent in employing joint forces. This is not yet the case for operations in cyberspace. As a result, JFCs tend to delegate responsibility for cyber to the communications, space, and

cyberspace is a manmade domain, and with existing technology cyberspace can be altered so commanders can choose from a variety of C² options tailored to the mission objectives and forces assigned

proportional use of force, and rules of engagement. The third key similarity is the degree of flexibility and responsiveness that exists in the cyber and terrestrial domains compared with space. In the terrestrial domains, warfighters can introduce new capabilities, tactics, techniques, and procedures much more quickly than in space, and in cyberspace, reaction time is exponentially faster than in any other domain. Finally, assuming we evolve cyber architecture as we should, the JFC can command and control (C²) cyberspace operations just as he does operations in the terrestrial domains. The capability exists to shape

directed to changing the GIG to provide the JFC unity of command and unity of effort for cyber operations. The commander must have visibility and authority over those components of cyberspace that are critical to mission success and must be able to assume cyber risk without passing that risk on to the rest of the GIG. The only way to achieve these objectives is to technically alter cyberspace to allow delineation of virtual joint operations areas (JOAs) and areas of interest (AOIs). The JFC must then be assigned cyber forces that provide the domain expertise necessary to integrate cyber operations with operations in the other domains.

intelligence career fields. These professionals play a key role in cyberspace operations, but the JFC is ultimately responsible for mission success, and with this responsibility comes the requirement for a thorough understanding of cyberspace operations.

3. *C² of cyberspace is the key enabler for exercising operational command and control.*

The exercise of C² is the JFC's primary contribution to the fight; C² is what the commander *does*. His ability to execute C² relies on his understanding of the complex technology that makes up his C² system of systems. Admiral Robert Willard coined the term *C² of C²* to describe the operational necessity of having command and control of the command and control architecture. If the JFC does not understand his C² systems, he cannot effectively control them—and control of the architecture is a basic requirement for exercising command and control.

The C² architecture can be thought of as having five components:

- sensors that deliver intelligence, surveillance, and reconnaissance
- telecommunications infrastructure consisting of wired and wireless links
- networks that organize and distribute information
- protection layer for identification, authorization, access control, and physical/virtual security
- knowledge management tools and decision aids that help organize and display information in ways that facilitate decisionmaking.

The commander's C² system is critical for mission success, so he must be responsible and accountable for its operation. Since most of the C² architecture lies within or is substantially enabled by cyberspace operations, the JFC must have C² of cyberspace if he is to have C² of C². Currently, the JFC has little authority over his C² architecture, particularly the components that are part of cyberspace. Defining the JFC's operating areas in cyberspace and establishing appropriate cyber C² structures are foundational requirements for C² of C².

4. *Defense is the main effort in cyber at the operational level of war.*

Cyber discussions in DOD tend to narrowly focus on computer network attack and computer network exploitation. Not enough attention is given to providing, operating, and defending the networks that define cyberspace. Attack and exploitation

Airmen are instructed on defending Air Force network cyberspace during basic training



U.S. Air Force (Robbin Cresswell)

get the most attention because they employ some of the most sensitive capabilities and require significant legal and operational considerations. However, it is the ability to provide, operate, and defend cyberspace that

for now, we must rely on a robust, diverse, defensible architecture that can absorb the strongest enemy assault and still allow the JFC to execute his operational C² mission

should be the JFC's top priority because these activities enable all other cyberspace operations. Providing and operating the networks are largely a Title 10 function executed by the Services and the Defense Information Systems Agency. The JFC requires a voice in the cyberspace Title 10 missions; but at the operational level of war, the JFC must devote his attention to computer network defense (CND). Because adversaries will attempt to position themselves within friendly cyberspace in preparation for follow-on actions in the physical domains, CND must be a daily priority for combatant commands.

Defense as the main effort is a key difference between cyber and the terrestrial domains. For example, the most effective way to gain and maintain air superiority is through offensive actions. Offensive counter-

air operations destroy the enemy's airplanes on the ground, deny him the use of airfields, blind him to our intentions, and degrade his ability to execute command and control. Offensive air operations provide friendly forces with the freedom to maneuver in the air, and they deny the same to the enemy.

This may someday be true for cyberspace, but we do not yet have the capability to gain and maintain cyber domain superiority through offensive actions. Attribution, access, authorities, approval processes, and capability are all limiting factors. For now, we must rely on a robust, diverse, defensible architecture that can absorb the strongest enemy assault and still allow the JFC to execute his operational C² mission.

Another reason defense requires priority is that in cyber, the offender enjoys some inherent advantages over the defender. For example, the offender is not disadvantaged by the concept of a culminating point. In land warfare, for instance, the attacker typically finds that the farther he penetrates defenses, the more difficult it is to sustain the attack. The attacker is on the move and expending resources, and his lines of communication become difficult to sustain and protect. If the defense is sufficiently strong, the attacker will culminate prior to achieving his objective. In cyberspace, the concept of a culminating point does not apply, and in fact, the offender may get stronger as he penetrates defenses. Consider the rapid spread of highly effective computer malware within a network. Once the malware is established in the

network, it can be difficult to detect and tends to become *more* dangerous as it spreads. The malware does not culminate; it must be tracked down and destroyed by the defenders.

Civilian, commercial, and governmental entities are daily victims of intrusion, exploitation, and low-level computer attack. Currently, this activity does not directly threaten U.S. national security, but it does demonstrate that potential. To some, it appears that defense is impossible, and this assumption leads to over-emphasis on the offensive mission. Offensive cyber capability will increase at a rapid pace, but for now, the JFC's critical requirement is an adaptive, dynamic defense that allows him to counter the attacks and continue to operate.

5. Cyber is the only manmade domain. We built it; we can change it. Creating a cyber JOA is the first requirement.

The single greatest barrier to giving the JFC C² for cyberspace operations is the open nature of the GIG. Cyberspace is a virtual world without boundaries, where a risk assumed by one is a risk assumed by all. In other words, it is all one big GIG. This is largely true, but it does not have to be. We have no control over the nature of the physical domains, so we develop forces, doctrine, and tactics acclimated to each. Using this model for cyber has been challenging because we have failed to take advantage of a key distinction between cyberspace and the physical domains: *we can change the structure of cyberspace*. If we change the domain to better accommodate operational mission requirements, we can more easily develop tools, tactics, techniques, and procedures that enable mission success. Enabling the equivalent of operational control measures in cyber is the first requirement.

According to joint doctrine, a JOA is an area defined by a geographic combatant commander in which a JFC conducts military operations to accomplish a specific mission. Geographic combatant commanders establish JOAs to delineate the JFC maneuver space and implement C² constructs that define authority, responsibility, and accountability. The cyber JOA is established for the same purpose. Most people cannot grasp the concept of a cyber JOA because they are stuck on the idea of drawing lines on a map. A JOA is not about the lines on a map; it is about establishing control measures. In the physical domains, this is done with lines on a map. In cyberspace, control measures are implemented by applying existing technologies in a way that allows implementation of control measures.

The cognitive barrier that must be overcome is that the cyber JOA cannot be defined by lines on a map. In all other respects, however, the cyber JOA is a parallel concept to a geographic JOA.

Most experts immediately dismiss the concept of a cyber JOA. Naysayers in the technical community typically do not understand the operational imperative for a cyber JOA and therefore do not envision engineering the GIG to facilitate it. Experts in the operational community cannot grasp how we could possibly implement control measures in cyberspace that mirror control measures routinely established in the terrestrial domains, which establish tiered authorities, define command relationships, and provide flexibility at the tactical, operational, and strategic levels. Control measures can be incorporated in cyberspace to accomplish the same objectives while preserving access to the wider GIG as required for mission execution.

The JFC cyber JOA is defined by those friendly systems and networks that the JFC relies on in order to execute C² of the joint force. At a minimum, the primary coalition C² network and associated applications are in the cyber JOA. The JFC should have operational control over the coalition C² network for the *provide, operate, and defend* missions. Using his command authority, the JFC decides where to extend the coalition C² network, who has access, what operations have priority on the network, and how best to defend the JOA. USCYBERCOM and the Services have significant responsibilities in these mission areas, and they provide support under the direction of the JFC. Other systems and networks could be in the JOA based on specific mission requirements. Examples include enclaves of

that they would be nested. For example, a geographic combatant commander may have a theater JOA within which are established one or more JTF cyber JOAs.

As opposed to a geographic JOA, which usually includes some enemy territory, adversary cyberspace lies primarily in the JFC area of interest. As defined by joint doctrine specifically, the AOI contains forces or other factors that could jeopardize friendly mission accomplishment. The nature of cyber warfare is such that the adversary can attack from anywhere in cyberspace to include the United States or even from within the DOD GIG. Therefore, it is impractical to include adversary cyberspace within the JFC cyber JOA, so enemy cyberspace is best defined using the concept of AOI. The JFC has a requirement for effects in his cyber AOI. By using the concept of AOI, it becomes easier to define the supporting-supported relationships that the JFC requires to generate effects in "red" cyberspace.

With mostly existing technology and infrastructure, we can create a cyber JOA. A set of controlled interfaces define the cyber JOA boundaries and make it possible for the JFC to sense the environment, make decisions, direct operations, and, most importantly, assume a risk posture that is different from the rest of the GIG. At the same time, the controlled interfaces allow and, in fact, require USCYBERCOM and the Services to execute their GIG-wide missions in substantially the same way they do now. Fully debating the technical feasibility of the cyber JOA concept is beyond the scope of this article; however, it is hard to imagine providing C² of cyberspace operations to the JFC without implementing something similar to a cyber JOA.

the JFC should have operational control over the coalition C² network for the provide, operate, and defend missions

U.S. classified and nonclassified networks, bilateral coalition networks, and networks that support other U.S. Government agencies. It is critical to understand that the cyber JOA boundaries do not mirror the geographic JOA boundaries. Some components of the physical architecture that define the cyber JOA will lie within the physical JOA, but significant portions will not. This is another critical distinction between the virtual and terrestrial application of the JOA concept. Optimally, cyber JOAs would not overlap, but it is likely

Failure to acknowledge the fact that cyber is a domain that we can change is a mistake. Accepting the one-big-GIG dilemma unnecessarily limits C² options and focuses command relationships at the national level. The operational requirements of the JFC must drive the design of cyberspace, and we cannot continue to let the current design of the GIG limit the JFC warfighting ability.

6. Cyberspace operations must be fully integrated with missions in the physical domains.

Early airpower advocates envisioned a day when attacks from the air would be so precise and effective that there would be little need for operations in any other domain to achieve mission success. Today, we can attack from the air with “pickle barrel” accuracy as predicted by the early airpower proponents. What has not been realized is the ability to achieve military victory with airpower alone. As with forces in the other domains, airpower is most effective when used in a combination of land, maritime, air, and space operations and in synchronization with the other instruments of national power. Cyberspace operations are no different. The ability to achieve effects in cyberspace will rapidly increase, but rarely should we rely solely on cyber. Attempting to achieve effects in any single domain limits the commander’s flexibility and agility, denies him the ability to present the enemy with a synchronized set of symmetric and asymmetric problems, and tends to create single points of failure.

Integrating cyber effects requires a complete understanding of cyberspace operations gained through experience and education as well as a clear delineation of command relationships and authorities. In the land, maritime, and air domains, the Services organize, train, and equip forces. At execution, the JFC typically assumes C² of terrestrial forces under operational or tactical control. This is not the case with cyber. USCYBERCOM and the Services currently retain command authority over cyberspace operations, and the JFC has limited directive authority as the supported commander. This dynamic must change. Without command authority, the JFC cannot integrate the full spectrum of cyberspace capabilities with operations in the other domains. The JFC can do this in the terrestrial domains, and there is no reason he should not be able to do the same in cyberspace. JFC authority over friendly systems and networks should be through a direct C² authority, and his ability to direct actions in the AOI is most appropriately handled via a supporting-supported relationship with USCYBERCOM. Effects in the AOI must be planned and executed in a sufficiently responsive manner if the JFC is going to integrate full-spectrum cyber operations with his operations in the terrestrial domains.

7. *The JFC must see and understand cyberspace to defend it—and he cannot defend it all.*

The JFC is responsible for defense of the cyber JOA, and he can only defend it if he can see it. The JFC needs complete situational awareness over his cyber JOA via a common operational picture that is integrated with the other domains. In addition, the JFC must have visibility on both “red” and “blue” components of cyber that exist outside his JOA but within his cyber AOI. It is important to note that significant portions of the infrastructure exist in the civilian and commercial sectors. Developing cyber situational awareness is a high priority for DOD. The challenge is providing a complete picture of the domain that is consistent, accurate, current, and customizable for commanders at all levels.

Gaining visibility and situational awareness in cyberspace is challenging, but it is even more challenging to understand the domain.

except for the most limited cyber attacks, we cannot with high confidence predict the full range of desirable and undesirable effects

The interactions are complex, responsibilities and authorities overlap, and our understanding of virtual operations is not well developed. A way to approach understanding the cyber domain as it applies to warfighting is to make sure cyberspace is part of the center of gravity analysis, which allows the JFC to identify critical capabilities, requirements, and vulnerabilities for cyber just as he does in the terrestrial domains. This work will help the JFC define the equivalent of key avenues of approach and key terrain to focus defensive efforts. If he does not do this, the JFC will find himself defending everything and in the end perhaps defending nothing. Consider our current operations on the nonclassified networks. Studies suggest that perhaps 20 percent of nonclassified network traffic is official business, and even less of it might be considered critical for mission success. Yet our defenses for the most part are equally distributed across the entire nonclassified infrastructure. We are effectively trying to defend everything. At both the global and regional levels, our defense must be prioritized to protect the most critical C² systems, and JFCs should have a significant role in defining those systems.

8. *Networks are critical and will always be vulnerable—disconnecting is not an option. We must fight through the attack.*

The U.S. military must be prepared to engage a variety of adversaries. Some are near-peer competitors with parity in equipment and technology. Others are nonstate actors who are not technological peers but who still pose a significant threat through insurgency and terrorism. The one advantage the United States currently enjoys against both groups is its ability to collect, analyze, and disseminate data in a way that gets the right information to the right decisionmaker in a format that allows accurate, timely decisionmaking. We do most of that work in cyberspace. There are those who argue that we should learn how to operate without cyber. That is simply not possible. We must acknowledge the fact that we will experience degraded cyber capability, but we cannot go back to semaphore and grease pencils. Our advantage depends on having freedom to operate in cyberspace—and that is a critical capability we must protect.

If networks are essential across the spectrum of conflict and defense is the main effort, how can the JFC guarantee the adversary never penetrates his cyber defenses? Unfortunately, no commander can create an impregnable cyber defense and still execute operational command and control. Thousands of years of warfare have taught us that for every new defensive capability, there will appear a credible offensive threat. Similarly, new offensive weapons have always given rise to an improved defense. This cycle is endless, and the only difference in cyberspace is the pace of technical evolution. Moves and countermoves in cyberspace are limited only by the time it takes for us to conceive a new idea. This means that no matter what we do to defend our networks, we will eventually find the adversary inside our perimeter.

Disconnecting from the GIG is the only way to keep the adversary out of our cyberspace. But *disconnecting is not an option*. This course of action would constitute a self-imposed denial of service that would deliver victory to the attacker. The JFC must have the capability to fight through the attack and continue to operate. Demonstrating that we can continue to operate in the face of the most determined adversary is an excellent form of deterrence that may result in the enemy looking for a different avenue than cyber to achieve his goals. Alternatively, the adversary may become so absorbed in conquering our cyber defenses that he expends energy and resources to the detriment of generating effects in the physical domains. In either case,

a robust, dynamic defense complicates the enemy's plan and sets the conditions for effective cyberspace operations.

9. Our understanding of nonkinetic effects in cyberspace is immature.

In the terrestrial domains, we model physical effects with high confidence. For example, if we drop a 500-pound bomb on a building, we can guarantee that it will hit the building in a specific spot. With high fidelity, we can predict structural damage, number of killed and wounded, and collateral damage. In cyberspace, our understanding of effects is much less mature. Except for the most limited cyber attacks, we cannot with high confidence predict the full range of desirable and undesirable effects. Moreover, while these effects occur in the virtual domain, their ultimate impact is real in the physical world. The fact that many of the undesired effects could significantly affect the civilian and commercial sectors makes it critical that we acknowledge our shortcomings in predicting nonkinetic cyber effects.

Estimating direct effects of an action is actually the easy part in both the physical and virtual domains. The real art comes

in predicting human reaction. Rarely will we conduct operations with the intent of demanding unconditional surrender. Instead, when we attack an adversary, our goal is to compel the enemy decisionmaker to change his behavior in a way favorable to us. We have been kinetically attacking each other for centuries, and we can predict human reaction to a kinetic attack with some confidence. Since there has yet to be a successful cyber attack that threatened a nation's core interests, we have little experience to rely on when we attack in cyberspace. Our estimate of the opposing leader's reaction will be imprecise, and the spectrum of possible reactions may be wide, especially if the attack threatens to collapse the financial system or degrade strategic level command and control. Predicting the leader's behavior will be further complicated because the targeted state will have difficulty assessing the full impact of a cyber attack. Cyberspace is complex, so figuring out what is happening in the middle of a crisis would be difficult and could introduce unnecessary urgency, even panic, into the targeted leader's decisionmaking process. By the way, we face the same situation in the United States. The

task of understanding effects becomes more difficult and more risky when "nonrational" actors with access to weapons of mass destruction are the target. By definition, irrational behavior is hard to predict, and cyber attacks have the potential to generate irrational responses from even the most rational leaders.

10. Understanding operational impact is the critical measure of cyberspace engagements.

If an adversary gains access to the JFC's cyberspace, the most important information for the commander is the operational impact of the intrusion. Unfortunately, operational impact is not always the focus of the staff. Frequently, the first area of attention is attribution. While attribution will eventually be relevant, especially if a counterattack is planned, the immediate effort should be to assess operational impact and appropriate countermeasures to stop the attack.

To determine operational impact, we must first understand that an attack has occurred, is in progress, or, preferably, is about to be launched. Then we must assess the impact or potential impact on our mission. The simplest attack to understand is one that completely and clearly disrupts a friendly



International forces prepare C⁴ systems for multinational operations during exercise Combined Endeavor in Grafenwoehr, Germany

U.S. Air Force (Jeremy Burns)

system. In this case, the attack is obvious, and determining operational impact and mitigating measures should be relatively easy. A more problematic attack is one that manipulates data such as position reports to a common operating picture or delivery details for a logistics movement. This type of attack is particularly troublesome because it may be difficult to detect and would likely cast doubt on the integrity of the entire system. The third type, data exploitation, is the most common. The tendency with this type of attack is for the staff to report the number of documents obtained or megabytes of data exfiltrated by the enemy. Without any operational assessment, these raw numbers are useless. The analysis needs to consider type of information captured, its relevance to the current operations, and the likelihood that the adversary can exploit the data within an operationally relevant decision cycle. Armed with this type of operational assessment, the JFC can make an appropriate risk assessment and determine the best mitigating course of action.

In these three representative cases, the JFC may determine that the cost of disconnecting from the GIG in order to expel the intruder may be more detrimental than fighting through the attack—the self-denial of service. In that case, he may accept the risk for at least a period of time. Or the JFC may decide to tolerate the intrusion in order to use the adversary access as a means to counter-attack. Another option may be to manipulate the intrusion to support friendly intelligence operations or military deception. In any event, the risk assessment belongs to the JFC, and he needs access to the right information and expertise to make the mission-risk decision. Again, the JFC requires a JOA in cyberspace so he can assume the level of risk necessary to meet his mission objectives without impacting the rest of the GIG. In the end, the JFC must be as comfortable assessing and assuming risk in the cyber domain as he is in the terrestrial domains. This will happen only with the right education, experience, and technical architecture.

Cyberspace is a collection of systems, networks, and software that nobody completely understands, yet we rely on it for our most critical national security missions. Because of this reliance, we have an urgent requirement for doctrine, policy, and resources that support cyberspace operations. Unfortunately, the complex nature of cyberspace has led some to believe that it is

such a unique warfighting domain that we cannot apply operational tenets that have proven successful in the land, maritime, and air domains. In fact, we can and we should. It is important to note that there is both a global and a regional aspect to cyberspace operations, and they are equally important. Currently, too little attention is paid to the vital role of geographic combatant commanders in cyberspace. These 10 propositions offer an analytic framework for approaching cyber from the perspective of the joint force commander as opposed to the business requirements of the DOD enterprise. Finally, accepting the limitations of “one big GIG” is shortsighted. Cyber is a manmade domain that should be shaped to align with the operational chain of command. In the end, this will all happen if joint force commanders take personal responsibility and accountability for command and control of cyberspace and demand the same unity of command in cyberspace that they have in the terrestrial domains. **JFQ**

NOTE

¹ I would like to acknowledge two other papers based on the 10 propositions construct. One is Major Jordon T. Cochran's thesis, *Ten Propositions Regarding Cyberpower*, presented to the faculty of the School of Advanced Air and Space Studies at Air University, Maxwell Air Force Base, in June 2008. The second is a working paper also entitled *Ten Propositions Regarding Cyberpower*, written by Dr. Kamal Jabbour and Colonel Fred Wieners, USAF (Ret.), dated April 11, 2010. I was not aware of either work when I originally wrote this article and with the exception of the title, there are no similarities between them and my work.

I had a lot of help thinking through these 10 propositions and would like to specifically acknowledge Colonel Daniel Baltrusaitis, USAF, and Colonel Harry Foster, USAF (Ret.), for their inputs.



NEW
from **NDU Press**

for the
Institute for National Strategic Studies

Strategic Forum 263

Conventional Prompt Global Strike: Strategic Asset or Unusable Liability?

As the world changes and threats evolve, has the time come for the United States to develop and deploy the so-called Conventional Prompt Global Strike (CPGS) capability? This is the basic question explored by M. Elaine Bunn and Vincent A. Manzo in this in-depth analysis. According to the CPGS concept, the United States would be able to deliver conventional strikes anywhere in the world in about 1 hour. After examining the pros and cons of CPGS, especially the potential for ambiguity and misinterpretation, the authors conclude that such a capability would be a valuable strategic asset. Although CPGS would not be the optimal strike option in all circumstances, it might provide the best available means for achieving U.S. objectives in some plausible, high-risk scenarios.



Strategic Forum 262

Small Nuclear Reactors for Military Installations: Capabilities, Costs, and Technological Implications

In recent years, the Department of Defense (DOD) has become increasingly interested in the possibilities of small (less than 300 megawatts) nuclear reactors for military use. This technology has the potential to solve two serious energy-related problems for the U.S. military: its dependence on the fragile civilian power grid and the vulnerability of fuel convoys supplying forward bases. Although the technology has a number of uncertainties and is still developing, Richard B. Andres and Hanna L. Breetz assess that DOD should consider taking a leadership role in this area. If DOD does *not* support the U.S. small reactor industry, it could be dominated by foreign countries, eroding U.S. commercial power capabilities and damaging U.S. control over nuclear energy proliferation.



Visit the NDU Press Web site
for more information on publications
at ndupress.ndu.edu

Cyber War

Issues in Attack and Defense

By ROBERT A. MILLER, DANIEL T. KUEHL,
and IRVING LACHOW

Dr. Robert A. Miller and Dr. Daniel T. Kuehl are Professors in the Information Resources Management College (College) at the National Defense University. Dr. Irving Lachow is a Principal Information Security Engineer at the MITRE Corporation.

Evidence of the magnitude of the changes brought by the information age is all around us. Networked computers link us together and control more and more of our infrastructures. By and large, this change has enabled significant increases in productivity and prosperity. Just-in-time operations have allowed us to streamline production, reduce warehoused inventory, and cut costs in many areas. Networked communications have slashed delays and improved our ability to control and predict all kinds of operations. It is difficult if not impossible to imagine life without ATMs, cell phones, or email, yet all of these are only a few decades old.

This is all good news, but it is mixed with new and worrisome problems. One of the major issues involves national security.

We are still struggling to come to grips with the impact of the information age on warfare. For most of the 20th century, war meant developing better ways to destroy the other side. Generally, this involved actual physical devastation (through what the military refers to as kinetic operations). However, the advent of computer networks,

and in particular their growing importance as command and control mechanisms, has significantly altered the traditional 20th-century battlespace.

The concept of cyber war has been in the news recently, with much commentary concerning what such a thing could look like, what its limits and limitations would be, what our national policies should be on the vexing questions of who should control American efforts in this area, and how the United States should respond to an attack on critical national infrastructures.

Experts in different fields are becoming increasingly worried about the risks of cyber war. To take one example, the flat bureaucratic prose of the following report does little to disguise the sense of concern:

The risk of a coordinated cyber, physical, or blended attack against the North American bulk [electric] power system has become more acute over the past 15 years as digital communicating equipment has introduced cyber vulnerability to the system, and resource optimization trends have allowed some inherent physical redundancy within the system to

be reduced. The specific concern with respect to these threats is the targeting of multiple key nodes on the system that, if damaged, destroyed, or interrupted in a coordinated fashion, could bring the system outside the protection provided by traditional planning and operating criteria. Such an attack would behave very differently than traditional risks to the system in that an intelligent attacker could mount an adaptive attack that would manipulate assets and potentially provide misleading information to system operators attempting to address the issue.¹

The U.S. military brings together its cyber activities under the umbrella term of *computer network operations*, which consists of three elements: defense, attack, and exploitation. *Computer network defense*, as its name suggests, focuses on keeping others from subverting our networks. *Computer network attack* is the obverse: breaking into the other side's networks and systems in order to create useful havoc—or, as the government puts it, to take actions that disrupt, deny, degrade, or destroy information.² Then there is *computer network exploitation*, a rather confusing term

Air Force technician performs preventive maintenance on base email servers at network operations and security center

U.S. Air Force (Rich McFadden)

that stands for taking actions that exploit data gathered from the other's systems and networks.

Obviously, there is a wavy and indeterminate line between exploiting and attacking, but the terms reflect a basic bureaucratic distinction: exploitation is the province of the Intelligence Community, especially the National Security Agency, while attack is the business of the military.³

Ten Assumptions

This article tries to go beyond these difficult issues and consider some operational problems in both cyber defense and cyber attack. The article starts with a simple set of 10 assumptions intended to spur debate and discussion:

1. Some sort of cyber war will be an inevitable component of most future military conflicts and future warfare.⁴ Cyber space is now and will remain a battlespace.

2. The shape of any future cyber war will be different in important ways from what we now confidently expect, but its primary targets will likely include civilian infrastruc-

tures as well as national security command and control. In this sense, the term *cyber war* is a misnomer, since computer-based attacks are merely one means to achieve the desired effect of crippling the other side's critical infrastructures.⁵ The true objective of such attacks will be to disrupt the adversary's civil society and inhibit its military action as a means of achieving the conflict's ultimate political objectives. So we are really talking about what could be called information and infrastructure war, or more precisely

exploitation is the province of the Intelligence Community, especially the National Security Agency, while attack is the business of the military

information and infrastructure operations (I²O), which we think is a more inclusive and therefore better term. The purpose of an I²O would be to disrupt, confuse, demoralize, distract, and ultimately diminish the capability of the other side. These are not weapons of

mass destruction, although they could have destructive secondary effects; they are more paralytic in nature—and are thus *weapons of both mass and precision disruption*.

3. Different adversaries will have different objectives and constraints. A major nation-state not only has many advantages in waging information war, but it also has a substantial stake in keeping its own systems and networks up and running. This need to prevent blowback damage may inhibit hostile actions. Nonstate actors (and, for that matter, smaller and poorer countries) have fewer capabilities but much less to lose. But all sides will realize that there are risks as well as benefits to cyber conflicts, and this fact *may* limit the scope of cyber operations—assuming (a large assumption indeed) that rational calculations of self-interest prevail.

4. Attribution problems are difficult to resolve and almost impossible to resolve quickly. This is important. Adroit attackers can find ways to disguise what they are doing, who is doing it, and how much they have done. *Planned confusion* may inhibit effective responses but will also tempt potential victims to preempt.

5. There is a significant first-mover advantage. In an I²O conflict, offense has a considerable edge over defense. Given sufficient time and opportunity, well-trained hacker units will often get through computer network defenses and may be able to inhibit counterstrikes. For this reason, both launch on warning and reflexive reactions (“use or lose”) can be expected, which may override the limitations mentioned above and lead to rapid escalation.

6. Even aside from the first-mover problem, uncontrolled escalation may take place. While in theory I²O conflicts can be carefully controlled, in practice it would be difficult to keep such operations within bounds because of the possibilities for intervention by so-called patriotic hackers—ordinary citizens and others who have the requisite technical knowledge—plus the difficulty in knowing what the other side’s capabilities really are, and also because of the attribution problem.

7. The likely confused nature of the cyber battlefields, unfortunately, may be a destabilizing rather than a stabilizing factor; victims who do not know where attacks are coming from, or what further attacks will follow, might be tempted to raise the stakes in any counteraction in order to deter more damaging second wave attacks.

8. There are many ways to prosecute an I²O conflict, and not all of them are limited to cyber attacks. Both classic information operations and physical attacks could and probably would play a role. The goals of attacks may include the denial of services, exfiltration of data, corruption of the

enemy’s information content, and, in some cases, infrastructure collapse.⁶

9. History offers some relevant examples of infrastructure-focused strategies in the pre-cyber period. Some of these infrastructures were functional, such as the entire British global supply chain attacked by German submarine warfare in both world wars. And some of the infrastructures were industrial, such as the German industrial web targeted by American strategic bombing in 1943–1945. However, analogies to previous periods and conflicts can be misleading. Cyberspace is now a battlespace, but it has its own characteristics. In particular, talk about dominating or controlling the cyber sphere is unhelpful, since the real touchstone of success is *effective use* rather than *physical control*.⁷ The former is possible, and the latter is probably not—which, of course, is exactly the way that the Air Force and Navy describe air and maritime superiority.

10. The cyber battlespace is rapidly changing. Both tactical and organizational agility will be necessary to achieve and maintain success.

*the real touchstone of success
is effective use rather than
physical control*

Approaches

One can imagine myriad ways that cyber attacks could be used to achieve national security objectives. However, most scenarios can be grouped into two major

variants: direct attacks and indirect attacks. Direct attacks would most likely involve the use of cyber capabilities in a blitzkrieg designed to gain strategic surprise and/or to produce effects that would impede the ability of the victim to take rapid and effective action. One could imagine this occurring via a large-scale distributed denial-of-service attack or by the activation of malware implanted across a large number of critical hosts in a target (or set of targets). This is the prototypical scenario often described when one considers how China might use cyber attacks to delay a U.S. response to a Taiwan crisis.⁸

But less straightforward actions are also possible. Such indirect attacks would be actions not easily recognizable either as “military” or as state-sponsored activities.⁹ The goal would be to create desired effects by using techniques that would not raise suspicions or cross the threshold into use of force or armed attack. For example, adversaries could conduct a series of attacks that appear to be classic cyber crimes directed at critical infrastructure (for example, the financial sector). Each attack would appear to be criminal activity and would fall under the purview of law enforcement organizations. However, a large number of such attacks over a long period could produce a sense of anxiety or instability in the target country, which could in turn have a strategic effect on the security posture of that nation. In some sense, such a series of attacks could be thought of as a type of blockade in that they would impede economic (and potentially military) activity that would weaken a country over time.

DOD (Cherie Cullen)



Deputy Secretary of Defense William J. Lynn III speaks at NATO North Atlantic Council cyber presentation in Brussels

U.S. Navy (Ryan G. Wilber)



Sailor sets up tactical data network on ruggedized laptops during command post exercise

Asymmetric Advantages

In many ways, I²O represents a classic example of an asymmetric opportunity. Compared to the cost of developing and maintaining robust and effective conventional or strategic forces, I²O capabilities cost relatively little in either money or skilled personnel. They are by definition stealthy. Mission-capable units can be created fairly quickly and often in secret. Capabilities can be masked or hidden before action is joined. And I²O can turn one of the main advantages of a conventionally armed force and highly developed society such as the United States into a disadvantage. During the past few decades, the developed world and its military forces have become increasingly dependent on a sophisticated array of networked services. If these were to become unreliable—even for a short time—the result might well be a decisive defeat, or at the very least partial paralysis.

Furthermore, it is a truism of cyber war that defense is much more expensive—in money, trained personnel, and effort—than attack. As attack vectors continue to multiply and network operations continue to become more complex, this gap will likely widen. That said, attackers and defenders alike face challenges in the realm of I²O. The following sections explore those challenges.

Problems for the Attacker. While the asymmetries of I²O clearly favor the attacker, the actual conduct of sophisticated operations is not easy. Here are just a few of the challenges facing those who wish to conduct such operations:

- **Target selection.** We live in an open world, and a surprising amount of information is readily available through open sources. However, selecting the profitable targets for I²O attacks and understanding the second- and third-order effects of targeted attacks will still require a long-term, systematic endeavor, and this intelligence-gathering and analysis effort will require the kinds of resources that only a nation-state or equivalent can provide.

- **Not fouling your own nest.** Attack vectors may have undesirable (and perhaps unforeseen) effects on the attackers' own networks, systems, and infrastructures. Therefore, attackers need to avoid collateral damage to critical infrastructures (notably including the Internet) that they need to preserve relatively undamaged for their own purposes, and steer clear of devastating the global assets that



U.S. Navy (Tyler J. Wilson)

Infrastructure cyber attack could disrupt ships' ability to pass through Panama Canal

will be useful after the conflict. This is not as easy as it sounds.

- **Not widening or deepening the conflict.** I²O wars are likely to have limited objectives (at least at first), and it will be important to control escalation and maintain exit strategies that allow for a comparatively peaceful postwar settlement. However, the difficulties noted above illustrate the challenges involved in escalation control. As Carl von Clausewitz noted, war has not only its own grammar but also its own logic, meaning that once it is initiated, it becomes a tiger that both sides may have difficulty taming.

- **Tying means (I²O) to ends** (what is “victory?”), avoiding “unlimited war,” and providing deescalation paths are all difficult problems, especially under wartime conditions.

Problems for the Defender. The difficulties facing the defense in an I²O situation are far greater than those confronting the attacker. As noted, cyber war offers significant asymmetric advantages to the attacker. To begin with, it is relatively cheap—certainly when compared to the cost and difficulty of developing significant conventional or strategic weapons. Second, it is fairly easy to ramp up one's activities without creating obvious signatures. The line between exploitation,

which many states and nonstate actors do routinely, and full-blooded attacks is often hazy and cannot be discerned until after damage is done. Even then, there is the attribution problem: attacks can be masked and attack routes can be muddled, so it is hard, even in retrospect, to determine who is doing what to whom, and attackers can expect to get away with plausible deniability for a considerable period. Attacks delivered at cyber speed give little or no time for human reaction, especially if such reactions involve several layers of decisionmaking.¹⁰ Furthermore, determining what has been damaged may pose significant problems. At first glance, this would seem to be relatively easy. If networks or infrastructures are taken down, and if services are denied or disrupted, the actions (if not the perpetrators) will soon be obvious. But this is not necessarily the case with attacks designed to change information content.

Choosing the Opponent's Bureaucracy.

As discussed above, separating the true beginning of an attack from the “noise” of constant exploitation and random hacker attacks and the like is difficult, especially if the attacker has taken prudent precautions to disguise his intentions and methods. One problem for defenders in the “indirect” attack scenario would be discerning between actual

cyber crime activity and apparent cyber crime activity that may in fact be part of a strategic campaign designed to achieve national goals. Determining the difference would require the extended melding of law enforcement information with intelligence information in a coordinated fashion and the ability to detect subtle patterns in a large dataset. This is quite a challenge both technically and organizationally.

It would also be difficult to determine how best to respond to such a campaign. First of all, there is likely to be much ambiguity in any attempt to ascertain the strategic goal of such an operation. Even if one can determine with some confidence that a given nation is behind a series of cyber crime activities, it may not be clear if the goal of those attacks is to steal information, gain intelligence, prepare for an attack, or cause harm in some other way. Secondly, there is the challenge of determining who should be in charge of any response. Cyber crime is clearly the domain of law enforcement. However, if a nation-state is attempting to cause harm to the United States, for example, the matter may come under the purview of several Federal agencies. And if the governing legal code under which events are occurring is the law of armed conflict—that is, if war is under way—

many actions that under peacetime law would be criminal would become the legitimate wartime acts of one belligerent state against another. In either case, it is likely that close coordination among law enforcement, homeland security, the Intelligence Community, and the military would be warranted.

On a related point, because of diverse jurisdictions in the United States and elsewhere, adversaries can determine, to some extent, which type of agency they wish to confront. For example, take the case of cyber-based attacks on the United States. If these attacks are launched from within U.S. borders (using proxy servers and other tools), the matter will fall to the Federal Bureau of Investigation. If they come from outside the United States, they will likely have to face off with the Department of Defense U.S. Cyber Command and/or the National Security Agency. In this way, the current structure of U.S. authorities allows adversaries some ability to both select their opponents and exploit the “virtual seams” between agencies.

Implications

If the assumptions and observations in this article are valid, they lead to a number of operational, policy, and legal implications, the most critical of which are discussed below.

First Strike, Preemption, and Deterrence.

The outcome of an I²O “war” may well be decided before the first shot is fired or airplane is launched. For this reason, preemption and deterrence are both important strategies for dealing with I²O threats. However, both of these strategies are difficult to implement in the cyber realm. Preemption depends on detecting early moves (or even intentions) and forestalling attacks by moving first (the equivalent of launch on warning). While kinetic attacks can easily be detected and there is seldom any doubt about their origins (especially if they are strategic in nature), neither of these realities applies to cyber attacks. A preemption strategy in the cyber domain is prone to misattribution of actors and intentions, overreactions, and miscalculations. The nature of cyber attacks, especially the convergence of attribution problems (which delay response) and the speed of execution (which makes instant decisions necessary), appears to limit the availability of preemptive strategies.

Similar challenges apply to a strategy of deterrence. Deterrence is based on either reducing the benefits or increasing the costs of attack so it is not launched in the first place. A key aspect of deterrence is creating a credible

“second-strike” capability that can survive an attack and allow retaliation and/or creating robust response capabilities that can mitigate potential damage so the gains from an attack are less than the risks to the attacker. This issue has been examined in detail by numerous scholars and government officials, so we will not go into specifics here other than to point out that deterring cyber attacks is a challenging proposition, and one should not assume that such a strategy will be successful.

On the other hand, the difficulties involved in deterrence and preemption (or any type of defense) may well increase the temptation for and urgency of early actions by a nation that believes it is under attack and needs to act while it still can—even if the precise parameters of who is doing what to whom and why are not yet fully understood. In other words, cyber operations are inherently destabilizing.

Resilience. The ability to withstand a cyber attack and continue operating is critical both as part of a deterrence strategy and if a deterrence strategy fails. This leads to the obvious conclusion that the development of a resilient and robust cyber infrastructure is necessary for any nation that is a potential cyber target. Resilience can be achieved in a number of ways, each of which has its own benefits and costs. For example, one approach is to rely on redundant capabilities, such as alternative sites, that can be turned to in an emergency. The benefit of this approach is that it can lead to high levels of resilience because one can, in theory, switch from one site to another with little interruption in service. However, there are several problems with this approach: because of their expense, redundant sites are necessarily limited in number, they are difficult to

*there is a significant
“first mover advantage”
for combatants in an I²O
campaign*

use appropriately in nonemergency situations (and therefore look wasteful), and they protect only a limited number of facilities and are almost impossible to field for entire critical infrastructures.

It is evident that a number of policy decisions will have to be made about the level of funding to spend on improving resilience and on prioritizing infrastructures that require attention. Making those decisions will involve



U.S. Army (Michael A. Simmons)

Rhode Island Air National Guard Network Warfare Squadron members monitor computer network for malicious activity during communications exercise

complex tradeoffs, but if these tradeoffs are not made and nations do not move forward with some improvements in resilience, they will be leaving themselves open to attacks that could cause great harm.

Public-Private Cooperation. Civilian infrastructures would likely be involved in an I²O war and would probably be the front line. Effective preparation for such a war would demand close cooperation between private sector infrastructure holders and the public sector. While there has been a great deal of attention focused on public-private information-sharing, certainly a necessary activity, insufficient attention has been paid to the government's role in strengthening the resilience of critical infrastructure/key resources (CI/KR) in the cyber domain. If our assumptions about I²O are correct, the creation of workable cyber response and resilience structures has become a strategic imperative for the Nation. The exact nature of these structures will need to be determined after careful consideration of technical, financial, and political factors. The list of options provided below is by no means exhaustive but gives a feel for the types of ideas that need to be examined:

- incentivizing CI/KR owners who invest in resilience-enhancing solutions
- penalizing CI/KR owners who fail to invest in resilience-enhancing solutions
- creating a Federal Emergency Management Agency–like capability for responding to cyber incidents
- leveraging Guard and Reserve units to augment private sector capabilities during cyber incidents
- determining whether existing laws appropriately balance civil liberties with the ability of the government to work cooperatively with the private sector in cases where national security is at stake.

To Not Decide Is to Decide

Some would argue that it is a mistake to weaponize the cyber realm and prepare for cyber war. If the United States had the only vote, this argument would carry a great deal of force. Unfortunately, others have votes as well. Weaponizing cyberspace is not necessarily, or even primarily, an American decision. Our only decision is whether or not to take the problem seriously enough to prepare for it. Time will tell if the assumptions and conclusions outlined above are correct, but one thing is clear: not taking the issue seri-

ously is a mistake. The United States needs to consider the implications of information and infrastructure operations and decide explicitly what it wishes to do about them. To not decide potentially allows others to decide for us. **JFQ**

NOTES

¹ North American Electric Reliability Corporation (NERC) and U.S. Department of Energy (DOE), *High-Impact, Low-Frequency Event Risk to the North American Bulk Power System* (Washington, DC: NERC/DOE, June 2010), 10, available at <www.nerc.com/files/HILF.pdf>.

² The official (unclassified) U.S. Government doctrine on computer network operations is found in Joint Publication 3–13, *Joint Doctrine for Information Operations* (Washington, DC: The Joint Staff, 2006), available at <www.dtic.mil/doctrine/new_pubs/jp3_13.pdf>. Recently, some of the individual Services have added formal doctrinal approaches as well: U.S. Air Force Doctrine Document 3–12, *Cyberspace Operations* (Washington, DC: Headquarters Department of the Air Force, July 2010), available at <www.epublishing.af.mil/shared/media/epubs/AFDD3-12.pdf>; U.S. Training and Doctrine Command Pamphlet 525–7–8, “Cyberspace Operations Concept Capability Plan 2016–2028,” February 2010; and the U.S. Marine Corps, “USMC Cyberspace Concept,” September 2009. Only the U.S. Navy has yet to publish a formal cyberspace doctrine, which should be coming soon.

³ Although there are obvious practical and legal differences between spying (computer network exploitation) and going to war (computer network attack), the issue of what differentiates computer network exploitation from computer network attack might not matter to the same extent to all nations or military forces. Nowhere in the literature on Chinese cyber war concepts, for example, does this issue seem to appear. But it does matter in the United States because of our unique legal and organizational structure. The capabilities and operations of U.S. forces are governed by the segment of U.S. law code known as Title 10, and congressional oversight of those forces and activities is conducted by the two Armed Services Committees, one in the Senate and the other in the House of Representatives. But the capabilities and operations of the Intelligence Community—the Central Intelligence Agency and National Security Agency, especially—are governed by Title 50 of the law code, and congressional oversight is conducted by the two Intelligence Oversight Committees. Thus, the three fundamental cyber activities shaping war and national security—attack, defense, and intelligence—are legally, organizationally, and operationally fragmented.

⁴ Furthermore, *information operations* will become an increasingly important part of foreign policy and operations other than war. However, the broader construct is beyond the scope of this article.

⁵ See Robert A. Miller and Daniel T. Kuehl, *Cyberspace and the “First Battle” in 21st-century War*, Defense Horizons 68 (Washington, DC: National Defense University [NDU] Press, September 2009), available at <www.ndu.edu/CTNSP/docUploaded/DH68.pdf>.

⁶ On this point, see Robert A. Miller and Irving Lachow, *Strategic Fragility: Infrastructure Protection and National Security in the Information Age*, Defense Horizons 59 (Washington, DC: NDU Press, January 2008), available at <www.ndu.edu/CTNSP/docUploaded/DH59.pdf>.

⁷ By *effective use* we mean the ability to use cyberspace to carry out meaningful I²O actions, maintain one's own command, control, communications, computers, intelligence, surveillance, and reconnaissance and logistics/mobility capabilities, and prevent others from denying the same.

⁸ For example, see James C. Mulvenon, “The PLA and Information Warfare,” in *The People's Liberation Army in the Information Age*, ed. James C. Mulvenon and Richard H. Yang (Santa Monica, CA: RAND, 1999), 175–186, available at <www.rand.org/content/dam/rand/pubs/conf/proceedings/CF145/CF145.chap9.pdf>. Also see Bryan Krekel, *Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation*, Report prepared for the U.S.–China Economic and Security Review Commission (McLean, VA: Northrop-Grumman, October 9, 2009), available at <www.uscc.gov/researchpapers/2009/NorthropGrumman_PRC_Cyber_Paper_FINAL_Approved%20Report_16Oct2009.pdf>.

⁹ This discussion of indirect attacks is partly based on Susan W. Brenner, *Cyberthreats: The Emerging Fault Lines of the Nation State* (Oxford: Oxford University Press, 2009).

¹⁰ This is a problem that the democracies' bureaucracies may have a particularly difficult time solving. If part of a coalition of democratic bureaucracies (for example, the North Atlantic Treaty Organization), this problem may become perniciously extended.

Digital Gunnery

IT'S ABOUT TIME

By JOHN A. MACDONALD
and MARTIN K. SCHLACTER

U.S., Japanese, and Korean naval officers discuss operational requirements aboard USS *George Washington* during exercise *Invincible Spirit*

U.S. Navy (Rachel N. Hatch)

The annual gunnery is complete, and we are feeling pretty good as a command. Ninety percent of the Bradleys and tanks qualified during first run—not bad, since we have been off them for a year while downrange. But are we really ready? How about the cyber domain? Is it qualified and certified like our Bradley/tank/F-16/AH-64/DDG crews?

In Combined Forces Command (CFC)/U.S. Forces Korea (USFK), we knew we had some issues when we did exercises, but we had no idea how complex, compounding, and confusing the issues were for stitching together a reliable and accurate common tactical picture

Major General John A. Macdonald, USA, is Assistant Chief of Staff, C3/J3, United Nations Command/Combined Forces Command (CFC)/U.S. Forces Korea (USFK). Lieutenant Colonel Martin K. Schlacter, USA, is Chief of Combined Data Network Operations for CFC and USFK.

for coalition and joint forces. The solution was the same one that has made us so successful in kinetic gunnery: basic skills, turret and gun system checks, electronics testing, and low-level tasks followed by platoon and company live fires. In the cyber-based world of common operating pictures (COPs), we've used that same approach—a deliberate and disciplined regimen of system checks, certification, and field exercises. We call it *Digital Gunnery*.

Cornerstone

Situational knowledge (that is, the next step beyond mere situational awareness) is one of the most critical advantages we have over an opposing force; it represents the foundational cornerstone of military decision-making. Sun Tzu's basic message of "know the enemy and know yourself" is augmented with specific guidance to use spies as a means to improve the commander's foreknowledge, which is one component of situational knowl-

edge that we strive to achieve with today's systems and processes.

Fast-forwarding over 2,000 years since Sun Tzu, military forces have continued the long march to improve the timeliness and accuracy of their common operating picture (COP), a lineage unbroken in today's COP and command and control (C²) systems. As the pace of technology continues to accelerate, the COP and C² systems that we field, while doctrinally distinct, become more interdependent. In our operational battle rhythm, we see this synergy clearly in the COP systems that enable the first half of John Boyd's OODA loop (observe and orient) and the C² systems that enable the second (decide and act).

Why So Difficult?

While modern COP systems function almost perfectly in tightly controlled and homogeneous/unilateral environments, their effectiveness dwindles rapidly in the face of

modern coalition/alliance warfare where different systems, messaging standards, security classifications, and languages or character sets are the norm, not the exception. The simple task of sharing information in coalition environments—whether in Afghanistan or the Republic of Korea (ROK)—is not so simple.

In today's national security environment, the heterogeneous environment of coalition/alliance warfare is so much a fact of life that it is an assumption in almost any national security discussion. Despite this reality, our COP systems (or at least the way in which most of them are implemented) have a decidedly U.S.-only feel, favoring direct database synchronization that is either proprietary or not releasable to foreign governments (the same coalition partners we are fighting with).

Hard Lessons

We found this out the hard way in Korea. Even if we momentarily set aside the broader interoperability issues with United Nations Command sending states, achieving comprehensive, accurate, and timely situational awareness is difficult—even in a bilateral U.S.–Republic of Korea environment. Each nation has its own COP and C² systems designed by different vendors to comply with different standards. In a cultural context, mirror-imaging leads to failures in the decisionmaking process. In a technological context, it leads to failed assumptions about interoperability.

Language and/or character sets pose hidden issues that are only exposed through routine bilateral or coalition use. While the effects quickly become obvious if data “fails to display,” it is far more difficult for system functions that are “hidden” from the average user, such as data exchange. Falling back to the lowest common denominator does not guarantee success, either. Has anyone ever seen a U.S. Message Text Format (USMTF) message written in Hangul, or a Korean Message Text Format message written in English?

Acquisition and life cycle sustainment philosophies vary significantly. Assuming that something can be fixed during the next “dot release” can quickly give way to the sobering realization that a 2- to 3-year funding and procurement process lies ahead. Most importantly, failing to test systems outside of simulation or command post environments naturally perpetuates assumptions on interoperability and operator proficiency—assumptions that tend to evaporate

under the harsh light of field exercises with real-world forces. If no one can remember the last time it was tested under field conditions, we are in for a surprise. As a result, without a deliberate effort to continually test the system, end-to-end, with real-world data, even the best COP systems are at risk of merely serving as a “cylinder of excellence” within their own national- or component-level stovepipes.

Digital Gunnery

The Digital Gunnery exercise program is the CFC/USFK response to this problem. The program was created in 2009 because of the sinking realization that our COP systems were not providing the accurate and timely situational awareness that U.S. and ROK leadership needed for operational planning. While we had

number of fielded forces. As a result, years of simulation data (while technically accurate) produced assumptions and a false sense of security about system interoperability under actual field conditions.

To address this, the Digital Gunnery program mandates two COP exercises per component per year (a total of 12 annual exercises) using actual data from fielded forces going through our real-world architecture. Prior planned component-level field exercises are used; we do not add extra events to the training calendar (we are busy enough). The data is real from end to end—nothing is simulated. For example, real-world Blue Force Tracker data are synchronized from the United States to South Korea, and Position Reporting Equipment data are synchronized

for the first time, ROK leadership can see U.S. Blue Force Tracker tracks in its COP—something that was considered impossible only 12 months ago

been using the COP for years, major theater exercises did not “load test” the real-world COP architecture—and in Korea, the exercise and real-world COP architectures are different.

For obvious reasons, we cannot field tens of thousands of soldiers, hundreds of jets, and equally as many ships in a major theater exercise without unintended second-order effects at a strategic level. Tension, escalation, and diplomatic reactions occur even in small exercises, let alone one with 10 times the

from South Korea to the United States—starting at the vehicle/tank level, then through the entire command, control, communications, computers, and intelligence architecture, and finally into the COP. The same goes for tracks from other systems that portray the friendly and enemy orders of battle.

For this to succeed, the Digital Gunnery program specifically focuses on ROK–U.S. interoperability, testing all data feeds in every format and ensuring that battlespace situational



Soldier enters mission data into Blue Force Tracker system aboard Light Armored Vehicle prior to patrol in Afghanistan

U.S. Air Force (Michele A. Desrochers)

awareness for one side of the alliance is the same as for the other. If different operational decisions are reached during the second half of the OODA loop (decide and act), at least we know it is not because of technical problems in the first half (observe and orient).

Successes

With over a year of experience in the Digital Gunnery program, the benefits have far exceeded expectations. Improvements to the COP are disproportionately higher than the amount of effort invested. For the first time, ROK leadership can see U.S. Blue Force Tracker tracks in its COP—something that was considered impossible only 12 months ago. Synchronizing friendly orders of battle for U.S. and ROK forces at all echelons is now a reality, 24/7, in both armistice and crisis, as well as for major theater exercises.

Interoperability has been greatly improved not just for track accuracy and latency, but also for accountability. For example, differences in how U.S. and ROK software designers interpreted Military Standard (MIL-STD) 6040 for USMTF messages previously forced all U.S. operational tracks into the ROK exercise database, increasing the risk of “data fratricide” with real-world implications. Through Digital Gunnery, that is no longer an issue.

Operator proficiency is greatly improved, with monthly opportunities for COP operators to group, filter, and display tracks along with corresponding overlays and amplifying

information. The quality and fidelity of data are also greatly improved, with brand new system patches developed just for Korea. For example, the Army’s Command Post of the Future system now supports Unit Identification Codes, and the Global Command and Control System (GCCS)—Army system now supports the ability to import MIL-STD 2525 combat effectiveness values from specially formatted (and USMTF-compliant) fields in S507 messages. For the joint community, GCCS-J now supports additional fields in its JUnit broadcasts—enhancing the fidelity of the order of battle exchanged not only between alliance partners and the United States, but also among U.S. systems themselves.

If all this sounds like “geek speak,” think about how a master gunner, fighter weapons instructor, or naval gunnery instructor speaks. To be digitally competent, we must understand all of this.

What’s Next?

As the Digital Gunnery program heads into its second year at CFC/USFK, we are now expanding its focus beyond its COP “roots” to include the integration of C² systems and data. For example, we all know that the presence of special operations forces (SOF) behind enemy lines generates fire support control measures and air control measures (for example, no-fire areas) to ensure our own forces are not inadvertently struck by friendly airpower or artillery. That is doctrine. But when was the last time outside of crisis or war that any of us actually

saw that process demonstrated, end-to-end, with real-world data?

Forcing everyone to “follow the electrons” across three components is an eye-opening process—from the SOF Joint Automated Deep Operations Coordination System (where the SOF order of battle is entered) to the Air Force Theater Battle Management Core Systems (where no-fire areas are established) to the Army Advanced Field Artillery Tactical Data System (where artillery fires are deconflicted with fire support control measures). Doing it across three components and two nations is even more eye-opening.

From Assuming to Proving

From improving the accuracy, timeliness, and reliability of the COP to optimizing the integration of our C² systems, the Digital Gunnery program is an ambitious concept that is long overdue. In fact, it serves as the missing link in joint and coalition doctrine for ensuring that friendly and enemy orders of battle (for all components) is 100 percent accurate for all alliance partners. It is the type of exercise program that we all talk about doing, but almost no one actually does it. If/when it is ever done, it is too late.

In the high-tech world of systems, no one deliberately tries to make COP and C² noninteroperable. Within each component or functional community, systems work as designed and as advertised. The unforgiving reality of coalition/alliance operations, however, cares less about rigid compliance with one nation’s standards, message specifications, languages, or character sets. What matters more are flexibility and a demonstrated commitment to make interoperability happen, especially if the underlying systems were designed for English-only operators in a U.S. joint environment.

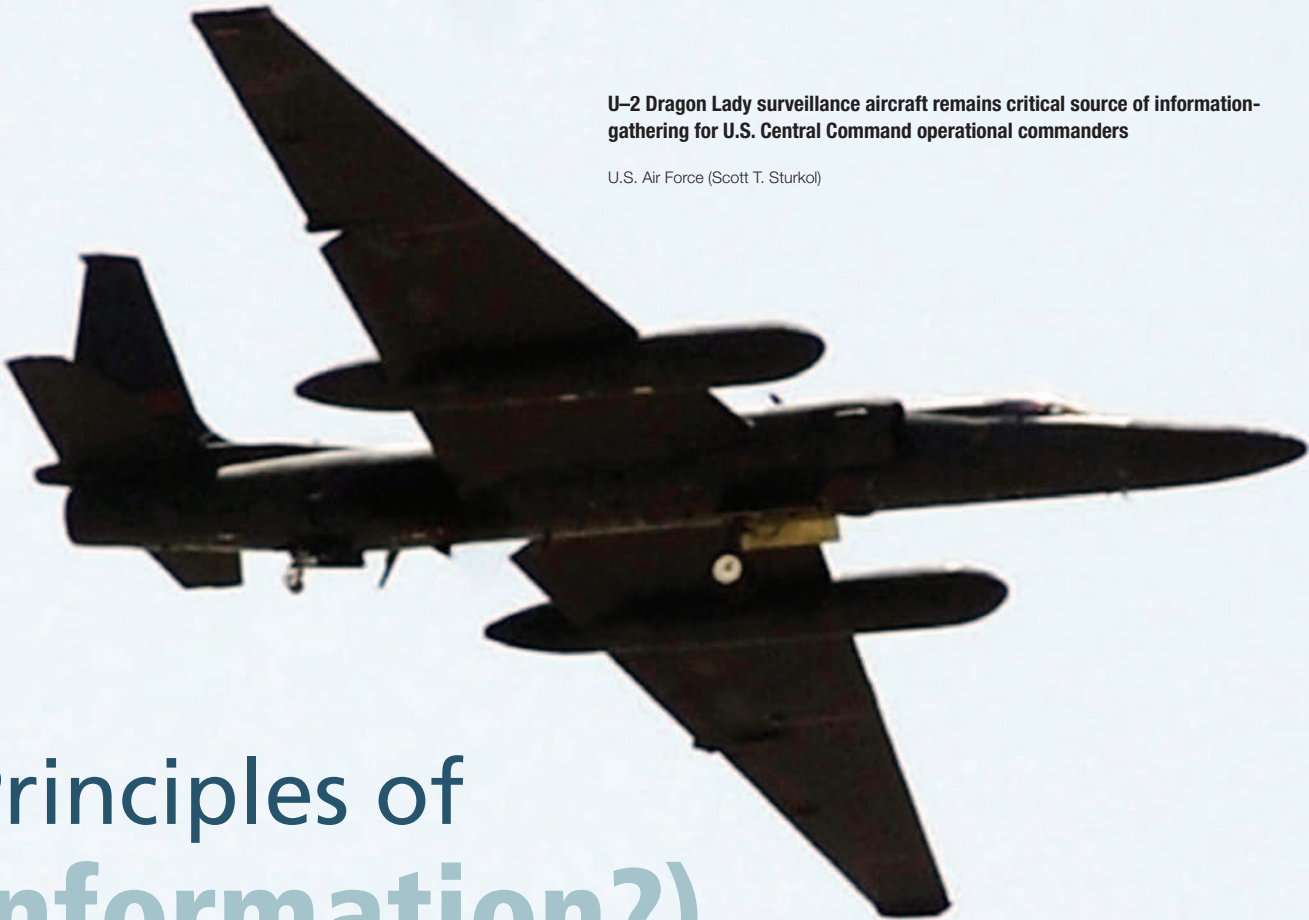
Simply put, a strong Digital Gunnery program changes our coalition COP and C² culture from one that is assumed to work to one that is proven to work. It has applicability anywhere coalition forces operate—from Korea to Afghanistan and beyond. Most importantly, it benefits everyone—from commanders at echelon, all the way down to fielded forces.

On the Korean Peninsula, as in Afghanistan and any area of responsibility where men and women serve in uniform, we simply can never have enough situational awareness or end-to-end command and control when people’s lives are at risk. **JFQ**

F-16s participate in U.S.–South Korean air force coalition flight over Kunsan Air Base



U.S. Air Force (Jason Wilkerson)



U-2 Dragon Lady surveillance aircraft remains critical source of information-gathering for U.S. Central Command operational commanders

U.S. Air Force (Scott T. Sturkol)

Principles of (Information?) War

Fortune favors the brave.

—Virgil, *The Aeneid*

By FRANCIS HSU

Francis Hsu is an independent researcher on strategic issues. His work centers on the impact of information technology on society. He served in the U.S. Army in Vietnam with the 1st Infantry Division and the Military Assistance Command–Vietnam Headquarters.

If God did not favor America, fortune certainly did. In the two-plus centuries since 1776, just as the forces of globalization, industrialization, technical innovations, democratic politics, and media propaganda spread worldwide, America moved onto center stage.

In history's most competitive environment, winning wars and maintaining leadership in peace, America orchestrated those forces better than anyone. But what next? Another force—the spread of information in all varieties—is changing the landscape. How will America respond? Will America still be favored?

In parks, towns, and cities all across the United States, weapons from past wars are displayed: armored personnel carriers, tanks, aircraft, and most often artillery pieces with cannon balls stacked in a pyramid pile close by. Despite the current wars in Southwest Asia, no one seriously considers putting these old weapons back into use. This is an advantage of hardware; it is physical and obeys natural laws. When it is obsolete, it is obvious.

At the onset of World War II, Major General John Kerr, the Army Chief of Cavalry, still wanted to ride horses into combat. Army Chief of Staff General George C. Marshall knew that would not do. Of his generation of Army officers, Marshall loved horses as much as anyone. He rode them often during the war as a form of exercise and relaxation. In short, he had nothing against riding horses, but he greatly opposed

cavalry charges against mechanized enemies. Horses and cavalry are also forms of hardware, though few would think of them as such. But they too are physical and obey natural laws.

It is much more difficult to determine the value of “software”—strategy, operational art, tactics, doctrine, and principles of war—than of hardware. One reason is because such information-based assets are intangible and presumably never wear out. For example, “surprise” was useful in past wars, and it is difficult to imagine a future when it will not be useful. However, not all software is of equal value. It is time to reconsider which software is vital and why.

Consider the principles of war as listed in U.S. Army Field Manual 3-0, *Operations*:¹

- economy of force: allocate minimum essential combat power to secondary efforts
- maneuver: place the enemy in a position of disadvantage through the flexible application of combat power
- mass: concentrate combat power at the decisive place and time
- objective: direct every military operation toward a clearly defined, decisive, and attainable objective
- offensive: seize, retain, and exploit the initiative
- security: never permit the enemy to acquire an unexpected advantage
- simplicity: prepare clear, uncomplicated plans and clear, concise orders to ensure thorough understanding
- surprise: strike the enemy at a time, at a place, or in a manner for which he is unprepared
- unity of command: for every objective, ensure unity of effort under one responsible commander.

Wars Ignore Boundaries

These nine principles reflect a strong streak of American experience: war as capital-intensive industrial machinery for getting from A to Z. Except for the principles of simplicity, surprise, and unity of command, there is little hint that people are involved. Machines do simple things, but they do not command, lead, or manage thousands of items (people, processes, and devices) with *simplicity*. We know machines cannot impose or be affected by *surprise*; neither can they practice *unity of command*. There is no doubt, however, that machines can enact all the other principles, perhaps even flawlessly. Consider this in

contrast to the opening paragraph of Sun Tzu’s *Art of War*: “War is a matter of vital importance to the State; the province of life or death; the road to survival or ruin. It is mandatory that it be thoroughly studied.”² No equivocation here—life or death, survival or ruin.

The next paragraph is the clincher. Sun Tzu identifies the inherent property of all wars: *they involve morality*—that is, wars are *human* problems. This, of course, means the perception of the *just* is vitally important—no obfuscation there. He continues with four other factors: weather, terrain, command, and doctrine. He explains the command factor

humans operate in the world of the physical, in which everything must obey natural laws, and in the world of data, in which natural laws do not apply

thus: “By command I mean the general’s qualities of wisdom, sincerity, humanity, courage and strictness.”³ Again, the emphasis is on *human-ness* in war.

The nine principles of war as enunciated clearly lack coverage in important areas of war. So what is missing? The wider scope is quite simple: humans operate in two vastly different domains. First, there is the world of the physical (hardware), in which everything must obey natural laws; and second, there is the world of data (software), in which natural laws do not apply. Since these domains are different, how we use resources in either or both of them determines the outcome of production and destruction in society. Without this wider scope, information warfare, information operations, and cyber war are impossible to understand, much less execute, with any chance of success.

Foundation Laying

In the physical domain, Colonel John Boyd explicitly tied fighter aircraft tactics to war principles. That is, he recognized how important it was to exploit the energy-mass transformations occurring during fighter combat: fighter pilots, like gladiators, must know natural laws or face the consequences. In the principles of war, *mass* means to “concentrate combat power at the decisive place and time.” Boyd’s tactical maneuvers certainly do that. But Boyd loved dialectics and dual-use-ism; to him, the term also means how the *physical mass* of the aircraft gains and loses energy potential during maneuvering. *Mass* embodies the concepts of both *concentration* and *energy potential*.

Boyd’s analysis is important for two reasons: air combat (in air-to-ground, ground-to-air, and air-to-air modes) extended war into the third dimension for the first time in history; and despite its novelty, air combat—in its air-to-air mode—shows in a clean, simple form exactly how natural laws shape what is possible to do and how to win or lose.

What Boyd managed to do was to ground the mechanical maneuvering of aircraft in precise patterns to determine winners and losers. What Carl von Clausewitz identified as *friction* for ground combat, Boyd did for air combat. But Boyd had several advantages

over Clausewitz. Being ground-based, Clausewitz had to deal with the thousands of moving parts of armies: individual soldiers, units, commanders’ quirks, soldiers’ equipment, large cannons, bridges, mud, chokepoints, missed communications, and wrongly interpreted commands. No wonder he had to invent the concept of friction to describe what can throw an army off course. It is not for nothing that an aphorism such as “for want of a nail, the battle was lost” came to be.

Being air-based, Boyd had to deal with only two objects: the dueling fighters. The physics of motion were well understood. He had equations to describe how potential and kinetic energies were gained and lost as the fighters maneuvered in Earth’s gravity. Boyd understood air combat physically because he *felt* it in flight during the Korean War. But he was not satisfied with that. He learned physics from entropy and beyond to know *intellectually* why what he felt was the correct way to act. In this way, he was one of the few true scientists of war. Boyd confirms for us that even in the most modern form of warfare, air combat, the laws of nature *must* be obeyed.

Boyd’s contribution was the end point of the trajectory of the American way of war: philosophically mechanistic, industrial, and capital-intensive. Both West Point and Annapolis were started as *engineering* schools. So technical competence, while initially not always highly prized, was the bedrock of their founding. When the Industrial Revolution that started in England jumped across the Atlantic, America was eagerly receptive

to the new technologies: steam engines, steel-making, railroads, mass-produced interchangeable parts, the telegraph. These formed the beginning of the American trajectory to greatness. Late in the 19th century, even as Kaiser Wilhelm's Germany built battleships to compete with British battleships, America seemingly kept a low profile. But even then, the great steel, railroad, and oil industries were spreading across the continent. By the early 20th century, Henry Ford perfected mass mechanization. It barely helped in World War I, but it would prove to be the ultimate arbiter of victory in World War II.

mass-produced automobiles, telephone, radio, road networks, air transport, radar, and other innovations in the early 20th century.

This transformation was purely practical: that which survived was deemed good and worthy. However, it leaves a large gap—that which is unknown or outside of one's experience. And with technological innovation, there is always a huge void in which *no one* has any experience. In this transforming tsunami, the principles of war found a home. After all, the principles were about a practical matter: how to win. And in no practice can natural laws be violated.

Natural laws constrain humans physically just as they do animals. However, once we started thinking and acquiring technology, that huge space called the unknown became the beachhead with an infinite horizon.

As our thinking and technology expanded into the unknown, it also enlarged our physical reach. The spear, slingshot, and bow and arrow expanded the range of what an individual could strike. By increasing striking distance, it also provided some safety—at least until the victim learned to strike back.

Technology was not the only scale that was expanding. Local populations that were

Air-to-air combat clearly shows how natural laws shape what is possible and how to win or lose



U.S. Air Force (James L. Harper, Jr.)

Mobilizing for War

With perspective, we can see how all the tides of history rose to become the American tsunami: the shelter of two oceans, unfettered capitalism, labor mobility, valuing individuals, abundant resources, entrepreneurship, technological innovation, and minimal public oversight. In such an unconstrained, free-for-all environment, everything—people, ideas, institutions, or technologies—seemingly had a chance to succeed. Such turmoil did destroy as much as it created. But that which it created and which survived transformed society: the railroad and telegraph in the 19th century;

Winning or losing, as the animal kingdom shows, is a physical matter. The outcome is bounded by scale, agility, strength, timing, chance, and the unknown. Since World War II, scientists have documented animals' ability to coordinate group actions. Whereas we once marveled at how ants and bees managed their colonies, we now know about the group actions of dolphins, killer whales, hyenas, lions, penguins, and many other species. Their group actions are all physical. They are always immediate in space and time. The energy expended is muscle. Little or no thinking or technology is involved.

once isolated from others began growing, destined to eventually bump up against strangers and often enemies. Though uneven, the expansion of population and technology ensures that clashes will occur. What defines these clashes? How can we identify where they might occur? While this short article cannot list all such possibilities, one is clearly identifiable: the FEBA.

A Boundary Defined . . .

FEBA is an old Army term for *forward edge of the battle area*. Prior to the Vietnam War, FEBA lines clearly separated friends from foes on battle maps. The term seems to

have faded from use in U.S. war experiences since Vietnam and guerrilla wars in general. The clarity that the term provides for today's conflicts is much less certain.

Let us dissect FEBA: *area* asserts that this is about land or geography of undetermined shape or size. *Battle* identifies this as a dangerous and contested space. *Edge* says only part of this area is designated. And *forward* further restricts this area. FEBA has never been defined as 100 meters, 3.5 kilometers, or 10,000 kilometers deep. The size of a FEBA correlates with its significance. A FEBA between two enemy squads or platoons is important to the members but is not likely to determine the outcome of a war. By contrast, the Battle of

of simplicity: TFs 16–17 were hiding (security) at Point Luck, massed to pounce (offensive) on IAF. TFs 16–17 also applied the economy of force principle. Nimitz's force had much better unity of command than Nagumo's and than Admiral Isoroku Yamamoto's, which was about 1,000 kilometers behind Nagumo at the start of the battle.

Admiral Yamamoto's Midway operation was flawed from the start in several respects. First, his plan was complex; it scattered his many fleets across millions of square kilometers in the northern Pacific. Given the technologies available to him, this violation of the simplicity principle destroyed his unity of command; his forces were scattered from the Aleutian Islands

over there; and second, the United States could transport its forces over there. The latter power converged with the former situation to keep America untouched for most of its history.

This is America's "managerial style of war." We do not take scalps or count enemies killed (with the exception of the Vietnam War), enemy territory taken, capitals occupied, or treasures confiscated. Instead, we measure people moved, tons shipped, distance traversed, ammunition expended, and meals served. Note how *every single metric* measures some physical, concrete thing governed by natural laws.

These were what America applied the principles of war on: economy of force, maneuver, mass, objective, offensive, and



U.S. Air Force

F-117A stealth fighter bomber's ability to elude radar detection embodied principle of surprise in Operation Desert Storm

Kursk (July–August 1943) between the German and Soviet armies occupied a frontage of a few hundred kilometers and occupied tens of thousands of square kilometers. As large as that was, it still does not compare with the Battle of Midway (June 1942), when the U.S. Navy sank four aircraft carriers of the Imperial Japanese Navy. In 4 days of maneuvering, that FEBA easily occupied several hundred thousand square kilometers of ground space, not counting the 4,000 to 5,000 meters of vertical space where aircraft flew.

The larger the FEBA, the more easily we can identify which principles of war played a role in its outcome. Doubtless, Vice Admiral Chuichi Nagumo's First Air Fleet (IAF) was surprised to find Rear Admiral Frank Fletcher's Task Forces (TFs) 16–17 on its left flank on the morning of June 4, 1942. That surprise reflected Admiral Chester Nimitz's maneuver to put TFs 16–17 at Point Luck about 600 kilometers northeast of Midway, waiting for Nagumo. Nimitz's maneuver was the essence

understanding FEBA goes a long way toward understanding how America prefers to fight its wars: far away and over there

in the northeast to Saipan in the southwest—a distance of 5,946 kilometers. Five other principles—economy of force, maneuver, mass, objective, and offensive—fell into disarray in one fell swoop. For how could such scattered forces maneuver economically to mass to a single objective offensively? They could not. Second, though unknown to him, Yamamoto's element of surprise and security were gone when Commander Joseph Rochefort⁴ broke the code that revealed his plan. Third, Nagumo was assigned two objectives: support the Midway invasion force, and sink whatever forces the U.S. Navy sent to intercept him. This was a dilemma that confounded Nagumo. And finally, Yamamoto let his emotions dictate his strategy. Like all samurai warriors, Yamamoto was proud to protect his Emperor. The Doolittle raid on Tokyo, while causing negligible damage, mortified army and navy alike, and Yamamoto's Midway plan got prompt approval.⁵ That is, the Doolittle raid determined that the Battle of Midway would take place.

Leverage Lost

Understanding FEBA goes a long way toward understanding how America prefers to fight its wars: far away and over there. This, of course, is exactly the type of fortune that no one in the old world of Africa, Asia, and Europe had. For them, it was literally everything and *their* kitchen sink. For them, the margins of error had greater consequences.

America's fortune of fighting over there was based on two facts: first, the conflict was

others. These played to the strengths of America: trucks, ships, aircraft, infrastructure, and organizational and managerial abilities to get from A to Z.

The American century was a triumph of both war and peace. America reached that pinnacle not only because it could destroy better but, more importantly, because it produced better. America did not willfully set out to dominate the world. It managed to do so by understanding and exploiting nature's bounties to produce for society at peace, knowledge that was easily channeled to produce for war. This was *dual-use* long before the term was coined.

The most apt phrase is *force multiplier*: we used science and technology for global leverage before anyone else did. This type of global historical leadership is, by definition, a passing phenomenon. When the Boeing 747 began flying in 1970, it democratized air travel to such an extent that it reshaped our image of the world. After its debut, even the other side of the world was only half a day away. One did not have to be an American to fly the plane—one had only to pay the fare and go. Then, Intel microprocessors democratized computing power and fiber optics; the Internet democratized communications; microchips made cell phones so cheap that even the poor could afford high-tech products. The world landscape is changing. What once enabled America to fight over *there* can now be reversed by adversaries to bring the fight over *here*. What was once far away and difficult to reach can now be reached much

more cheaply and easily. What was once the purview of the wealthy and powerful is now commonplace.

The 9/11 Commission recognized a dangerous truth: al Qaeda spent about \$500,000 and 2 years to plan and execute its attacks.⁶ America has spent many billions of dollars for almost 10 years to defend itself. This cost ratio of attack versus defense cannot be sustained no matter how wealthy a society is. This form of asymmetry is well understood by al Qaeda and its followers worldwide. Their recent announcement on their Web site confirms they know how to exploit this imbalance to our detriment.⁷

So the cost equations of war shifted hugely in favor of the attack over the defense. Merely throwing money (or capital) at the problem cannot solve it. We need to rethink the basis of strategy: the principles of war practiced in the past. This will be tough, disruptive, and unsettling for strategists everywhere. Get used to it; we either do it voluntarily, or because we are *forced* to (like after 9/11).

Washington's recent creation of the U.S. Cyber Command makes clear that a whole new domain of warfare has opened up. From what is publicly available, no doctrine, theory, or principles have yet been established to govern this domain.

In the past 500 years, the West extended its reach globally both physically, with hardware, and intellectually, with software. This two-front attack devastated the world (including huge parts of the European West itself). What the hardware conquests could not do, the software did do. America entered the last half of this period mastering those forces to dominate a world still uncomfortable with Western ideas, values, and technologies. This forceful impact on "the Rest," as the non-West has been called, has at least been absorbed by many Asian and South American nations. They have taken the blows and are now readjusting themselves to this new world. Today, whether the Rest like it or not, the West's hardware has flooded the world. They drink Coke, eat fast food, talk on cell phones, compute on Wintel machines, surf the Internet, and fly in Boeing and Airbus aircraft. By and large, they do not complain about using these riches of a consumer society.

But resistance remains to Western and, in particular, American "software" of the cultural kind—ideals, values, and practices. In this domain, the fight continues. The lack of clear boundaries is a plus for the defenders: they can fight back without needing to

build and maintain an expensive industrial infrastructure. Recent cyber attacks show how this is being done. The principles of war that served the United States so well during the American century are showing their age. A retooling is overdue.

History does not sleep. Time keeps moving on. During the American century, we saw how specialized capabilities available only to the few enabled the West to dominate the world. What globalization has done is to generalize those capabilities and make them cheaply available anywhere to anyone. This has upended some of the principles of war. What the FEBA defined with such clarity has again been blurred. The easy distinction of "war" and "peace" has itself been called into question. Since 9/11, the U.S. Government has maintained that we are at war. Yes, but as a society, America is not fully mobilized for these wars. And more to the point, globalized trade and development—the historical signs of peace—have not abated. Kipling's "savage wars of peace" are more apt than ever.

... a Boundary Globalized

The fortunes that favored America are historically unique. Vast untamed lands, rich resources, industrialization, democracy, markets, innovations, and isolation from the old world combined as an incubator for a new and different type of society. Through both war and peace, America spread the fruits of its production worldwide. In applying the principles of war through much of that time, America exploited nearly all of the physical endowments that Nature provided. That era is now over; those tangible physical means are now the norm worldwide, thanks in no small part to American proselytizing.

In creating this new environment, what once worked for America now works for anyone. That competitive edge that America developed is now a commodity. The famous dictum that "amateurs talk strategy, professionals talk logistics" is now false. Today, logistics management is an outsourced service that private companies such as Federal Express and UPS do expertly. Do not misunderstand: logistics remains a complex and difficult task, but as 9/11 and information warfare show, moving tangible things is no longer a prerequisite to having a huge impact. In fact, it can be argued that having a big "boots on the ground" footprint is a liability. Dollar for dollar, life for life, our strategic efforts in Iraq and Afghanistan are costing

America much more than it is costing al Qaeda and Muslim extremists. Such strategic imbalance is imprudent.

The Greeks leveraged the triremes to good effect for generations. The Romans leveraged the legion to dominate for centuries. The British leveraged their fleets for almost 200 years. The American century seems to be peaking already. The American experience—and ours—is different in this respect. The Romans did not supplant the Greeks because they built better triremes. The Barbarians did not supplant the Romans because they made better legions. The Americans did not supplant the British *merely* because of better fleets, though America surely had them. America is being supplanted by tools and methods that it provided. But more importantly, those tools and methods no longer impart dominance to their employers. The situations in the Korean Peninsula, Afghanistan, Iraq, Iran, and elsewhere testify to the impotence of nuclear-armed nations to tame primitive tribalism.

There has been a tectonic shift in the nature of strategies because controlling *physical* means confers less advantage than in the recent past. Whatever new *abstract* means exist are not yet known or ready to be used. The urgency is real.

What now? What next? Are the nine principles of war still relevant? Can they be retooled for the 21st century? Or do new principles need to be discovered? Who will fortune favor next? **JFQ**

NOTES

¹ Field Manual 3–0, *Operations* (Washington, DC: Headquarters Department of the Army, June 2001), 4–11.

² Sun Tzu, *The Art of War*, trans. Samuel B. Griffith (Oxford: Oxford University Press, 1963), 63.

³ *Ibid.*, 65.

⁴ Frederick D. Parker, *A Priceless Advantage: U.S. Navy Communications Intelligence and the Battles of Coral Sea, Midway, and the Aleutian Islands*, Series IV, World War II, Vol. 5 (Washington, DC: National Security Agency, 1993), 53.

⁵ Matsuo Fuchida and Okumiya Masatake, *Midway: The Battle That Doomed Japan, The Japanese Navy's Story* (Annapolis, MD: U.S. Naval Institute Press, 1955), 71.

⁶ *The 9/11 Commission Report* (Washington, DC: U.S. Government Printing Office, 2002), 172, available at <www.9-11commission.gov/report/911Report.pdf>.

⁷ Scott Shane, "Qaeda Branch Aimed for Broad Damage at Low Cost," *The New York Times*, November 21, 2010, A16.

Institutionalizing Economic Analysis
in the U.S. Military

The Basis for Preventive Defense

By CARL J. SCHRAMM

Carl J. Schramm is President and Chief Executive Officer
of the Ewing Marion Kauffman Foundation.



Development agencies must approach efforts through eyes of local
entrepreneurs, such as these vendors in Kabul, Afghanistan

U.S. Army (Teddy Wade)

The United States has reached the point of exhaustion in rebuilding war-torn countries. At the same time the country downgraded operations in Iraq from combat to advisory status in 2010, the effort in Afghanistan escalated on both the kinetic and nonkinetic fronts. Despite the strategy review undertaken by the Obama administration last December and promises that the July 11, 2011, timeline is really just a marker for assessment, there is a growing sense among policymakers and the public that the United States should get out of the nation-building business.

Such sentiment is perfectly understandable; we have heard over and over the refrain that the United States should not engage in economy-building in places such as Afghanistan when we cannot even get our own economy in order. Concerns over government debt also complicate matters. With debt posing a threat to American economic health, can we really afford to keep spending money on trying to jumpstart overseas economies? This is an especially serious argument in light of the coming struggles over how to reduce the Federal deficit—defense spending has already become a target because it is the largest discretionary item in the budget. In this light, moreover, the current balance of reconstruction resource allocation—tilted as it is toward democracy promotion—should come under increased scrutiny and opportunity cost analysis.

Paradoxically, however, and perhaps somewhat disappointingly to many observers, this is precisely the moment at which the United States, particularly the military, needs to engage in deep thinking about its approach to postconflict economic reconstruction. In particular, the military should establish a new institution, independent of political and budgetary cycles, for economic analysis related to national security and strategy.

For one thing, in the immediate future, the United States still has operational room in Afghanistan and even Iraq to make a difference in those countries' emerging economic trajectories. After nearly a decade in Afghanistan, economic development has come to be seen as integral to any notion of sustainable success. It now appears as if the United States will maintain some level of force presence in Afghanistan for the next several years—which means the U.S. military will continue to engage in economic reconstruction even

as civilian agencies take on a greater share of this activity.

On a longer time horizon, however, we should fully expect that the United States and its military forces will engage in economic reconstruction again and again, notwithstanding the present level of weariness and calls for the military to pull back to its core function: warfighting. Reports on the future operating environment and emergent threats facing the United States and its allies—such as the *Joint Operating Environment 2010* and the 2008 National Intelligence Council

simply a matter of a dearth of monetary and intellectual resources.

Instead, part of the problem is that the U.S. military has been asked, and will again be asked, to play a leading role in economy-building, whether by default or express designation. Yet in matters related to economic development, the military has had to defer to the expertise of its partner agencies and contractors. To some extent, this is understandable. The military has little economic expertise of its own and, moreover, is expected to fall in step with the mantra of interagency

at the core of Expeditionary Economics is the idea that the people of any given country must own the economy

report *Global Trends 2025*—make clear that economic growth across the world is never far from considerations of national security and strategy.¹ Whether the topic is intensifying nation-state rivalry, resource competition, or failing states, economic growth must be seen as central to how we think about defense. Consider, for example, a scenario in which North Korea collapses. There will clearly be an economic dimension to the ensuing turmoil, whether or not there is actual combat. Over the past decade, economic reconstruction has come to be seen by some as merely a part of counterinsurgency, but the North Korean economy would be a leading area of concern for the United States and other countries in the event of utter collapse or even conventional warfare.

The Need

The proverbial observation is that the three Ds—defense, diplomacy, development—comprise the three-legged stool of foreign policy but that development has consistently been the short leg. This imbalance is sometimes ascribed to fewer resources allocated to civilian development. Secretary of Defense Robert Gates has even gone so far as to request that monies allocated for foreign assistance to the Pentagon be redirected to the Department of State. Skeptical commentators in the world of development economics would say that there is good reason to shortchange civilian development—that we generally have little idea about fostering economic growth in poor countries and that foreign aid can do more harm than good. But the problem is not

cooperation. But unfortunately, an inconvenient truth has been overlooked: the expertise one would hope to find in other agencies and contractors does not exist.

Many in the military are acutely aware of this and are searching for alternatives. Working with many within the military over the past year, the Kauffman Foundation has developed the emerging field of Expeditionary Economics to help meet this demand.² At the core of Expeditionary Economics is the idea that the people of any given country must own the economy. Rather than a rehash of Marxist political economy, this is an explicit recognition that part of America's difficulties in Iraq and Afghanistan stemmed from a focus on large-scale reconstruction projects that made little connection with local populations and aggravated underlying issues around power and corruption. In particular, for people to own their own economy means the formation of indigenous commercial ventures. The military and civilian development agencies must approach their efforts through the eyes of local entrepreneurs. While every country's path to economic success is different, one common thread running through economic history—whether pertaining to the United States, China, Taiwan, India, or Brazil—is the overriding importance of entrepreneurship to economic growth.³

The centrality of new business formation has not been lost on the U.S. military. "Enterprise creation" is emphasized by counterinsurgency and stability operations field manuals (FMs).⁴ FM 3–07, *Stability Operations*, states:

*Host-nation enterprise creation is an essential activity whereby the local people organize themselves to provide valuable goods and services. . . . Host-nation enterprises may provide various goods and services, including essential services such as small-scale sewerage, water, electricity, transportation, health care, and communications. The availability of financing through banking or microfinance institutions is essential to enterprise creation.*⁵

Yet the efforts to promote such private sector development have consistently fallen short in Iraq and Afghanistan and even in the Balkans in the 1990s. Because the American military will face economic reconstruction tasks in the future, the United States needs to engender an independent capacity for economic analysis within the military.

Reforming the Development Apparatus

In our work with a wide range of officers and institutions in the military, we have sensed that many parties wish to break out of the conventional box of consultants and contractors. This box has always defined the contours of debate, advice, and new ideas on economic reconstruction. For example, the idea of a “whole-of-government” approach and talismanic references to “the interagency” have dominated this box. *Whole of government* refers to the notion that, when engaging in the reconstruction of a country such as Iraq, the effort should not be left solely to the Departments of Defense and State or the U.S. Agency for International Development (USAID). Because American aid programs cover agriculture, education, health, and business, it has seemed sensible to involve the corresponding Federal agencies in foreign assistance. So the Departments of Agriculture and Commerce have come to have a say in reconstruction. This is not necessarily wrong, but the very phrase *whole of government* implies two things. First, it conceptually precludes any contribution from the American private sector, and, when such involvement does occur, it is mediated through the Federal Government. Second, the United States has quite literally applied the whole of government in Iraq and Afghanistan, bringing the full force of the Federal bureaucracy and “counter-bureaucracy,” as Andrew Natsios has written, to bear on reconstruction and development.⁶

What inevitably occurs is a “too-many-cooks-in-the-kitchen” syndrome: the Organisation for Economic Co-operation

and Development counts 26 Federal agencies in the United States that contribute in some capacity to foreign aid and reconstruction. Whole of government thus gives rise, almost inevitably, to the interagency solution: with so many actors involved, collaboration across agencies becomes necessary to get anything done. Federal agencies like the State and Defense Departments end up signing formal memoranda of agreement to resolve barriers to cooperation. Yet when the problem is defined solely in terms of “low collaborative capacity” across government agencies, it operates as an intellectual constraint on any proffered solutions. If only this or that agency could work together, the thinking runs, they could *really* get something done. The constant appeal to the interagency eventually turns into an extreme example of bureaucratic navel-gazing, and the interagency becomes the end in itself. When I visited Iraq in the spring of 2010, one officer giving a briefing carried on about the interagency so much that several members of the audience were tempted to ask for the address of this mythical organization.

Likewise, the impulse to turn to established experts engages yet another limiting factor if the goal is to have innovative solutions to problems that often have never arisen before. The carefully calibrated dialogue that

time cycles of policy and politics in Washington operate almost to the exclusion of time for deep thinking

government contractors sustain with their sponsoring agencies has been observed many times to be inherently unimaginative. This is apparent in the case of many private sector consulting firms, among them those with the most prestigious reputations for independent thinking. When it comes to government, advice is inevitably tailored to make individual sponsors confirm thinking that might, among other things, help career advancement. Even think tanks, which are purportedly more independent, often have clear institutional constraints (many times political) that are seldom mentioned.

Time and again, the Kauffman Foundation and its collaborators on Expeditionary Economics have run up against the default impulse of this established community of thinkers. During a phone conversation with

a prominent think tank several months ago, one of its scholars asked us: “Which org chart box does Expeditionary Economics go in?” How can the military expect to tap innovative thinking when the expectation for any new idea is that it will simply be grafted onto the existing bureaucratic structure as the new “Bureau of” or “Office of”?

Part of the problem is something the military can do little about: the time cycles of policy and politics that in Washington, at least, operate almost to the exclusion of time for deep thinking. For the military to circumvent this, it must establish a new institution devoted to the study and crafting of Expeditionary Economics and that will help push the military and civilian development agencies to engage in entrepreneurial thinking about economic growth.

If-Then vs. What if

Expeditionary Economics is one part practical (what are the concrete objectives that can be achieved, and how do we get there?) and one part intellectual. Even as it places indigenous entrepreneurship at the forefront of postconflict reconstruction, it demands that the military and civilian agencies approach the task not through the usual “if-then” framework but through the entrepreneurial lens of “what if.” A useful nonmilitary way to think about this distinction is by considering the genesis of innovations. Historically, in the U.S. economy and elsewhere, breakthrough innovations are typically achieved by entrepreneurs—outsiders to the establishment—while more incremental advances are the province of existing organizations. Consider the automobile. There is a good reason why tinkering machinists such as Ransom Olds and Henry Ford rather than horse-carriage companies were pioneers in commercializing and developing automobiles. The same is true of the personal computer revolution. The innovation of the personal desktop computer upset an entire established industry, mainframe computers, and accordingly did not originate in that industry.

Existing organizations whose success and perpetuation are premised on established ways of operating usually approach problems and solutions through the lens of what has come before and rely on an inductive if-then mode of innovating. By contrast, breakthrough innovations usually emerge from a much more open what-if process of thinking. IBM looked at computing and *said*: If main-



U.S. Air Force (Brian Wagner)

PRT engineer discusses erosion control project with Afghan contractors near Qalat

frame computers are the dominant product, then we will build those. Microsoft and Apple ignored the logical lines of development and *asked*: What if computing was radically reduced to the desktop level? It should be quite apparent that if-then thinking, as presented here, is a perfectly reasonable and indeed natural approach to innovating. What-if thinking can only succeed sometimes because it originates *outside* of the establishment.

If-then thinking is also pervasive across the military, and for a good reason: strategists and planners must inductively conceive of a wide range of possible futures from present scenarios and what the responses would be. Yet it might not be appropriate for situations when soldiers and officers and aid workers face the daunting task of rebuilding a shattered economy. Instead, we must think like entrepreneurs and ask the sort of questions they would ask. What if this was true? What if we imagined this trajectory? What if we did such and such?

Entrepreneurial thinking entails an approach that is not only more proactive, but also much more imaginative. The most transformative entrepreneurs in business envision or create market needs rather than “filling” them, something we see in terms of

organizational innovation as well. The founders of the Mayo Clinic did not perceive that a world-class medical center was “needed” on the plains of Minnesota; they envisioned and created it there. The founders of Habitat for Humanity saw an ever-present need for low-cost housing for the less affluent, but there was no demand for providing it in the creative way they envisioned (that is, not until they brought that method to fruition; then it was wanted everywhere). Astute and imaginative military thinkers—especially those who have been on the ground in occupied countries—have special knowledge that few others in the world have, and they have the opportunity to apply that knowledge in ways beyond imagining for the rest of us.

The Military Is Innovative

It may strike many as contradictory that the U.S. military should want to seek out new and innovative ideas. Many associate the military with rigid hierarchy rather than fertile ground for innovation. Yet, as mentioned, the military has borne the burden of an undeveloped capacity for economic development and is determined to be better prepared for the next assignment. And it does possess a history of supporting innovation in one way

or another. The Defense Advanced Research Projects Agency is the most well-known example, but this would also include the adaptations made by individual soldiers and units on the ground in Iraq and Afghanistan that perhaps kept things from getting worse. The official history of the Iraq War, *On Point*, is filled with examples of such adaptations. The Commander’s Emergency Response Program is probably the best-known example of this, but tactical units all over Iraq and Afghanistan devised reconstruction strategies and action for their areas of responsibility: “All Soldiers had to become [Civil Affairs] officers and many became engineers. Most were not trained to manage even the smallest reconstruction project. Yet they often embraced their new role as nation-builders.”⁷

The challenge now is to institutionalize the lessons learned from Iraq and Afghanistan (as well as from prior reconstruction episodes that perhaps have not been adequately studied or absorbed by the military). The word *institutionalize*, of course, immediately suggests something bureaucratic, but we have in mind something more fundamental: building an independent economic analytic capacity for the military. Importantly, such a capacity requires a strong role to be played by civilians,

particularly those with expertise and experience in economic development and reconstruction. This should be approached as a way to help not only the military but also our aid agencies to break out of the bureaucratic confines within which they are trapped.

Military Economic Analysis Institute

What is envisioned is not the construction of another task force or unit that takes “off the shelf” economics and applies them to military issues. Rather, it begins from the assumption that an entirely independent organization should exist to conduct analysis and speculative theorizing around the what-if questions that are particular to military planning. There are few parallels, in terms of analytical substance, to the experiences of line officers of the 10th Mountain Division in the field.

Elsewhere, researchers at the Kauffman Foundation have proposed the recreation of a School of Military Government along the lines of the school that was established in 1940 at the outset of World War II. The analytic institution proposed here could conceivably be connected with such a school. This institution would not be a contracting agency but rather a permanent entity that has the capacity to provide completely independent economic analysis to military theorists and planners. Ideally, it would have the capacity to follow a speculative chain wherever it might lead and present the findings to American military leadership whether asked for or not. And it

likely should not be located in Washington, which is not a small matter. There is a reason that General David Petraeus was able to successfully develop a new doctrine of counterinsurgency at Fort Leavenworth, Kansas. As noted above, Washington time cycles can militate against reflective thinking, and this

the military's pragmatic culture and its quest for what really works could force the emergence of Expeditionary Economics

institution would need to be separate from the daily and weekly give-and-take of policy and politics in Washington.

Such an organization, devoted to speculative economics in the realm of geopolitical power relationships independent of the Pentagon but existing solely to support U.S. military thinking, might provide the imaginative challenges to both military policy and development economics. In the end, the military's pragmatic culture and its quest for what really works could force the emergence of a new kind of economics, Expeditionary Economics. Not only would development economics benefit from the pressure of testing theory in rapid succession in real circumstances, but the whole arena of future international contests, which could change the concept of warfare itself, might result from the American

military becoming the driving force for a new realism in economic science.

So what would such an entity look like? Titles are such that no organization's name can capture the full scope of its *raison d'être*, especially as its work shapes its very nature over time. But a name such as the Armed Forces Institute on the Economics of Security and Strategy would be broad enough to include a variety of programs under its auspices and would sufficiently convey its intended methodological approach—that is to say, economic analysis. As suggested by the predicates laid down thus far, the institute's focus would be on developing effective approaches to economic development in instances of American intervention, including preconflict (preventive defense), during conflict, and following conflict. Its purview should also include the study of and preparation for economic development in postdisaster scenarios, such as the January 2010 earthquake in Haiti and the floods in Pakistan last summer.

The institute's principal discipline would be economic analysis. In this regard, its name would align it with the military's unique capacity to advance other disciplines because of its singular experience. The Armed Forces Institute of Pathology and the Armed Forces Institute of Regenerative Medicine were created because the medical needs that arose in combat had such limited parallels in civilian sector medicine (or so it was thought) that there was little practical medicine that could be applied in the particular conditions of warfare. As it has turned out, by creating its own capacity to discover and elaborate medical knowledge in the worlds of trauma, communicable diseases, and rehabilitation, military medicine has been able to make enormous contributions to medical knowledge and practice as applied throughout the civilian world.

The Armed Forces Institute on the Economics of Security and Strategy might hold the similar promise of expanding the discipline of economics. The questions posed in the context of being able to bring about significant growth in various stagnant economies and establish economic ecosystems that are sustainable and that lead to expanding human rights and the coming of democratic institutions are ones not well developed in conventional economic theory. In graduate schools of economics, it is rare to hear the question: How do you start an economy over,

U.S. Navy (Rufus Hucks)



Microgrants, designed to stimulate local economies from bottom up, are distributed at Joint Service Station Tal Abtha, Iraq

or restart one destroyed by conflict? Indeed, the American record of being unable to point to instances of real economic development in countries where our aid policies have been at work over decades supports this observation. The institute, driven as it must be by crafting a theory of economic practice that can guide action that brings forth undeniable economic expansion, could work as an enormous force for clarifying domestic economic policy.

In order for the needed practical alternative to received development theory to emerge within the institute, there are obvious organizational considerations that must operate. At least five predicates must be in place for it to be successful. First, it must be independent in its financing and operations. While complete independence from the Pentagon may not be feasible, its resource needs should be arranged outside of normal budget cycles and constraints. Ideally, a private, public, or mixed endowment-type funding base would be established, much like an independent foundation. This is required to ensure as much as possible the freedom to follow various lines of inquiry wherever they might lead.

Relating to its operations, while the institute is housed within the military and is respectful of that culture, the military must regard it as having the objective credibility that attaches to medicine: it deals with reality in a way not influenced by political judgment or prevailing military or civilian doctrine. It is a place purposely set up to be independent and is chartered to develop new theory—ideas that when put into practice really work to bring about economic development. Because of the nature of its funding and its capacity to deliver new insight that might be unconventional and easily dismissed, the organization must be free to militate for doctrine and policy that reflect its understanding of economic matters as it has established them. This is the only way the institute can make a difference in doctrine over the long run.

Second, it should be seen as an asset that informs, but does not operationally report to, the Secretary of Defense or Joint Chiefs of Staff. As in all military resources, it is legally within the custodianship of the Joint Chiefs; operationally, it functions without seeking primary direction from the Secretary or Joint Chiefs, neither does it take its near-term priorities from them. The institute is a long-ball organization focused on how economic analysis, coupled with complementary analytic resources (for example, demography), can

produce strategies that may in the long run prevent conflict by establishing job-creating regimes and in the near term produce actionable plans that have a demonstrably greater capability of bringing about growth in post-conflict and disaster settings than prevailing development practice.

Third, it must develop its own ways of thinking and its own vocabulary. The institute must appreciate that like the other disciplinary-based institutes, it should absorb economic theory that applies to the questions at hand, but it must also test and develop new theory that is required to solve practical problems. Its method should be to assert that theory always precedes the development of practical solutions but that a high degree of skepticism exists for all theoretical postulates. In this regard, the institute's intellectual culture must be self-referential; its standard of excellence is shaped from within, not according to what the leading graduate programs are doing. Its staff must not care what "real" economists might think of this work. The institute's task, namely economic expansion,

from the beginning, skeptical of conventional economic doctrine, especially as it relates to development theory. While it would be good to have staff members who are military officers, it must be appreciated that the culture of the institute would require long-term stays so the collective work of the team of researchers continuously expands. For military analysts, appointment to the institute staff might be seen as a career capstone, much as a senior faculty position at one of the military academies might be. The institute might be guided by a civilian head, but not out of necessity. It would be a particular achievement if a military professional could be found who would be uniquely suited to manage the institute over a prolonged period. Again, the career risk is such that appointment to this post would be seen as a career capstone.

Finally, as noted, the institute should be physically removed from Washington, DC. Because it is a joint force asset, it might be located on neutral ground. Just as in the past certain research-intensive assets have been located proximate to university campuses,

the institute must absorb economic theory that applies to the questions at hand, but it must also test and develop new theory

is an area where civilian economists have little record on which to stand—or from which to resist new insight from institute scholars.

The institute should set out to develop an approach whereby its engagement with the Defense Department and other agencies is managed using the vocabulary and rhetorical conventions that it devises, appropriate to leveraging its insights into doctrine that governs actions on the ground. The military did just this as it invented what it called the field of trauma medicine and the ways in which it described its theory and practice. One benefit of this approach was that, as it was applied, it required physicians and nurses to conceive of the conditions of traumatic challenges to the body and their treatment in ways other than the expected or received ones.

Fourth, the institute should be staffed with particularly curious individuals whose formal training equips them for the rigors of scholarship that is different from that which they would perform in a university or think tank setting. The work and culture of the institute compel joint efforts as the *métier* of the organization. Those recruited must be,

given the central role that new firm formation plays in any emerging theory of development, it might be well advised to place it in the middle of a business incubation campus.

Of course, while the institute is decidedly an asset of the military, it should nevertheless be founded as a bridge that plays a particularly important role in changing the theory and doctrine of the State Department relating to overseas development work as well as the approach to economic growth that animates USAID. In fact, its presence might be welcomed by USAID as an institution independent of Federal budget cycles that perpetually operate as a constraint on the ability of USAID to develop a substantive in-house economic development capacity.

Current Development

At a much larger level, of course, serious thought needs to be given to how the United States overhauls or reorients its civilian development capabilities for the coming decades. This, obviously, cannot be the concern of the Defense Department, but the creation of a capacity for strategic economic analysis



NEW
from **NDU Press**
for the Institute for
National Strategic Studies



INSS Strategic Perspectives 3

Russia's Revival: Ambitions, Limitations, and Opportunities for the United States
by John W. Parker

Nearly three decades since the break-up of the Soviet Union, Russia has high ambitions for a return to great power status. With abundant resources, its nuclear power status, and United Nations veto power, Russia will retain the ability to project power beyond its own borders across a large swath of former Soviet territory. Such aspirations, however, are tempered by the realities of its social, economic, and military shortcomings and vulnerabilities. Russia likely is facing the prospect of decades of decline relative to other global powers. As a result, Moscow sees the West as crucial to Russian modernization and seeks to strengthen ties with Europe and the United States. This situation presents opportunities for U.S. diplomacy and strategy to move Russia toward positive change.



Visit the NDU Press Web site
for more information on publications
at ndupress.ndu.edu

within the U.S. military is an unavoidable part of this larger conversation. There will continue to be numerous instances in which the instigation of economic growth in certain countries furthers international security, but in which an American military intervention is neither necessary nor feasible. In those cases, U.S. civilian capabilities must be up to the challenge; ideally, this proposed institute would inform those efforts as well.

The approach advocated here and elsewhere is not meant to be simply a different rhetorical argument for what is pejoratively called nation-building. There should be serious doubt concerning the ability of the U.S. Government—military or civilian—to transform entire societies. What is beyond doubt is that economic growth elsewhere in the world will be critical to national security and strategy in the 21st century, and the United States must prepare accordingly. The establishment of the Armed Forces Institute on the Economics of Security and Strategy, dedicated to rigorous thinking about the abilities and limitations of the United States to foster such growth, would be a positive force for the shaping of strategy. **JFQ**

NOTES

¹ U.S. Joint Forces Command (USJFCOM), *The Joint Operating Environment 2010* (Suffolk, VA: USJFCOM, 2010); National Intelligence Council (NIC), *Global Trends 2025: A Transformed World* (Washington, DC: NIC, 2008).

² See Carl J. Schramm, "Expeditionary Economics: Spurring Growth after Conflicts and Disasters," *Foreign Affairs* (May–June 2010); Rebecca Patterson and Dane Stangler, *Building Expeditionary Economics: Understanding the Field and Setting Forth a Research Agenda*, Kauffman Foundation Research Series on Expeditionary Economics No. 1, November 2010, available at <www.kauffman.org/uploadedfiles/ee_report_1.pdf>. For a record of the proceedings at the inaugural conference on "Entrepreneurship and Expeditionary Economics," held in conjunction with the Command and General Staff College Foundation in May 2009, see <www.expeditionaryeconomics.org>.

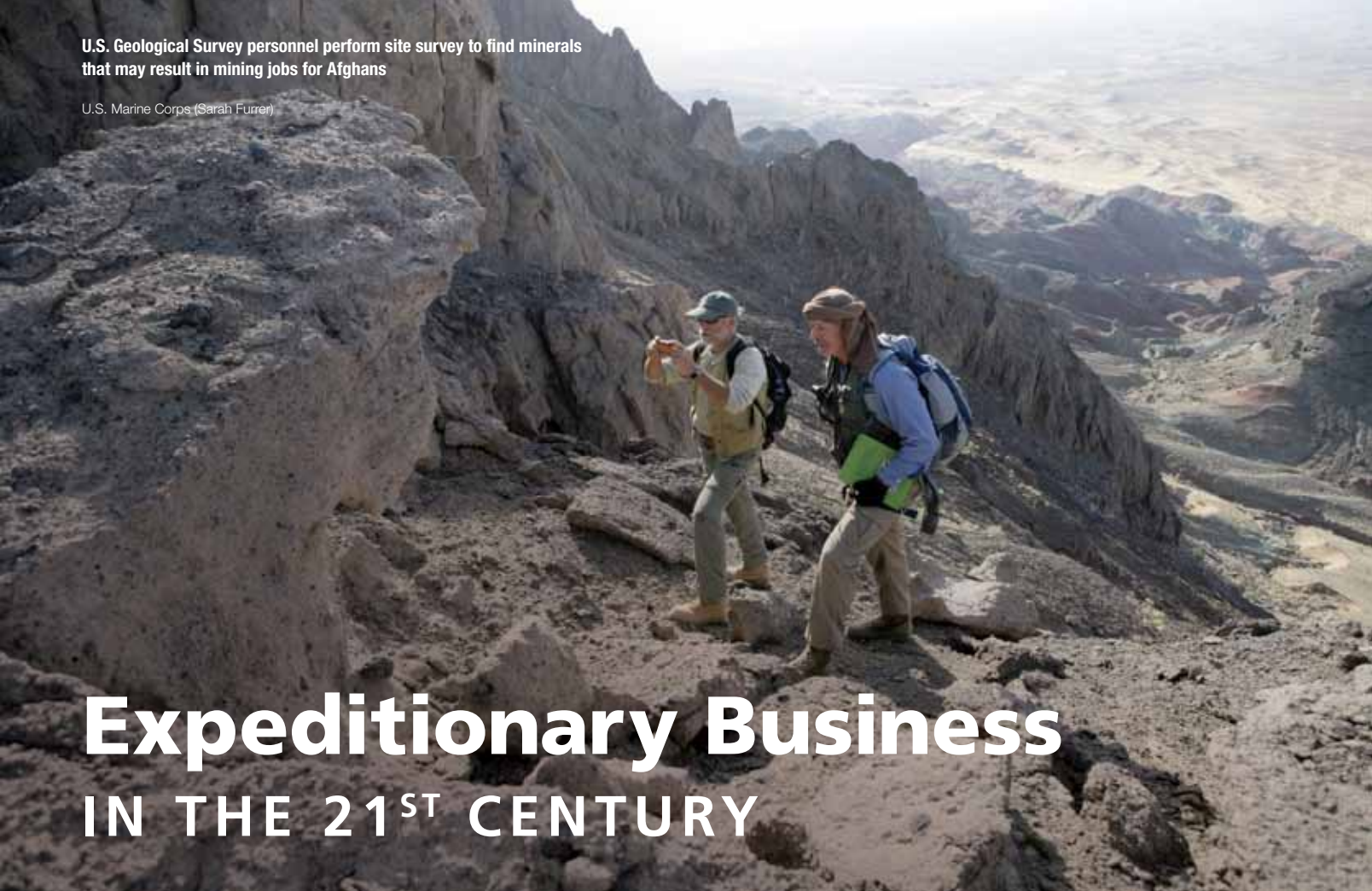
³ See David S. Landes, Joel Mokyr, and William J. Baumol, eds., *The Invention of Enterprise: Entrepreneurship from Ancient Mesopotamia to Modern Times* (Princeton: Princeton University Press, 2010); Carl J. Schramm, "Building Entrepreneurial Economics," *Foreign Affairs* (July–August 2004); Tarun Khanna, *Billions of Entrepreneurs: How China and India are Reshaping their Futures—and Yours* (Boston: Harvard Business School, 2007).

⁴ U.S. Army Field Manual (FM) 3–24/Marine Corps Warfighting Publication No. 3–33.5, *The U.S. Army and Marine Corps Counterinsurgency Field Manual* (Chicago: University of Chicago Press, 2007); FM 3–07, *The U.S. Army Stability Operations Field Manual* (Ann Arbor: University of Michigan Press, 2009).

⁵ FM 3–07.

⁶ See Andrew S. Natsios, "The Clash of the Counter-Bureaucracy and Development," Center for Global Development, July 2010, available at <www.cgdev.org/content/publications/detail/1424271>. See also Todd Moss, "Too Big to Succeed? Why (W)Hole-of-Government Cannot Work for U.S. Development Policy," available at <www.huffingtonpost.com/todd-moss/too-big-to-succeed-why-wh_b_750900.html>.

⁷ Donald P. Wright and Timothy R. Reese, *On Point II: Transition to the New Campaign: The United States Army in Operation IRAQI FREEDOM May 2003–January 2005* (Fort Leavenworth, KS: Combat Studies Institute Press, 2008).



Expeditionary Business IN THE 21ST CENTURY

By ROBERT E. LOVE and STEVE R. GEARY

*Conditions change. Objectives change. Strategies change. And we must change.
If we don't, we will lose.¹*

We live in a dangerous world. The unfortunate truth is that when one danger fades, another appears. And nobody has yet come up with a reliable crystal ball to predict what the next danger will look like.

For too many years, the governments of the developed world have poured their hearts, souls, and national treasures into fractured or failed states in an effort to establish or restore functioning societies, improve quality of life, and integrate the states into the global family of nations. Much has been written on the benefits and perils of unrestrained aid packages, soft loans, and government-sponsored attempts at rehabilitating these impoverished nations.

Fortunately, a number of countries have made progress (Rwanda, Ghana, Liberia, Uganda, the Balkan nations, and Northern Ireland, to name a few). There have been numerous cases of government transfers of power without the threat of violence or civil unrest. But in terms of a “return on investment” (over \$1 trillion by the United States alone in the last few decades), the results have been marginal. Citizens of Sudan, Somalia, East Timor, and many other countries continue to live below the poverty level and without the benefit of reliable, credible, and compassionate civil government.

So what is to be done, and by whom? Is it solely the province of governments to improve economies and reduce violence? On the ground, where reality defeats rhetoric, people

in failed and failing states need hope, and hope requires the belief in a better tomorrow for all of our children. But hope alone is not enough. It must be accompanied by real and credible action.

Indeed, peace and prosperity walk hand in hand, but prosperity—delivered by a healthy and growing economy—is the province of business.

A New World Order

Author Rita Mae Brown wrote, “Insanity is when you keep doing the same things expecting different results.” The world is a different place than it was during the colonial and Cold War timeframe. The time has arrived for a new and focused approach to supporting a stable world. The 21st-century

Robert E. Love is Director, Strategic Initiatives, Systems Engineering Solutions, BAE Systems, Inc. Steve R. Geary is President of Supply Chain Visions, Inc.

environment can be characterized as having a dynamic security threat—including the rising tide of radical and violent pan-national religious fundamentalism, interdependent mutually supporting international economies (abhorrent to the type of radical religious

organizations (NGOs), international governmental organizations, and the business community. Campaign plans for stability operations are complex strategies spanning civil security, civil control, essential services, governance, economic development, and

reducing corruption, and facilitating culturally acceptable best business practices is both socially responsible and good for business. This approach allows for the opening of new markets while creating a viable, honorable alternative employment option to those who might otherwise be drawn to terrorist cells. Hiring local nationals (versus third country nationals) is good for business, good for the local economy, and good for civil society. Terrorists prey on the unfortunate to do their bidding. They breed instability and destroy market opportunities.

peace and prosperity walk hand in hand, but prosperity—delivered by a healthy and growing economy—is the province of business

fundamentalism espoused by the Taliban), and colossal global environmental challenges. As Tom Friedman so eloquently posits in his bestseller of the same name, the world is flat.

Today, in the hallways of power around Washington, it has become fashionable to talk about “whole-of-government” efforts, bringing together the elements of defense, diplomacy, and development to craft sustainable solutions. Unfortunately, this line of thinking often does not go far enough. Private industry and commercial enterprise are often the critical and overlooked link in a truly comprehensive solution set. The private sector has a valuable role to play in responding to this new world order, but it is as a catalyst, a collaborator, and an integrator. By using innovative approaches to opening new markets, improving capacity in developing nations, and leveraging legitimate and acceptable business standards tailored to fit with local customs, the private sector can fulfill its responsibility and improve the quality of life for impoverished people while concurrently generating revenues that will sustain the momentum.

Practical economic initiatives, both macro and micro, are required to support the evolution of capabilities throughout the developing world. No longer can we *reach back* behind the line for business solutions and capabilities to capitalize on soft power. Business solutions, as well as complementary essential capabilities such as rule of law expertise, must be *pulled forward* as an instrument for stability operations and as a component of smart power. Security and economic stability precede an effective and stable government. They go hand in hand—not sequentially. The Cold War is over.

In pre- and postconflict situations, stability operations are emphasized. Stability operations must use a broad array of nonkinetic capabilities resident in the U.S. Government, coalition partners, nongovernmental

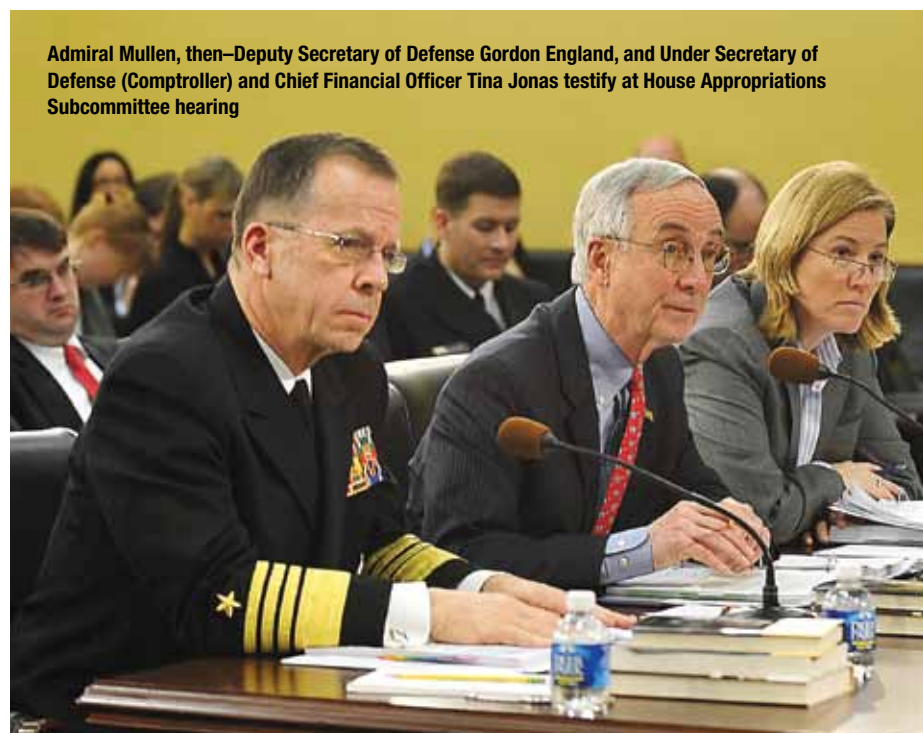
infrastructure development, wrapped within offensive and defensive operations. Within this complexity, there is a consistent thread: while many things are required, it is always true that stability operations inherently include some element of business solutions—the policies, processes, data, technology, and people—available forward in the expeditionary operations environment to win the battle for hearts and minds and thereby secure the peace. Generating business, creating and sustaining legitimate jobs, and improving the quality of life will go a long way toward eradicating terrorism. Putting a pair of wingtip shoes on the ground, in addition to or in lieu of boots on the ground, can be an important part of creating sustainable progress in failing states.

The role of multinational corporations (MNCs) in supporting good governance,

Governments and the private sector must work together in an environment of trust to combat radicals and thugs who threaten human security. What is required is controlling and directing “the spend”—that is, converting business operations into a tool that can be used to mitigate threats.

On the ground in Iraq, Afghanistan, Africa, or anywhere in the developed and developing world, there is a need to push business solutions forward, linking together capabilities from a variety of sources. The business community cannot sit idly by while government forces combat terrorism. Terrorism affects all of us; it restricts freedom of movement, impedes free trade, increases costs, threatens employees, and limits the market.

It is about creating unity of effort without unity of command. Governments can and must establish and enforce the law, set



Admiral Mullen, then–Deputy Secretary of Defense Gordon England, and Under Secretary of Defense (Comptroller) and Chief Financial Officer Tina Jonas testify at House Appropriations Subcommittee hearing

DOD (Cherie A. Thurby)



U.S. Army (Jeanita C. Pisachubbe)

Election officials and Afghan National Police in Baghlan Province deliver ballots to CH-47 Chinook helicopter

standards, and encourage investment. Businesses must have the freedom to establish relationships, develop investment and business opportunities, and bring or add legitimacy by leveraging their accepted and recognized business practices to developed nations.

Expeditionary Business

The emerging 21st-century security environment of soft power projection and highly visible collaboration outside of traditional military operations will continue to require new visibility tools, collaboration technologies, information flows, economic expertise, and support processes in the capability set, adapted to bring peace to a developing nation in a multinational, austere, and forward expeditionary operations context.

At the Senate Budget Committee hearing of February 12, 2008, Deputy Secretary of Defense Gordon England testified that “the challenges we confront today defy an exclusively military solution and demand an integrated approach. Secretary [of Defense Robert] Gates has said that, in the future, ‘Success will be less a matter of imposing one’s will and more a function of shaping

behavior—of friends, adversaries, and most importantly, the people in between.” The likelihood of a successful outcome is increased by the influence provided by traditionally nonmilitary activities such as economic development, infrastructure reconstruction, employment generation, and humanitarian interventions. Frequently, needed business capabilities reside outside of the government. Some call this a collaboration challenge, but in truth it is a partnership opportunity, a chance to bring the full suite of capabilities to bear to overcome the forces of tyranny while spurring economic growth.

Economic development in pre- and postconflict situations includes both short- and long-term aspects. The short-term aspect concerns immediate problems, such as large-scale unemployment and reestablishing an economy at all levels. The long-term aspect involves stimulating indigenous, robust, and broad economic activity. The stability a nation enjoys is often related to its people’s economic situation. Without a viable economy and employment opportunities, the public is likely to pursue the false promises of those seeking to undermine freedom and democracy.

Sometimes insurgents foster the conditions keeping the economy stagnant in order to create discontent and foster antigovernment opposition. Opponents attempt to exploit a lack of employment or job opportunities to gain active and passive support for their cause and ultimately to undermine the government’s legitimacy. Unemployed males of military age may take up arms to provide for their families.²

One of the key obstacles to establishing stability in Iraq was the inability to get the economy going. A senior military leader asking for a business solution in a country emerging from the depths of instability observed, “A relatively small decrease in unemployment would have a very serious effect on the level of sectarian killing going on.”³ According to Keith Mines, Governance Coordinator for Anbar Province in Iraq, “If economic tools will not compensate for the lack of a viable political and security framework, they can nonetheless be a major support to counterinsurgency efforts in support of a well-crafted strategy, especially at the local level. To be effective, they should be short-term, focused on people, and flexible.”⁴

Indeed, MNCs are large, monolithic enterprises that tend to follow long-term strategic plans and may not consistently demonstrate the attribute of flexibility. Nonetheless, they can play a vital role in counterinsurgency operations by adapting their modus operandi to the expeditionary environment.

The government needs access to entrepreneurial savvy. But where will the business savvy come from? According to Theresa Whelan, former Deputy Assistant Secretary of Defense for African Affairs, "You cannot promote security and stability successfully in a vacuum. Stability and security are

of enterprise capabilities in a new context. For this reason, business capabilities must continue to grow to secure the peace, just as military capabilities evolve to meet the threats of the future.

The challenge facing the private sector is in how to make a business case to engage actively and support the effort, sooner rather than later. For stability operations to succeed, hard and soft power activities must take place concurrently. Yet too often, Western business leaders wait for the emergence of a more secure environment as a precondition to investment, but without business activity, a

paid to ensure that required business skill sets are embedded into the expeditionary business environment.

Welcome to the 21st century, the era of business savvy and interagency collaboration as a necessary instrument for world peace. **JFQ**

NOTES

¹ G. Terry Madonna and Michael Young, "Fighting the Last War," June 4, 2002, available at <www.fandm.edu/politics/politically-uncorrected-column/2002-politically-uncorrected/fighting-the-last-war>.

² Selected points from Field Manual 3-24, *Counterinsurgency* (Washington, DC: Headquarters Department of the Army, December 2006), 5-46, 5-48.

³ Josh White and Griff Witte, "To Stem Iraqi Violence, U.S. Aims to Create Jobs," *The Washington Post*, December 12, 2006.

⁴ Keith W. Mines, "Economic Tools in Counterinsurgency and Postconflict Stabilization: Lessons Learned (and Relearned) in al Anbar, Iraq, 2003-04," Foreign Policy Research Institute E-Notes, September 28, 2006, available at <www.fpri.org/enotes/20060928.military.mines.economictoolscounterinsurgency.html>.

⁵ Steven Donald Smith, "Africa Command Poised to Help Continent's Security, Stability," American Forces Press Service, September 21, 2007.

⁶ James Risen, "U.S. Identifies Vast Riches of Minerals in Afghanistan," *The New York Times*, June 14, 2010, A1.

U.S. troops are still fighting the war, and the Chinese have already moved on to the business of developing the peace

interlinked with other elements such as good governance, the rule of law, and economic opportunity.²⁵ By having interagency personnel with different areas of expertise integrated into the command, the knowledge base will be broadened, which will help the command fulfill its duty. "This does not represent an acquisition by the command of authority," Secretary Whelan stated. "It represents simply an acquisition of knowledge." To be sure, the U.S. Agency for International Development and Department of State, as well as NGOs, the World Bank, private sector, and other stakeholders, bring subject matter expertise.

Economic stabilization consists, in part, of the restoration of employment opportunities and the regeneration of market activity. This is a challenge, a requirement for business solutions that often extends into the diplomatic, information, and economic arenas.

Different Results

The challenges facing the private sector are many, but the opportunities are infinite. Corporate leaders must have the vision to:

- identify strategic business cases (tailored to developing nations)
- mitigate risk (to employees, shareholders, and indigenous populations) in innovative ways
- team with nontraditional partners (such as NGOs)
- create and sustain capacity (while maintaining revenue streams).

The use of private sector capabilities in developing nations is simply the application

more secure environment cannot develop. An overly developed sensitivity to risk puts the private sector into an irresolvable Catch-22 and precludes the opportunity to capitalize on economic opportunity.

While it could be argued that the Western business community cannot sit idly by while government forces combat terrorism, a more fundamental issue is in play. If the business community does not collaborate and participate in stability operations before a secure environment emerges, it is in fact doing a disservice to stockholders. In the world of venture capital, early participation is called first-mover advantage.

The United States has discovered nearly \$1 trillion in untapped mineral deposits in Afghanistan. It includes huge veins of iron, copper, cobalt, gold, and critical industrial metals such as lithium. Today, the largest developer of minerals in Afghanistan is China, the winner of the development rights to the Aynak copper mine in Logar Province.⁶ China, a nation with ostensibly a communist economy, is outmaneuvering the capitalist economies of the West in high-risk environments. U.S. troops are still fighting the war, and the Chinese have already moved on to the business of developing the peace.

The diversity of needs at the tip of the spear means that monolithic enterprise solutions conceived thousands of miles out of harm's way to address strategic requirements may not readily link to reality on the ground. Care must be taken to weave and integrate the needs of the forward environment into stability operations, and attention must be

SAVINGS

and the Defense Logistics Enterprise

By C.V. CHRISTIANSON

I am directing the military services, the joint staff, the major functional and regional commands, and the civilian side of the Pentagon to take a hard, unsparing look at how they operate—in substance and style alike.

—Secretary of Defense Robert Gates



U.S. Navy (Kelly Chastain)

Floating causeway delivers relief aid from Military Sealift Command ships in Port-au-Prince, Haiti

Lieutenant General C.V. Christianson, USA (Ret.), is the Director of the Center for Joint and Strategic Logistics at the National Defense University.

want to take this opportunity to voice my strong support for Department of Defense (DOD) efficiency initiatives and to encourage further thought and discourse about whether these initiatives will be enough to deliver the kind of savings necessary to produce affordable, sustained defense capabilities for the long-term support of our national security requirements. Global uncertainty, regional volatility, and the growing complexity of our security environment are combining to challenge us like never before. Add to this potent mix the clear and present need to reduce and reshape defense expenditures, and we find ourselves confronting a gauntlet of difficult and risky decisions that will shape our security capabilities for years to come. In this ambiguous environment, defense logistics has necessarily become an area of focus for those who are determined to make a difference.

The Challenge

Secretary Gates, in his May 8, 2010, Eisenhower Library speech in Abilene, Kansas, laid the foundation for savings in the defense “business” by directing a series of wide-ranging efficiencies designed to deliver more than \$100 billion in overhead savings over the next 5 fiscal years, starting in fiscal year 2012:

The goal is to cut our overhead costs and to transfer those savings to force structure and modernization within the programmed budget. In other words, to convert sufficient “tail” to “tooth” to provide the equivalent of the roughly two to three percent real growth—resources needed to sustain our combat power at a time of war and make investments to prepare for an uncertain future. Simply taking a few percent off the top of everything on a one-time basis will not do.

The last sentence of the statement is fundamental to the thesis of this article: We cannot achieve the wide-ranging improvements he envisioned if we remain focused on delivering “one-time” savings. I would like to propose a view of how we might reach beyond the current initiatives and realize even deeper, longer-term systemic savings in the defense logistics enterprise without creating unmanageable risk to the operating forces. This idea is offered as a starting point—to encourage the serious dialogue necessary to promote change and, in a perfect world,



U.S. Air Force (Margo Wright)

Tinker Air Force Base personnel celebrate kickoff of \$2.9 billion computer and ground systems upgrade to Air Force E-3 Sentry Airborne Warning and Control Systems aircraft

to help transform defense logistics in ways that would not only reduce resource requirements, but also enhance the effectiveness of the outcomes the community is responsible to deliver. Thus, phrased as a question, are we looking deep enough to deliver the sustainable savings needed?

Logistics is arguably the largest consumer in the defense budget. Therefore, if we are to achieve realistic savings over time, logistics will have to play a predominant role in generating those savings. At the same time, logistics is also the common thread linking the operational ends of our national security with the resources of the Nation. As a result, there are risks involved in generating significant savings across the logistics enterprise.

Probably the greatest paradox in generating savings is time—the natural tendency to focus on delivering *near-term results* is often at odds with achieving *long-term savings*. Current initiatives are focused on delivering results over the next 5 years—the length of the DOD programming horizon—but I believe that the most meaningful and relevant savings in the defense logistics community may not provide immediate return on our investments. Focusing on short-term savings could lead to a vision and strategy concentrated on targets of opportunity while continuing many of the expensive and inefficient practices that increase enterprise costs. Just extinguishing the “fires at our feet” could create long-term risk by imparting a sense of accomplishment based on near-term savings while avoiding the downside impacts of cumbersome processes and bureaucratic structures that drive signifi-

cant long-term costs. I do not mean to imply that the current initiatives are not needed; these actions are *absolutely essential*. Rather, I am proposing that a longer-term view is just as critical—maybe even more so—to meet the imperative of reducing the defense logistics costs that deliver operational capabilities.

A Framework

I see three fundamental areas where the defense logistics community can generate significant long-term savings while improving outcomes to the operating force. The first area is best described as *supply chain operations and management*, the network of

the most meaningful and relevant savings in the defense logistics community may not provide immediate return on our investments

organizations, information, and processes responsible for responding effectively to the changing requirements of the operating forces. The second area exists within a philosophy and culture of *life-cycle systems management*, a framework responsible for the design, development, production, sustainment, and disposal of the systems/capabilities needed by the operating forces. The third area is related to *resourcing national security strategy*, the ability of senior logistics leaders to manage national resources with business discipline and to develop alternatives in the

context of cost, operating results, and return on investment.

These three areas of emphasis represent a high-level framework within which we can address long-term improvements to the way the defense logistics enterprise does its business. These areas will help us focus on the quality of leader decisions, the efficiency of logistics processes, and the effectiveness of relationships that are fundamental to driving sustainable change and continuous improvement in the defense logistics enterprise.

Supply Chain Operations and Management. We must optimize defense logistics players, policies, and processes against common outcomes as defined by the customer.

Previous generations of logisticians were able to deliver success by finding ways to interoperate within a linear defense supply chain that most viewed as unique to our business and was comprised of several distinct activities. There is no question that in the future we will be required to view our supply chain not as a chain per se, but as a *network* (military, interagency, multinational, and commercial) of suppliers, distributors, manufacturers, and customers linked in a complex global federation.

Today's organizations and processes were not designed to work in harmony. Tomorrow's world demands that we understand the interactions, relationships, and interdependencies among various organizations, processes, and data across the entire defense logistics enterprise. This is the essence of systems thinking and is essential to enabling future logistics leaders to make better decisions with regard to supply "chain" outcomes. Tomorrow, we must have a supply network that is flexible and resilient enough to support rapid changes in strategies—and we require leaders who will thrive in a self-organizing environment.

One could argue that today there is no single outcome metric to drive optimization across our global supply chain. Tomorrow's environment will demand that we find ways to deliver unity of effort across this global network without having unity of command over all the elements executing actions within that network.

Throughout most of our nation's history and in the current environment, we have been committed to delivering supply chain outcomes at almost any cost and are, in most cases, unable to determine the fully burdened cost to deliver those outcomes. Tomorrow we

will not have the resources to give support at any cost; therefore, we have to optimize activities so the supply chain delivers what

Increasing efficiency and productivity separately from the processes that drive how we buy and sustain systems investments

the separation of execution from budgeting will not facilitate the synergy between acquisition and sustainment necessary to reduce systems' life-cycle costs

the operational force requires—at a price our nation can afford.

Life-cycle Systems Management. We must effectively merge acquisition and sustainment to ensure that we deliver required systems' life-cycle availability at best value to the Nation.

The philosophy of life-cycle systems management (LCSM) demands policies, structures, and processes that deliver decisions that balance operational outcomes against fully burdened life-cycle costs. This implies a fusion of acquisition and sustainment to a degree few realize and requires that we build in a culture of the "long view" with regard to systems support.

This philosophy argues for initiatives that are, at the core, elemental to acquisition reform. The separation of execution from budgeting will not facilitate the synergy between acquisition and sustainment necessary to reduce systems' life-cycle costs.

does not support LCSM. A pervasive culture of life-cycle systems management would certainly generate significant gains in productivity, drive down system sustainment costs, improve partnerships with industry, and force the acquisition and sustainment communities to optimize their collective efforts against common operational requirements.

Over the life of a system, a more holistic approach to acquisition and sustainment would offer the most potent method to improve both execution/outcomes and optimize the processes behind those outcomes. However, we have a long, challenging road ahead in this area. Congressional language with respect to both life-cycle systems management and weapons systems acquisition reform, although reflected in recent DOD actions, has not yet changed the distinctive organizational cultures attached to the acquisition and sustainment communities. In this case, LCSM would fully embrace the



Army Tactical Missile System is recertified by member of team responsible for environment, safety, and occupational health facets of Army aviation and missile acquisition, sustainment, and disposal

U.S. Army

congressional language on weapons systems acquisition reform and program support assessment by merging those initiatives within a common framework for processes, information, and decisionmaking. LCSM can effectively link acquisition and sustainment by enabling support decisions based on total life-cycle costs, where all costs are fully visible to the enterprise. As a result of having clear representation of the fully burdened costs to deliver availability, the quality of tomorrow's decisions would be exponentially better than today's. The investment in making better decisions to reduce life-cycle costs would easily pay for itself several times over the life of a system, producing massive savings across the many systems in the defense portfolio.

Resourcing National Security Strategy. We must develop a much deeper understanding of the confluence of resource planning

that ensure the defense outcomes required in support of our national security are fully sustainable and delivered at best value. Significantly reducing costs in the defense logistics enterprise without unacceptable risk requires leaders who can effectively analyze the components of the industrial base and evaluate them as potential resources to apply against our national security challenges.

Education as the Ultimate Efficiency

We must establish a developmental framework that gives logisticians the right knowledge, skills, and attributes to succeed in an uncertain, complex, and volatile environment. We cannot be certain that decisions made today will be valid for years to come. In an ambiguous environment, we should expect that our senior leaders be able to continuously reassess their environment and understand

edge and attributes of systems thinking will give tomorrow's logistics leaders the greatest opportunities for quality decisions and, ultimately, success.

Second, how can we offer the most effective learning environment for tomorrow's logisticians? Establishing a learning environment grounded in the principles of cognition and using student-led learning as its core will foster learning for tomorrow's logistics leaders. Moreover, establishing an interactive culture in our classrooms will further facilitate student-led learning, and, when integrated with case study methodology and serious gaming, will create a learning environment that looks and feels like the complex, uncertain world in which we expect our logistics leaders to excel.

The most important element to creating an effective and dynamic learning environment is our logistics faculty. If we expect tomorrow's logistics leaders to benefit from a learning environment that is rapidly adapting to changing operating conditions and reflecting the most critical learning outcomes for the enterprise, how can we better prepare the faculty to provide that environment? Developing logistics leaders who will succeed in an uncertain future requires an investment in our logistics faculty. This may be the most critical investment of all.

What Stands in Our Way?

As mentioned earlier, the natural tendency to zero in on close targets can sap resources needed to focus on longer-term strategies. Our culture does not make addressing long-term solutions easy; the resistance to change is deeply embedded when outcomes cannot be realized during the tenure of those currently in leadership positions. However, delivering systemic, long-term, meaningful improvements in the defense logistics enterprise mandates that we look beyond our respective tenures.

The approach I have offered may not deliver short-term gains, but I believe it is within this type of framework that the defense logistics community can achieve the most significant long-term returns in both effectiveness and efficiency. Delivering a 2 to 3 percent improvement in efficiency over the next 4 to 5 years is mandatory, but driving longer-term improvements in how we manage the business of defense logistics requires a more holistic view of logistics itself and of those who lead that community. **JFQ**

tomorrow's logistics leaders must be able to understand relationships among processes, organizations, and information in ways few can imagine today

and execution, systems readiness, and operational outcomes.

Optimizing our national resources against prioritized operational outcomes and maintaining a constant awareness of the total costs to deliver required outcomes are at the heart of this focus area. Today, this business area is underserved in our logistics developmental continuum; it is not a "knowledge" requirement clearly identified for our senior leaders. The understanding, knowledge, and skills needed to fuse human resources, raw materials, finance, acquisition, and sustainment in support of our national security objectives must become fundamental to tomorrow's logistics leaders.

This focus area also lies at the heart of relationships between the defense logistics community and our industrial base and is essential to developing the type of partnerships that can deliver value to the Nation while offering reasonable profits to industry. It is imperative that we develop logistics leaders who not only understand but also can synthesize issues related to defense and industry acquisition, sustainment, and financial processes, and who are able to develop business case-based assessments of defense and industry partnerships and relationships. An in-depth understanding of the business of defense logistics will result in decisions

the problems they face in the context in which those problems are presented. Furthermore, we should expect that those same leaders be able to develop approaches to managing problems that deliver the best outcomes for our nation. In that regard, I believe the most critical area related to improving efficiency in the defense logistics enterprise lies in *educating its leaders*.

The most crucial element to driving down costs in the defense logistics enterprise will be the quality of our defense logistics leaders' decisions. We will not achieve sustained, long-term savings without a sustained, long-term investment in the leadership responsible for directing actions toward those ends. We have a community of institutions, curriculum, and knowledge responsible for shaping the thinking of tomorrow's logistics leaders, and it is there that our investments can have the highest return.

Our venture into this critical area should resolve to answer three fundamental issues about learning. First, can we agree on what tomorrow's logistics leaders need to be? Even though there is a strong consensus that we need to develop critical thinkers, I offer that tomorrow's logistics leaders must be able to understand relationships among processes, organizations, and information in ways few can imagine today. Developing the knowl-



Rethinking Foreign Area Officer Management

By WILLIAM E. WARD

Attachés, security assistance officers, and other U.S. military personnel stationed at Embassies abroad perform vital functions in support of advancing the Nation's security interests. They establish important links with host nation militaries. They articulate requirements for military programs, activities, and exercises that help build partner nation security capacity. They serve as the forward "eyes and ears" of the parent geographic combatant command, the Services, and our military intelligence community. As military representatives to our Embassies and Chiefs of Mission, they are key sources of information about security environments, threats to stability and security, and civil-military relations.

As members of Country Teams, these personnel are accustomed to operating as

part of an integrated interagency effort that addresses diplomatic, developmental, and security needs in support of U.S. foreign policy objectives. Their presence fosters unity of action across the joint, interagency, inter-governmental, and multinational spectrum.

These are specialized assignments normally reserved for the Services' Foreign Area Officer (FAO) corps. Many join these communities as new majors and lieutenant commanders who were exceptional performers within their Services at junior tactical assignments. Upon accession, they receive specialized education in regional studies and cultural awareness, develop advanced language proficiency, and improve their ability to operate independently (often alone) in austere environments. Their training and education are extensive and necessary to ensure they are effective.

However, we have seen numerous occasions where these vital functions are being performed by personnel without the requisite training or experience, and the results can negatively impact the mission. The following examples come from Africa, but similar situations occur elsewhere.

One critical Central African partner nation had an extensive security assistance account of \$40 million, which included \$35 million for a training and equipping package. However, the security assistance officer position at the U.S. Embassy was gapped for an extended time, causing U.S. Africa Command to rotate personnel out of hide on short temporary duty stints to usher the portfolio along. Meanwhile, the only enduring presence was

General William E. Ward, USA, is former Commander of U.S. Africa Command.

an administrative sergeant who lacked security assistance training or Africa experience.

A key Western African partner was serviced for over 2 years by an Army Reserve logistics officer with no FAO or language training because of shortages in available personnel. Due to the officer's lack of French language skills, the Embassy's political-military officer had to perform escort duties to all meetings with the host nation military. This arrangement was rightly criticized by the Ambassador as unsustainable.

Some U.S. Embassies in key partner nations have experienced significant gaps in Department of Defense (DOD) presence. In one nation, an Air Force attaché billet that

career progression are outmoded. There is also insufficient ability for the FAO community to feed their critical skills back among the general purpose forces in ways that facilitate military activities with new or emerging partners. The FAO community and the joint doctrine of security assistance require a sizeable transformation effort.

This article first focuses on two common functions that FAOs perform overseas, Security Assistance Officer (SAO) and Defense or Service attaché, to show how requirements have evolved while doctrine has not kept up. Then it presents necessary and appropriate functions for the FAO community, such as cultural intelligence and knowledge

procured capacities against evolving security threats. But because these particular programs are used as the basis for justifying FAO personnel, many Embassies in Africa find the defense attaché dual-hatted in a security assistance capacity, which often disadvantages both positions.

Moreover, because this is a demand-driven process, the manpower follows the program. Once an FMF or FMS case is established, DSCA determines and sources the FAO requirements over time based on when the program is executed. This is fine for partners with established Offices of Security Cooperation (OSCs)² who already have FAOs on hand serving as requirements developers, planners, and implementers, in addition to performing liaison functions with the Country Team and back to the combatant command. But partners where no OSC is established are disadvantaged. The requirements development process among new and emerging partners is methodical and deliberate, based on mutual trust and confidence built over time. FAOs are ideally suited to performing this task, but establishing new OSCs or growing existing ones is too slow and unresponsive a process in an environment of limited joint growth. This additionally undermines efforts to establish relations with countries where none have existed in the past. Simply put, we need more FAOs forward.

the doctrine associated with the FAO community is out of date, and the models of accessions, utilization, and career progression are outmoded

opened in 1999 was only filled for a total of 24 months during the period of 1999 to 2005. In two other nations, the rapid ramp-up of military programs and activities exposed the problems of longstanding gaps in FAO billets. To meet the immediate needs, these slots were filled with motivated officers who wanted to help but lacked the formal skills and experience to do the job effectively.

These examples are symptoms of a greater problem. The joint FAO community's accession patterns and doctrinal utilization have not sufficiently kept up with the evolving needs of the Country Teams. Demand is already exceeding supply, and the call for FAOs is increasing further as the United States broadens its global engagement to encompass more nations.

Defense Secretary Robert Gates noted this in his February 2010 address to the Nixon Center and his *Foreign Affairs* article in May 2010,¹ in which he stated that security force assistance was a key U.S. military function requiring higher priority, that cultural awareness and sociopolitical acuity were important in establishing trusted relationships with partners, and that such relationships enhanced the ability to prevent conflict and ultimately reduced the overall need to commit U.S. forces to military operations.

But as this article shows, simply increasing the number of FAOs is not the complete answer. The doctrine associated with the FAO community is out of date, and the models of accessions, utilization, and

development, which are presently missing in action. The current state of the joint FAO community is then presented, followed by recommendations for improvements.

The Security Assistance Function

The management practice within DOD aligned the role of SAO with well-defined security assistance programs exercised by a partner nation. In particular, these programs were Foreign Military Sales (FMS), Foreign Military Financing (FMF), and International Military Education and Training (IMET). This created a demand-driven approach in which the establishment of FMS/FMF cases or the recruitment of partner members to attend IMET in U.S. military schools drove the size and scope of an SAO within the Embassy. The management of the joint manpower allocated to these offices was given to the Defense Security Cooperation Agency (DSCA). Subsequently, the Services have generally defined the roles of these FAOs in terms of the requirements of these programs.

This method clearly disadvantages those partner nations whose security capacity-building requirements do not centrally involve FMF, FMS, or IMET. Such is the case in Africa, where FMF and FMS cases are comparatively small or limited, or the partner nations are acquiring equipment elsewhere but are looking to the United States for training and leader development. FAOs find themselves serving integrative functions, helping partners to align existing or newly

The Defense Attaché Function

The defined roles that U.S. military attachés perform for the Ambassador have changed little since the U.S. Defense Attaché System was centralized under the Defense Intelligence Agency (DIA) in 1965. The current arrangement was established with the intent of standardizing the observance and reporting of politico-military issues regarding the host country. In addition, attachés serve protocol functions and represent their respective Services at official functions. Attachés from different Services were grouped into Defense Attaché Offices (DAOs) under a senior attaché and assigned to Embassies.

In the 20th century, attaché activities were still largely defined in terms of ongoing or potential military operations against Communist influence. DAO presence was generally more robust in a well-defined set of countries that were either developed strategic partners or areas of contention such as around the Korean Peninsula, Eastern Europe, or Southeast Asia. In locations with lesser priority, DAOs had limited presence.



U.S. Army (Terence Ewings)

Soldier helps Iraqi troops identify map terrain features during training exercise to improve target-locating skills

The scope and complexity of those roles, however, have increased with globalization. With today's transnational threats, such as violent extremist groups working in undergoverned areas and safe havens, the politico-military landscape is far more complex, and no nation can be ignored. Furthermore, the speed of information flow in our globalized society puts increased pressure on the attachés to keep up.

Complicating the matter is the shortage of SAOs. In countries where there is no security assistance presence, those functions are added to the attachés' already full plates. In many cases, the SAO functions overwhelm the attachés at the expense of their ordinary duties and therefore of the Ambassadors they support.

It should be noted that the recent initiative to create a Senior Defense Official in U.S. Embassies has no impact on the respective roles and functions of either the SAO or DAO. This initiative is mainly to simplify the relationship between the Ambassador and DOD presence in country by identifying the most senior military officer as responsible for all DOD matters.

The Knowledge Development Function

Another vital function FAOs perform—which is not documented or established in doctrine—is the development and dissemination of cultural intelligence. It is not a true intelligence function in the traditional military sense because it does not involve espionage and its primary purpose is not the provision of specific critical information for military plans and operations. Rather, it is the result of gathering information and understanding the total sociocultural environment, of which the military is but a component, so the effects and risks of U.S. military activities on that environment, including security force assistance efforts, can be better understood.

Since *cultural intelligence* can be a confusing term, this article instead refers to its collection process, known as *knowledge development* (KD). KD is an enduring function that seeks to capture and model the sociocultural and political processes that are active at steady state and how they respond to various stimuli or crises. The differences between KD and intelligence are easily demonstrated using the phases of joint campaign plans.

During phase zero, intelligence-gathering ultimately seeks to differentiate actual and potential adversarial, friendly, and neutral elements along with their tactics and decisionmaking processes in order to facilitate effective U.S. and coalition military operations. KD's holistic understanding provides a modeling of the sociocultural systems as a whole, especially noncombatant behaviors, to better illustrate how U.S. military posture or

the speed of information flow in our globalized society puts increased pressure on the attachés to keep up

activities could be perceived. They overlap, and ultimately both serve to provide information that can help influence these elements in order to avoid conflict altogether and seek peaceful resolution of disputes, to disadvantage adversarial forces should conflict occur, and to enhance force protection.

Knowledge development has tremendous added utility in the development and conduct

of civil-military operations and activities that directly reach the populace. One example is the Medical Civil Action Program (MEDCAP) that provides U.S. military doctors to treat patients from partner countries. MEDCAPs have great immediate impact both in training for the doctors and in improving the health of the patients. However, the long-term results can be counterproductive if the program is conducted in ways that cause dependence on care not available after the doctors leave or if it encourages unhealthy behaviors. KD helps explain the underlying sociocultural influences so such risks can be mitigated. Similarly, it is helpful in addressing the impacts of humanitarian and disaster relief efforts. It also provides a lens through which the nondefense aspects of security—police forces, customs offices, border patrols, and judiciaries—can be included in the total operating context.

Knowledge development is a more suitable process for understanding the roles played by nontraditional partners, such as humanitarian assistance organizations and nongovernmental organizations. These groups often operate among remote populations and have important insights that might not be available through traditional intelligence means. Often, these groups eschew contact with militaries or intelligence agencies, so working with them is generally a sensitive process.

As operations are conducted during phase one through phase three and intelligence processes focus on fixing and defeating the enemy, KD helps us understand the impacts on the civilian population and the conditions that need to be set for postconflict stabilization. Once operations are concluded, KD is vital in the development, implementation, and assessment of phase four activities, which include peacekeeping and ensuring conditions that prevent the resumption of hostilities.

Knowledge development is not a joint doctrinal concept and is not declared in any FAO's duty description, but it is an inherent part of his or her responsibilities. The modern joint security environment simply no longer recognizes a distinction between defense and nondefense aspects, and combatants and noncombatants will continue to be intertwined. As winning the war is increasingly about winning the peace, insights from FAOs—as DOD's only boots on the ground in many countries—become more vital, particularly in places where the United States has a limited history.

There is a precedent for creating a KD function within a combatant command. During the planning for the creation of U.S. Africa Command, it was recognized that the overall joint corporate knowledge base for Africa was lacking. The remedy was to create a Knowledge Development Division (KDD) in the headquarters staff. The KDD seeks out information on the sociocultural environment to help support the command's efforts at

*knowledge development
is not declared in any
FAO's duty description, but it
is an inherent part of his or
her responsibilities*

building and sustaining long-term military-to-military relationships, identify and formalize security force assistance requirements of partner nations, and develop effective and tailored programs to serve partner needs while adding to our understanding of the engagement environment and supporting U.S. foreign policy objectives.

Some elements contributing to the KDD have been the Socio-Cultural Research and Analysis Teams (SCRATs), consisting primarily of Africa experts from academia. SCRATs routinely travel around the continent to gather a comprehensive understanding of the socio-cultural environment. They have considerable ground to cover and should best be used as targeted complements to FAOs who are already knowledgeable on an area. Africa is broad, dynamic, and complex, comprising 53 nations with unique histories, 800 ethnic groups speaking over 1,000 languages, and a population of a billion, which some expect to double over the next 40 years. Many of Africa's security challenges, such as violent extremist organizations, trafficking, insurgencies, and piracy, are elusive, and its infrastructure and information-gathering and -sharing capabilities are limited. Equally important is understanding the interrelationships of the various groups in country, so the second- and third-order effects of U.S. security force assistance are understood, and we can ensure they are conducted in ways comfortable to partner nations.

Current State and Recommendations

It is unfortunate that this community of practitioners—so vital to our ability to prevent conflict and, if needed, set conditions for

victory—gets so little priority. The state of our FAO community is not what it should be, and that needs to be fixed.

Realign FAO Roles in Security Assistance. The demand-driven, program-based approach has caused SAOs to concentrate primarily on the training and materiel elements of the doctrine, organization, training, materiel, leadership and education, personnel, and facilities (DOTMLPF) spectrum. True partner capacity-building demands an equal concentration across all elements, just as it does in fielding new weapons systems or conducting organizational structure changes in the U.S. military. More than ever, DOTMLPF analysis is a function performed at forward locations on a continual basis, and FAOs are the primary practitioners.

Increase FAO Accessions. Even against the original program-driven requirements, the FAO community is underresourced and has been for some time, yet we, the joint community, are in denial. While highlighting a number of Service initiatives that sought to increase FAO accessions and improve their use, the most recent *DOD 2009 Annual Foreign Area Officer Report* still noted two fundamental problems: too few qualified FAOs to satisfy the demand, and inability to meet language proficiency requirements.³ Yet the tone of the report is positive and appears to promote the Service initiatives as the path to ultimate success.

But these initiatives will not be enough. The overall FAO fill rate in combatant command headquarters and the Joint Staff decreased from 92 percent in fiscal year (FY) 2008 to 87 percent in FY 2009, and that was against validated positions programmed through the Services and DSCA in accordance with a program-driven requirements model. These do not account for all articulated requirements of the commands, nor do they account for the functions that FAOs currently perform.

For example, U.S. Africa Command has an identified requirement for new OSCs in several partner nations, but due to programmatic limits, these have been spread out over several years and thus are not counted in the total number of FY09 requirements. Furthermore, there are several cases in Africa where the situation may dictate the need to surge a security assistance presence to a nation with which U.S. policy shifts may cause the issuance of direction for the military to engage immediately. This has occurred in instances where a

coup or other political situation was resolved in ways that caused U.S. policymakers to initiate or renew bilateral relations, with military engagement as a core element. Surging people with no experience in Africa may be counterproductive, thus necessitating a readily deployable pool of experienced FAOs within the Services.

Accessions into the FAO program should not be a problem. Indeed, the DOD report highlights the fact that far more candidates apply than there are positions. While some might screen out regardless because of mismatches in skills and aptitude, there would be no shortage of work for those officers.

Extend FAO-like Program to the Non-commissioned Officer Corps. There is a legitimate question as to why the domain of practitioners is limited to the officer corps, mainly in the field grades. While field-grade officers are well suited to cultivating relationships with midgrade and senior partner nation military leaders, they might not always be the best for conducting KD or managing security force assistance at the tactical and operational levels. Beginning with our supporting efforts in Central and Eastern Europe after the Cold War, we found that relationships among noncommissioned officers (NCOs) were effective at bringing about attitudes and behavior leading to a more capable partner force. The relationships bring perspectives, and therefore sometimes intelligence, that might not ordinarily be made available to officers.

Unfortunately, NCOs currently working in Embassies perform mainly administrative and budget work and rarely interact with partner nation militaries. This is a missed opportunity. Today's U.S. NCO corps is rife with fresh experience in partnership and engagement activities in operational theaters and would excel at performing roles and functions that are appropriately aligned with those of SAOs and DAOs. There is certainly nothing inherent in the FAO education program to suggest that NCOs could not participate, graduate, and use similar skills to further U.S. security interests.

One attractive proposal is to create a Foreign Area Leader (FAL) program that provides similar FAO training and education opportunities to selected senior NCOs for future service in Country Teams and command headquarters. The advantages of incorporating FALs is the long-term expansion of the pool of cultural talent in the joint force and the increased ability for NCOs to relate to partner NCO corps, particular those



U.S. Marine Corps (Alicia R. Giron)

Colombian marines line up for nonlethal weapons class as part of subject matter expert exchange with U.S. military

undergoing professionalization efforts. A potential short-term avenue of approach is to employ current Civil Affairs NCOs in FAL capacities, which would increase their knowledge and ease coordination. However, the goal would be to recruit high-quality NCOs from all Military Occupational Specialties, especially combat and combat support, where the

in particular is highly sought for helping train deploying forces, and few outside of the FAO community receive as much practical experience in interagency integration, which is vital in postconflict stabilization operations.

Too many FAOs are merely shuttled between jobs in Embassies. Others alternate assignments as staff officers in geographic

there is nothing inherent in the FAO education program to suggest that NCOs could not participate, graduate, and use similar skills

ability to interact with partner NCOs would be enhanced. DSCA and Service response to the idea was encouraging, and steps to develop the idea further are being taken, but this needs to be accelerated as the requirements for FALs are present today and will only increase.

Fix the FAO Career Path and Utilization. Although the FAO community draws the best and the brightest from the Services, too many wind up being overworked and underappreciated. FAO communities are segregated too far from the mainstream of their respective Services. While their contributions to making strategy and informing policy are well known, the skills and experience they bring have tremendous utility and relevance to the Services as a whole through assignments with troops, serving as military instructors, or preparing doctrine. Knowledge development

combatant commands, joint staffs, or other higher headquarters but do not get to utilize their FAO skills for the betterment of the Service. Instead, the FAO time is looked upon as an aberration to be discounted. The DOD report demonstrates this with promotion rates to lieutenant colonel and commander, as well as colonel and captain, consistently below the Service averages over the past 4 years. In particular, the Navy's FAO promotion rate to these ranks was about half of the overall selection rates, with the Air Force and Army rates remaining generally low.

Notably, FAO communities do not feed the Services' flag officer corps, which is surprising given that two-star flag officers serve as chiefs of OSCs to important strategic partners such as Egypt, Turkey, Saudi Arabia, Russia, and now the Middle East and Central



INSS Strategic Perspectives 2

Chief of Mission Authority as a Model for National Security Integration

by Christopher J. Lamb and Edward Marks

The U.S. Government lacks the ability to effectively integrate the efforts of its departments and agencies—civilian and military—on priority missions, such as the operations in Afghanistan. To achieve this unity of effort, Presidents have tried various approaches such as National Security Council committees, “lead agencies,” and “czars,” but none has been effective. The authors examine one precedent of a relatively successful cross-agency executive authority that already exists: the Chief of Mission authority delegated to U.S. resident Ambassadors. Building on this precedent, the authors make a case in favor of legislation giving the President authority to delegate his integration authority to “Mission Managers.” They examine in detail how to implement this authority, concluding that while such reform would be politically challenging, there are no insuperable legal or organizational obstacles to it.

Visit the NDU Press Web site
for more information on publications
at ndupress.ndu.edu

Asia. Instead, with limited opportunities before them, a number of highly intelligent, motivated, and superbly performing FAOs are forced to retire earlier than necessary, at a time when the demands for experienced FAOs are increasing.

Fixing these problems should require only minor adjustments as long as the accession problem is also addressed. Given widespread recognition of the requirements that FAOs are well suited to satisfy, it should be straightforward to expand the slate of positions within the professional military education, doctrine, and general purpose forces where FAO skills can be listed as required or desired. Broader exposure and opportunities to demonstrate value added beyond the current limited FAO utilization path also bring about improvements in promotion rates. Additionally, promotion boards should be encouraged to recognize and promote categories of FAOs such as those who have already been assessed as high performers operating in difficult environments.

Improve Sustainment Training for FAOs. From an educational standpoint, FAOs are too often treated as “fire and forget.” They rarely receive any sustainment or follow-on education after their 2-year accession program. The Naval Postgraduate School recognized this situation and began instituting a 2-week pilot program to give FAOs a chance to get together, reflect on their experiences, and give back to the schoolhouse. Initiatives such as these need to be encouraged more widely.

Ultimately, it falls upon the FAO community to serve as an important conduit between the Department of State, through its U.S. missions abroad, and the Department of Defense. FAOs perform a great service that adds value to unified action in support of U.S. foreign policy objectives and national security interests alike. We must stop channeling them so narrowly that we miss opportunities to bring their special talents to bear for the U.S. military as a whole. The doctrine, education, and utilization of FAOs performing the roles of security assistance officer, military attaché, and especially knowledge developer must be reviewed and updated. FAO requirements need to reflect this doctrine and be accessed and utilized according to where their skills and education can add value anywhere in the U.S. military, and not be channeled within a narrow set of positions that ultimately insulates them from the force. **JFQ**

For their contributions to this article, the author thanks Colonel Thomas P. Galvin, USA; Lieutenant Colonel Christopher Varhola, USAR; Lieutenant Colonel Laura Varhola, USA; and Command Sergeant Major Mark S. Ripka, USA.

NOTES

¹ Robert M. Gates, “Helping Others Defend Themselves: The Future of U.S. Security Assistance,” *Foreign Affairs* (May–June 2010), 2–6.

² Also known as Offices of Defense Cooperation in Europe and Offices of Military Cooperation in Kuwait and Egypt.

³ Department of Defense (DOD), *DOD 2009 Annual Foreign Area Officer Report* (Washington, DC: DOD, August 2, 2010), 2.

A SMARTER FORCE

for Less Time and Money

By STEPHEN D. POMPER

U.S. Navy (Chad J. McNeely)



Admiral Mullen poses with Navy ROTC students after speaking at Harvard University

DOD (Cherrie Cullen)



Secretary Gates speaks to students, faculty, and ROTC cadets on achievements of all-volunteer military force

The last good idea I had was a duffle bag that opens on both ends—that was 23 years ago when I was a Cadet. Maybe I should have capitalized on the thought, but then I might not have found myself back in the Reserve Officers' Training Corps (ROTC) and U.S. Army Cadet Command as a professor of military science, which led me to another great idea. This one would educate our officer corps and save money and time for the Department of Defense (DOD), and will likely be received by Cadets and Midshipmen as a lucrative incentive (and even promote enrollment).

As we know, conditions change rapidly on the battlefield, in the air, and at sea, but not so rapidly in academia. In the past several years, more and more colleges and universities are offering 5-year master's degree programs. The students are accepted late in their sophomore or early in their junior year; they complete the associated undergraduate degree work, simultaneously begin master's work in the fourth year, and are conferred with a graduate degree in the fifth (sometimes both on the same day).

I am not certain of the motivation for such programs, and they differ greatly; but neither am I convinced that it is solely based on providing students with a "good deal." The benefit to the university is ensuring select stu-

dents complete their matriculation (first) and then "locking" them in for at least another year. Since students can apply to any advanced program after graduation, this allows the university some additional assurance of people and tuition. Still, it is a good deal financially, and DOD should capitalize on it.

Great idea: *Allow ROTC Cadets/Midshipmen to participate in 5-year advanced degree programs.* The precedent is already set in educational delay programs for doctors, lawyers, and clergy. There already exist provisions that allow for certain undergraduate programs that take 5 years as well. A more educated force today and tomorrow is the greatest advantage of this proposal. We gain a second lieutenant or ensign with an advanced degree. That means something everywhere else; it should for the U.S. military as well. Knowledge is a force multiplier, and we already ask so much of our junior officers; the result would equate to improved mission accomplishment and expanded officer education. There is no need to wait for DOD Directive 1322.10, whose goal is to "[d]evelop or enhance the capacity of the Department of Defense to fulfill a present need, anticipated requirement, or future capability."¹ Still, DOD directives such as this are derived from law.

Lieutenant Colonel Stephen D. Pomper, USA, is a U.S. Cavalryman in the Army Reserve Officers' Training Corps and is the Professor of Military Science at The Johns Hopkins University.

The U.S. Code is what needs to be changed if we truly want a smarter force for less time and money.

The proposed educational advantage is also exponential. With an available and larger pool of advanced degree holders, those selected for Advanced Civil Education (ACE)² can use that period to gain doctoral degrees. Some would argue against this (it is true), but our profession is more than worthy. At least that is what we tell ourselves. And one would not need to wait to be a colonel, captain, or flag officer to use this expert knowledge. There is no reason for ACE or other Service equivalents to go away. These programs also tend to direct the education at some specific Service need (for example, the academies need teaching-certified officers), whereas this idea would increase education and have a broad effect.

The second advantage is simply a better use of an officer's career timeline, and the entire DOD benefits from it. The upfront time saving is obviously the year less that it takes to gain a degree (most of them). Then, consider that the precommissioned person has never been part of the operational side and therefore is not missed (versus 2 years in school and the associated and potential utilization assignments). Accessions forecasting and diligence would ensure that they are not missed as second lieutenants or ensigns.

it is not inexpensive to send an officer to graduate programs, and hence we do not do it nearly as often as we should

Until the personnel gurus can deliver an alternative to the 20-year retirement Catch-22, this idea could act as a partial bridge on the officer education front. A hurdle would be the sheer amount of time that doctoral candidates need (although some of this "need" is actually "want"). Then there is the caliber of officers selected. This program would be merit based, and therefore only the brightest would be selected. This begins at the institution, which we should rightly assume is best qualified to make this determination (from among sophomores or juniors).

Then there is advantage three: money. I am not saving the best for last, since I led with that, but at a time when the Secretary of Defense is calling for billions in savings, every bit counts. It is not inexpensive to send an officer to graduate programs, and hence we do not do it nearly as often as we should. There are the moving costs, the tuition and fees, and the officer's salary (the most expensive part even if he or she attended the Massachusetts Institute of Technology or an Ivy League school). I am sure an economist could calculate the financial loss of officers'

professional judgment and, of course, their directed mission to produce qualified officers for their Service, and on time. In some exceptional cases, students even complete their undergraduate work early. (I know one brilliant young man who could get his undergraduate and master's degrees in only 4 years.) Does this create some "have" and "have not" schism? Yes, and one clearly in line with existing merit-based lists used by every Service. Students who qualify for this should already be considered for unique positions in the Services. Currently, they are lumped in a

that we educate Cadets and Midshipmen must begin with the law establishing ROTC. Then a larger and more holistic approach to pre-commissioning education, both military and academic, could be championed. Still, ROTC "ain't broke," but there are certainly more efficiencies and good ideas that could be born from a more progressive law. The alternative is literally ignorance. **JFQ**

NOTES

¹ Under Secretary of Defense for Personnel and Readiness, Department of Defense (DOD) Directive No. 1322.10, "Policy on Graduate Education for Military Officers," April 29, 2008, available at <www.dtic.mil/whs/directives/corresp/pdf/132210p.pdf>.

² Formally known as Advanced Civilian Schooling and the Air Force Institute of Technology Civilian Institution Programs.

³ DOD Directive 1322.10.

a change to the law would demonstrate the importance of education in the military and would go a long way in reversing some (incorrect) perceptions of a knuckle-dragging military

"un-utilization" while they are learning as well as the gain when they return (the idea proposed here is all gain). Again, that is 2-plus years away from the fight. Whole operational fronts change in this time, and we are consistently reminded of the persistent nature of our enemy and mission.

A short but dedicated study could determine the best means to calculate some duty Service obligation—if one is needed at all. The fifth year could be paid for by DOD, or not. Based on my experience, students would gladly incur this expense for the lifelong benefit it provides. And if they cannot afford it, the military should be ready to offer scholarships in return for some obligation.

DOD Directive 1322.10 addresses serving officers only: "Raise professional and technical competency, and develop the future capabilities of military officers to more effectively perform their required duties and carry out their assigned responsibilities."³ A good idea indeed, but a bit limited in scope. My idea is that ROTC Cadets and Midshipmen be afforded a similar opportunity, with the notion that everything they do in their Service can benefit from "competency." The results will surely "[p]rovide developmental incentives for military officers with the ability, dedication, and capacity for professional growth."

Is this idea for every young precommissioned person? No. Institutions already limit enrollment in such programs for obvious reasons. Professors of military and naval science and aerospace studies can further discriminate eligible students based on their

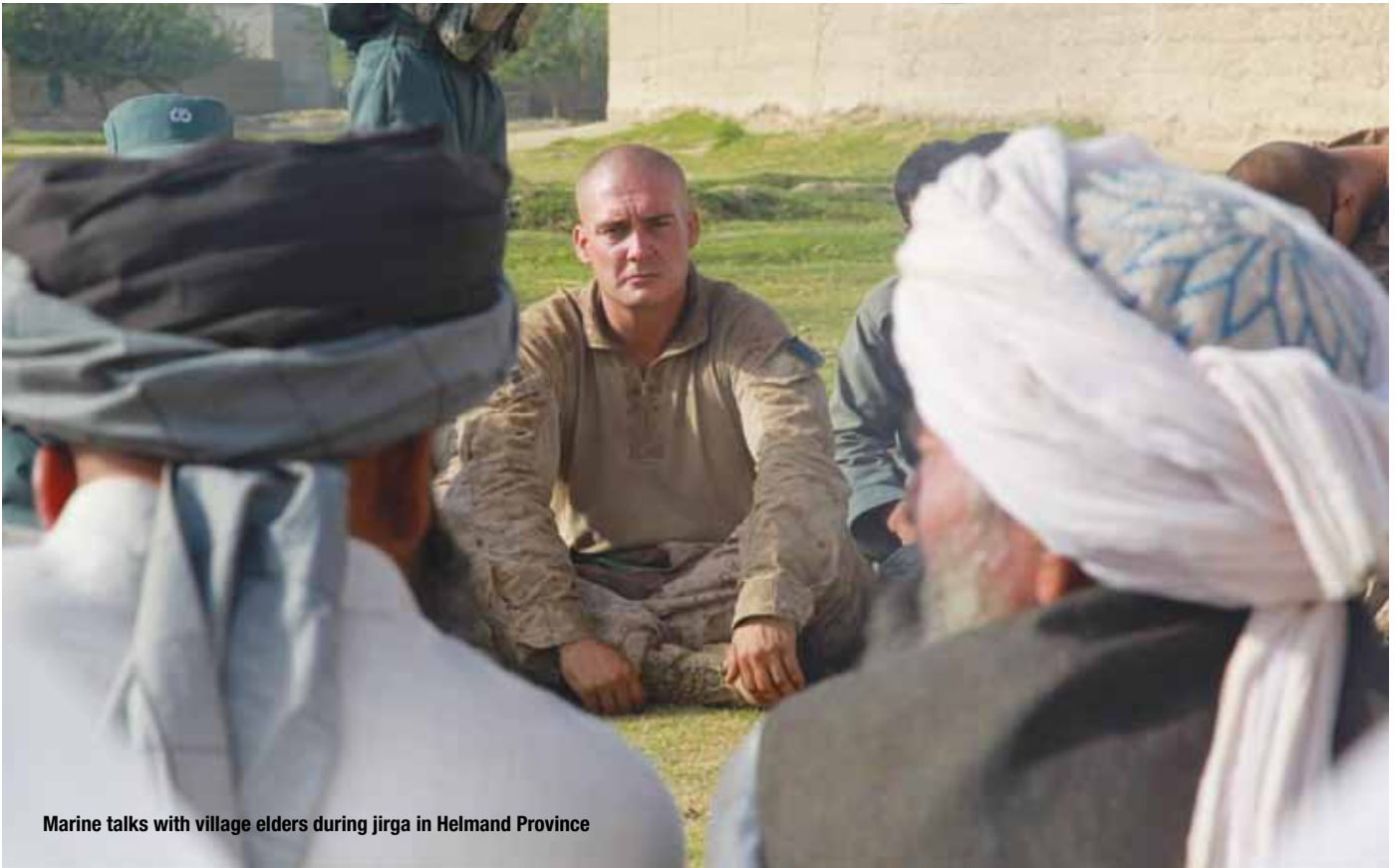
cohort of "qualified," and years might go by until they can prove their academic prowess (if they are still in the Service). A change to the law would demonstrate the importance of education in the military and would go a long way in reversing some (incorrect) perceptions of a knuckle-dragging military. Allowing our future leaders the opportunity to excel in these programs would say a lot, even if the number would be small.

I am not certain how to change DOD policy or what discretion the Services have in executing it. Any modifications to the way



Midshipman mans simulated bridge of USS Freedom during summer training on navigating harbors

U.S. Navy (Daniel J. Taylor)



Marine talks with village elders during jirga in Helmand Province

Building Credible Voices

Traditional Communication in Afghanistan

By ROBERT M. HILL

A respected Afghan religious and legal scholar who was partnering with the International Security Assistance Force (ISAF) related why he had decided to work alongside the force. He did so through a story, which reinforced the power of narrative among Eastern cultures and demonstrated why authentic “credible voices” such as his are among the most powerful channels to reach the Afghan people.

The scholar spoke of a recent trip to the United States—his first—in the company of other colleagues from Afghanistan. While waiting for a delayed connecting flight at John F. Kennedy International Airport, he realized it was prayer time. The crowded terminal was

not conducive to the practicalities of Islamic prayer. He scanned the gate area and noticed a small space in a corner, not far from a television monitor broadcasting the news. He spoke to his colleagues and reminded them of their obligation, but they demurred, pointing out the crowded room and remarking that their religious act might seem intrusive and unwelcome. Not unlike Christians who shy away from saying grace in public, their excuses masked fear and embarrassment at expressing their faith overtly. The storyteller understood and left his colleagues alone. He, however,

decided to pray despite his own trepidations. He made his way to the corner of the air terminal and went about the ritual of *salat*.

What happened next surprised him. He expected strange or disapproving stares, possibly even taunts. Instead, parents pulled back their children to give him more space, someone moved to the television and turned down the volume, and the entire room grew quiet in respect. Seeing this, his colleagues overcame their fears and joined him. He had come to the United States believing that it was intolerant of Muslims, particularly in the

Dr. Robert M. Hill is Deputy of Leader Development, Education, and Training in the U.S. Army Combined Arms Center Information Proponent Office at Fort Leavenworth. He served on the Deputy Chief of Staff Communication Staff, International Security Assistance Force, from July 2009 to July 2010.

aftermath of 9/11. He left with a deeper appreciation of American acceptance of others and a reaffirmation of the danger of uninformed perceptions and stereotypes.

When he and his colleagues returned to Afghanistan, each told this story to a wide range of friends, colleagues, and acquaintances, who in turn repeated it to others. Because of their stature in their communities, their story and its message were deemed both credible and meaningful. When some of them subsequently chose to work with ISAF on its efforts to reach the Afghan people more effectively, their decision was respected by those who might earlier have questioned it. The event itself affected only a handful of Afghan religious scholars, but their recounting of it touched hundreds. Such is the power of what ISAF has come to term *traditional communication*.

Traditional communication is organic. The notion of formalizing it into a process risks losing that organic quality. Yet not employing it to reach local populaces is to lose a potent tool in the communication kitbag. The purpose of this article is to explain the ISAF Traditional Communication (TRADCOM) program and the ways in which it has dramatically enhanced our ability to reach the Afghan people with messages that matter—to them and to us.

Genesis

In some ways, TRADCOM is a misnomer because the term seems to be strictly about communication when, in fact, it is about relationships. In Western societies, by and large, there is an emphasis on effect, on ensuring that a message is conveyed, received, and understood whether we have a relationship with the recipient or not (although we intuitively recognize that established relationships foster more effective communication). In Eastern societies, the message becomes meaningful—that is, it achieves its effect—*after* a relationship is established with the recipient. More simply, the difference in approach may be characterized as *transactional* (Western) versus *relational* (Eastern). These differences are influenced by the degree to which East and West value individualism versus collectivism.¹

In Eastern societies, given their emphasis on collective behavior, relationships are rarely informal. They are governed by culture and tradition, such as the respect yielded to tribal and religious elders. If no codified scheme of relationship exists, then—as Greg



U.S. Air Force (Daryl Kneel)

Muslims gather at worship site at Kandahar Airfield to pray before Eid al-Adha holiday

Mortenson and David Oliver Relin make clear in *Three Cups of Tea*—it must be cultivated and formalized through a succession of interactions. Only then can formalized, meaningful, and actionable communication occur—because only then is the recipient willing to receive the message.²

in Eastern societies, the message becomes meaningful after a relationship is established with the recipient

In Afghan culture, the nexus of relationship and communication is fundamentally rooted in the concepts of respect and honor. A transactional relationship is a matter of business; a personal relationship is one of honor. Once a personal relationship is established, guided as it will be by tradition, honor demands full commitment to the relationship and the object of the relationship. When one side speaks to another and asks for something, the other side is bound by honor to oblige. While new technologies such as the Internet and text messaging are beginning to change this dynamic, it remains largely intact in Afghan culture and will be for years to come.

A legitimate question arises: Why is ISAF only now tapping into traditional communication networks to reach the populace? It is a question that we asked ourselves as we

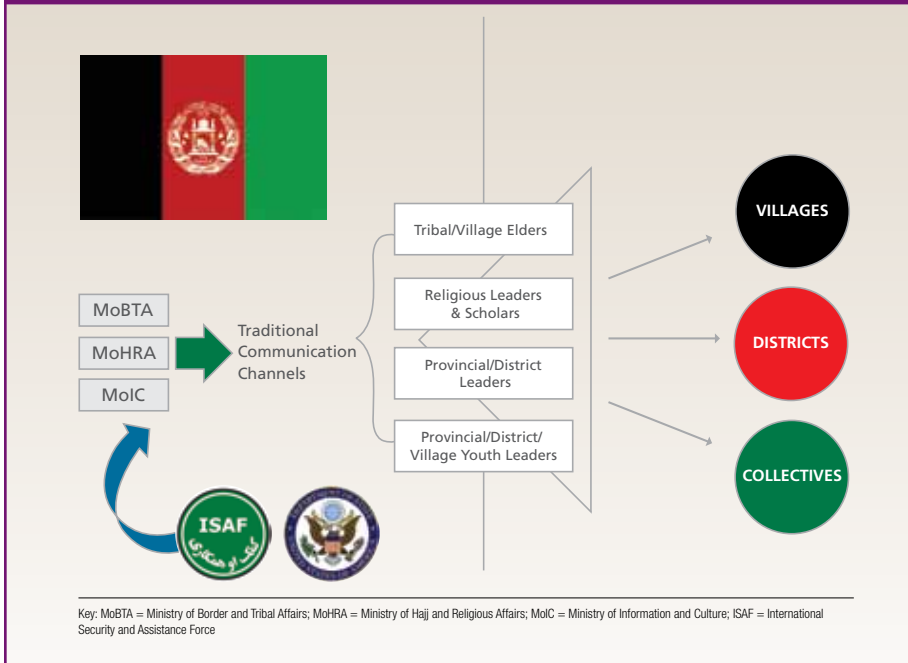
undertook the strategic assessment in the summer of 2009. Reviewing the international community's efforts in Afghanistan over the past 8 years, we came to the following conclusions:

- we had previously reached out almost exclusively to the Afghan elite or Afghan government
- we focused on killing insurgents rather than protecting the people; the latter process, by its nature, demands engagement with an open hand, not a clenched fist
- we defaulted to our own cultural mores and habits and projected them onto the Afghan people
- we overrelied on technology and mass communication to reach a culture still rooted in face-to-face, word-of-mouth communication.

Perhaps, too, we considered traditional communication something the insurgency did (and well), which we had to counter with more sophisticated methods. In short, we failed to view communication through the lens of counterinsurgency (COIN), which doctrinally forces us to immerse ourselves in and among the population, all the while recognizing the disadvantage our “otherness” creates.

Ironically enough, the Afghan government faced similar challenges. It was, and remains, Kabul-centric and largely out of touch with the common citizen. An entirely

Figure 1. Communication Channels Connecting the Afghan Government to the People



separate article could be written on Afghanistan's realpolitik and the tension that exists between local and national instruments of governance. Suffice it to say that most Afghans do not view the national government as worthy of their allegiance, often placing two COIN principles at odds: protecting the people and putting the government in the lead.³

Overcoming this impasse necessitated giving the Afghan government and ISAF access to and influence over credible voices at the local level. Out of this realization grew the ISAF TRADCOM effort, the mission of which is to “enable the [Afghan government], through partnership, to empower credible Afghan voices in promoting the benefits of development, the legitimacy of [the government], the disadvantages of the insurgency, and community responsibility for a better Afghan future.” Figure 1 captures the essence of the program, which seeks to bridge the Afghan government to the people.

ISAF has been criticized for using terms or phrases such as *partnership* and *put an Afghan face on it* to characterize operations and activities that are only cursorily Afghan-led. But in the complex environment that is Afghanistan, with its nascent, immature, and often dysfunctional central government, *saying it is so* is a necessary first step to *making it so*. TRADCOM provides a way for

voices of credibility to amplify the “saying it is so” step and, in due course, guide more positive, productive, and enduring outcomes.

ISAF's TRADCOM program works with three vital ministries: the Ministry of Border and Tribal Affairs (MoBTA), the Ministry of Hajj and Religious Affairs (MoHRA), and the Ministry of Information and Culture (MoIC), which, with funding and administrative support from ISAF and the international community, take the lead in organizing and conducting a series of shuras, jirgas, and religious seminars designed to encourage and cultivate credible and responsible voices that serve as a potent counterpoint to insurgent propaganda.

In many ways, TRADCOM is a unique kind of influence that is based primarily on relationships rather than on radio broadcasts, television commercials, leaflets, pamphlets, and billboards. It seeks to influence people through personal, trusted channels of communication. These relationships make this kind of influence powerful and lasting.

Theoretical Roots

All human experience is fundamentally rooted in narrative.⁴ Counterinsurgency might just as readily be characterized as counternarrative, where success depends on offering the populace an alternative storyline to the one being promulgated by the insurgency. The notion of full-spectrum operations

is predicated on the realization, sometimes underappreciated, that all actions speak, while all speaking affects subsequent action.

We often think of storytelling as an exercise of the creative imagination, but it is also fundamental to making sense of our existence. Put another way, we must use our imaginations to create narratives that structure and give meaning to “equivocal inputs.”⁵ Meaning has to be forcibly hewn out of the “undifferentiated flux of raw experience and conceptually fixed and labeled so that [it] can become the common currency for communicational exchanges.”⁶

The stories we create to make sense of things answer two basic questions:

*In the context of everyday life, when people confront something unintelligible and ask, “what’s the story here?” their question has the force of bringing an event into existence. When they then ask, “now what should I do?” this added question has the force of bringing meaning into existence, and they hope that the meaning is stable enough for them to act into the future, to continue to act, and to have the sense that they remain in touch with the continuing flow of experience.*⁷

Sensemaking through narrative is both individual and collective, but since so much of our existence is spent in community, sensemaking, of necessity, is collaborative. There are pros and cons to both approaches. Singular sensemaking provides only one frame of reference with which to answer the two questions posed above. Multifaceted sensemaking has the potential not only for more inputs, and thus a more probable picture of what is going on and what it might mean, but also for conflict and indecision. This is where sensegiving can help. *Sensegiving* is “a sensemaking variant undertaken to create meanings for a target audience.”⁸ The value of sensegiving is that it can ground and give direction to sense-makers in their struggle to shape meaning.

The West's fascination with i-everything (iPods, iPads, iPhones) has heightened the challenge of sensemaking by dramatically increasing the amount of information to be sorted through, while simultaneously providing high-tech tools to process, prioritize, visualize, and decipher this information. Afghanistan, in stark contrast, is still deeply rooted in the oral/aural tradition of sensemaking through one-on-one conversations and/or group dialogue and storytelling. Sensegiving

is primarily the task of tribal elders and religious leaders, although there remains space for other and younger voices and narratives to impinge on the sensemaking process. In this space, TRADCOM is gaining a foothold.

Sensemaking “is not about truth and getting it right. Instead, it is about continued redrafting of an emerging story so that it becomes more comprehensive, incorporates more of the observed data, and is more resilient in the face of criticism.” Moreover, “people may get better stories, but they will

and trust.” TRADCOM’s goal is to link the Afghan government with the populace at all levels by fostering trust among representatives of the MoBTA, MoHRA, MoIC, and tribal, religious, and youth leaders and/or elders at both provincial and district levels. At the same time, it seeks to empower local and regional leaders so they believe they can reach upward to their government and be heard. One disadvantage of trust-based communication is that it can become myopic. This potential pitfall is avoided or overcome by

where the program operates in order to know who the key influencers (sensegivers) are, both formal and informal. In Afghanistan or any other heterogeneous culture, what works in Paktiya will not work in Kunduz or Helmand. Most important of all, cultural context recognizes that indigenous channels are by far the most effective for conveying messages. In the past, we developed the messages from our own cultural perspective and simply translated them from English into Pashto and/or Dari. Invariably, something got lost in translation. Today, we focus on the campaign and theme level, letting the indigenous sensegivers frame the messages through their own cultural lens and deliver them through their own means.

success depends on offering the populace an alternative storyline to the one being promulgated by the insurgency

never get *the* story.”⁹ Human nature makes us prone to *think* we have the full story, to settle somewhere on the path to absolute truth and accuracy or else feel the unease of indeterminacy. John Milton, in *Areopagitica*, uses the metaphor of “pitching our tent here” to signal man’s tendency to think he has discerned *the* truth when in fact he is always far short of it.¹⁰ What TRADCOM seeks to ensure is that this “tent pitching” is influenced by moderate and responsible voices and is situated well away from insurgent voices and toward that of the Afghan government. It achieves this aim by reaching out to and then through indigenous sensegivers, namely tribal elders and religious leaders such as *ulema* (independent religious scholars) and mullahs.

Guiding Principles

While these guiding principles arise from the specific and unique environment of the Afghanistan-Pakistan region, they can just as readily apply to any region in which U.S. forces might find themselves. The key to success is discovering the underlying wisdom of the land and its people and to employ historic processes, practices, and cultural norms to reinforce and expand responsible rhetoric and behaviors. The outgrowth of this inside-out approach is enduring change.

Centers on Relationships. TRADCOM is as much about relationships as it is about communication; one cannot be separated from the other. If sensemaking is a process of shared conversing and understanding, then relational sensemaking places premium value on the object or objects of these conversations. It is as if to say, “I want to make meaning but only with those I truly know

encouraging wider circles of trusted agents so local leaders feel comfortable being engaged by and engaging with the government and ISAF representatives.

Culturally Attuned. TRADCOM works with and, in fact, leverages indigenous cultural traditions and, in so doing, gains traction in ways that more modern, progressive, and Western strategies do not. Success requires that those executing TRADCOM become immersed in local customs, beliefs, and ways of communicating so they optimize opportunities to build understanding and cooperation while mitigating insensitivities and mistrust. Success also relies on mapping the human networks within each local area

Leverages Embedded Cultural Processes. The primary means by which the MoBTA, MoHRA, and MoIC connect with the populace are such venues as jirgas, shuras, and religious seminars or events. Jirgas and shuras are nearly synonymous. Jirgas come out of Pashtun culture and serve as a mechanism for conflict resolution. Shuras also settle disputes but often are more advisory in function. Religious seminars are collective gatherings focused on achieving common understanding of Koranic texts. All should be viewed as instruments of governance that are deeply embedded in Afghanistan’s culture and history; they should be respected as such and not viewed as simply another delivery platform for our messaging.



Muslims working with ISAF in Afghanistan attend Eid al-Adha prayers at Camp Leatherneck, Helmand Province

Royal Air Force



District governor speaks to village elders during shura in Zabul Province

Demonstrates Respect and Trust. We are prone to overuse the phrase “winning hearts and minds.” Such phraseology connotes a level of control we wish to avoid. The value of TRADCOM is its inherent goal of mutually empowering the government and Afghan people while ISAF stays well in the background. The greatest respect we can demonstrate to our partners is to allow their historic patterns of communication and grievance resolution to enact themselves with just enough of a nudge from us to gain traction. When we respect their traditions and actively cultivate their occurrence, we are perceived as genuine about our commitments to honor Afghan ways—political, social, and religious.

Consultative, Not Dictatorial. A direct consequence of respecting Afghan communicators and ways of communicating is the ability to adopt a more consultative posture in our relationships and transactions. The opposite also proves true: the more consultative we are from the outset, the more we demonstrate and therefore engender respect. A consultative approach takes time and patience. The advantage of being dictatorial is that we can set both the agenda and timeline for action to occur.

Being consultative means allowing relational dynamics time to play out; invariably, those we consult with will need to consult with their own circle before finalizing a decision.

Expects and Accepts Reasonable Risk. Developing trusted partners means that sometimes we may interact with someone who will prove untrustworthy. Small setbacks are to be expected and even have the benefit of making malign actors transparent so they can be marginalized or circumvented. And it is possible to mitigate this risk by leveraging the relational dynamics at the heart of collectivist societies. Once we have identified trusted partners, we can turn to them to identify other trusted partners and influencers, and so on.

Vignette: The Tsamkani Jirga

In early June 2010, Afghanistan held the National Consultative Peace Jirga (NCPJ) to find consensus on ways to achieve lasting peace in the country and region. Over 1,600 delegates attended the 3-day event and developed a 16-point resolution that articulated specific recommendations for achieving peace, ranging from freeing prisoners who

were being detained on inaccurate or unsubstantiated charges to a commitment on the part of participants to act as messengers of peace within their communities. The event drew praise from the international community but some skeptics worried that the NCPJ would go the way of previous such events, offering meaningful rhetoric and great promise but little substantive action.

The NCPJ framed national-level aspirations but no guaranteed mechanisms to convert these aspirations into either allegiance or action at the regional and local level. Operational Detachment Alpha (ODA) teams operating in Paktiya Province, in consultation with the province’s subgovernor, saw an opportunity to reinforce the outcomes of the NCPJ in their operational area by convening a jirga in the Tsamkani district on June 10, a week after the NCPJ.

The ISAF TRADCOM cell, in concert with the MoBTA, U.S. Embassy, Gardez Provincial Reconstruction Team, and ODA, rapidly planned and executed the jirga, which was attended by more than 1,500 local and provincial elders and leaders. MoBTA Deputy Minister Muhammad Yaqub Ahmadzai

represented the Afghan government at the jirga and made good on efforts to improve ties between the national government and province, especially through outreach to the province's deputy governor.

The Tsamkani jirga resulted in the release of a four-point resolution that ratified the outcomes of the NCPJ and demonstrated a tangible commitment at the provincial and district levels to advance these outcomes. The four points were:

- support for the entirety of the NCPJ resolution
- importance of protecting the territorial integrity of Afghanistan
- readiness to sit down with the opposition within the framework of the NCPJ
- commitment to carry out the decisions of the NCPJ.

In the days that followed the jirga, 20 of the 60 most influential elders in the province, including former mujahideen, were elected members of a Peace Shura. This consultative body asked its members to travel throughout the province to spread the reintegration message. At the same time, recorded messages from the jirga were being broadcast. The upshot of these efforts was the reintegration of four insurgents in the first few weeks following the event. More tellingly, the jirga and its follow-on activities resulted in a known improvised explosive device facilitator turning himself in to the ODA, saying he no longer desired to maim his country or countrymen. Within a few weeks, the Peace Shura reintegrated an influential mullah who is now working to recruit *ulema* and mullahs for a future election to expand the Peace Shura and extend its outreach via mosques, madrasas, and religious shuras. Additionally, he regularly broadcasts Koran-based messages of peace and reconciliation via radio that reach throughout Pakiya and into the surrounding provinces and Pakistan. Lastly, the elected president of the Peace Shura campaigned for the Wolesi Jirga, Afghanistan's lower house of parliament. Although he lost, his desire to serve his country and his people is clear. He continues to work with the government to advance the interests of northeastern Pakiya.

Almost 6 months later, the elders of the Peace Shura continue to meet and travel across the province. They have procured funding and intend to conduct numerous district shuras to encourage formation of local

police and to close the gap between the people and the government. The Peace Shura is also coordinating directly with TRADCOM and local ISAF commanders to foster the completion of community projects to be announced at each shura. Meanwhile, other provincial and district leaders continue to expand efforts

vate, and strengthen the appeal and impact of credible and responsible voices.

Determine Key Communicators. Credible and responsible voices exist in every community and at every level. In collectivist, relational cultures such as Afghanistan, discovering these voices involves asking

skeptics worried that the NCPJ would go the way of previous such events, offering meaningful rhetoric and great promise but little substantive action

to enact the decisions of the NCPJ and Tsamkani jirgas. Like other programs and initiatives designed to connect the government to communities, this one remains fragile and dependent on a variety of factors. The value of TRADCOM, if nothing else, is to quietly bolster government efforts to fulfill its role as provider and protector of the people.

TRADCOM in Action

The guiding principles of TRADCOM apply to all cultures, no matter how sophisticated or technologically enabled their communication, although it remains particularly relevant to COIN. The key is to study—with new eyes—the surrounding culture and pay close attention to how communication is enacted to ensure that indigenous patterns are mimicked and amplified in such a way as to produce more efficacious and enduring results.

The game plan that TRADCOM has employed consists of several tenets.

Determine Intent of Desired Dialogue.

The ultimate goal of TRADCOM is to link the national government with its constituency, the people, engendering greater trust and confidence in the ability of the government to protect and serve the population. Clearly, such efforts would not be needed if that trust and confidence already existed. Nascent governments are often understaffed, poorly trained and equipped, and overwhelmed; at their worst, they are beset with corruption and self-serving interests. Even with the best intentions, they can struggle to say and do the right thing when it comes to fulfilling their responsibilities. While honoring the government's inherent ability to know what is best for its country, TRADCOM seeks to guide the themes and messages that arise from indigenous channels of communication. Whether it facilitates a jirga, a town hall, or an online forum, TRADCOM's goal is to discover, culti-

questions and, more importantly, listening to answers. Over time, the same names get mentioned again and again, names of those who are respected and honored, and these individuals are most often the ones to whom others will listen. The process of uncovering and entrusting these credible voices takes time but is well worth the investment.

Develop Relationships and Partnerships. Enduring results require enduring relationships and partnerships, whether one is operating within a society that values collectivism or one that favors individualism. At the end of the day, humans want to be valued and belong to something that binds them to a larger cause. The challenge is to provide both time and space for these relationships and partnerships to grow while simultaneously satisfying and tempering the demand to achieve demonstrable results quickly.

"Nudge" Newly Cultivated Partners in the Right Direction. Two words are operative here: *nudge* and *right*. Right is not, by default, what *we* believe is best. Nor is it, by default, what the host nation partner believes is best. TRADCOM seeks to honor local traditions, mores, mindsets, habits of practice, and channels of communication. However, ultimately, it is another tool to achieve operational objectives and the commander's intent and necessitates deliberate shaping activities to bring about desired outcomes. Like any influence activity, the goal is to shape or nudge our partner to do something and make him believe it was his idea.

Prepare to Step Outside of Comfort Zones. A contributor to this article was invited to attend a hastily held jirga with a suspected Taliban sympathizer in northwest Afghanistan. She was unarmed and wore no protective clothing, instead wearing slacks, a traditional blouse, and a scarf over her head. Despite the traditional attire, as a blond-haired female she readily stood out among

the men assembled in the courtyard. When it came time to eat, she squatted on the ground and noticed that the others were watching her intently to see what she would do. There were no utensils, and a prepared goat lay on the ground. She ripped off a piece of meat and popped it in her mouth. From that moment forward, she was just another member of the jirga. For many reading this article, participating in native customs is a no-brainer, but there always remains some local habit that takes us to the edge of our comfort zone, and we must be ready to leap off that edge and demonstrate respect for our partners' cultures.

Do Not Allow the Desire for "Effects" to Constrain the Process. TRADCOM must resist the tendency of most military organizations to overplan. Success is less about planning and more about planting ideas, being nimble within a cultural space, and keeping pace alongside our partners. TRADCOM is consultative and cooperative. It is about taking time to listen and nourish friendships and shared ideas. An overemphasis on changed mindsets and behaviors or on holding a specific number of events within a set time may short-change or prevent meaningful relationships, real dialogue, and genuine progress.

Integrate TRADCOM into Larger Efforts. The integration of civil-military communication efforts is critical to overcoming duplication of effort, ensuring wise use of limited resources, and amplifying results. In late 2009 through early 2010, the ISAF Communication Directorate (now Deputy Chief of Staff for Communication) worked in partnership with the Communication and Public Diplomacy Office of the U.S. Embassy, as well as the U.S. Agency for International Development Public Affairs Office, to develop a comprehensive, integrated communication plan, titled the Blue Plan. TRADCOM fulfilled many of the plan's objectives and thus received cooperative support and funding. In fact, grants from the Embassy have been crucial to the program's early success. The key will be to obtain sustained funding to build on the gains made to date.

The Way Ahead

The ISAF TRADCOM effort arose from the belated realization that we were ignoring the most potent channels of communication within the country: face-to-face, word-of-mouth, and communal channels that reached the populace more completely than any other

means. Starting in October 2009, we stood up the effort with a staff of three (realigned from other duties). In the 9 months that followed, this small team, assisted by one contractor and an Afghan company that specialized in planning and executing district-level shuras, was able to accomplish a significant amount, most especially the mentoring of the MoBTA and MoHRA to plan and execute deliberate outreach to tribal and religious elders across the country.

Initial efforts focused primarily on extending the reach of the MoBTA as it dealt with issues that nested more readily with national-level efforts, such as the London Conference, NCPJ, and Kabul Conference. Also, funding support for MoBTA outreach, such as grants from the U.S. Embassy, was easier to obtain because it was not laden with the religious overtones involved with supporting MoHRA efforts.

From October 2009 until September 2010, the MoBTA, with TRADCOM support, conducted 14 provincial jirgas across the country. These events were no small undertakings. They involved finding a suitable venue, sending invitations, offering stipend support to elders to underwrite their travel costs, and providing room and board during the event. It also involved lining up speakers, framing presentation content, and preparing and printing handouts. On average, a provincial jirga can cost upward of \$15,000.

MoBTA's program objectives for the coming year seek to increase the number and frequency of jirgas three- to four-fold. They also seek to expand the network of credible voices to more than 10,000 tribal and/or village elders. One of the most valuable aspects of these events is the atmospheric data they allow us to collect. Formalization of the TRADCOM program, along with consequent funding and manning, will enable enhanced data-gathering and data-sharing. Finally, the coming year should see the maturation of two complementary efforts: nationally planned and nationally led provincial jirgas and provincial office capacity-building. The latter will facilitate MoBTA's ability to conduct district-level shuras, with the aim of ensuring that local grievances are better addressed by GIROA and that national-level programs, policies, and initiatives are understood, welcomed, and implemented at the local level.

Because of the religious implications involved with supporting the MoHRA,

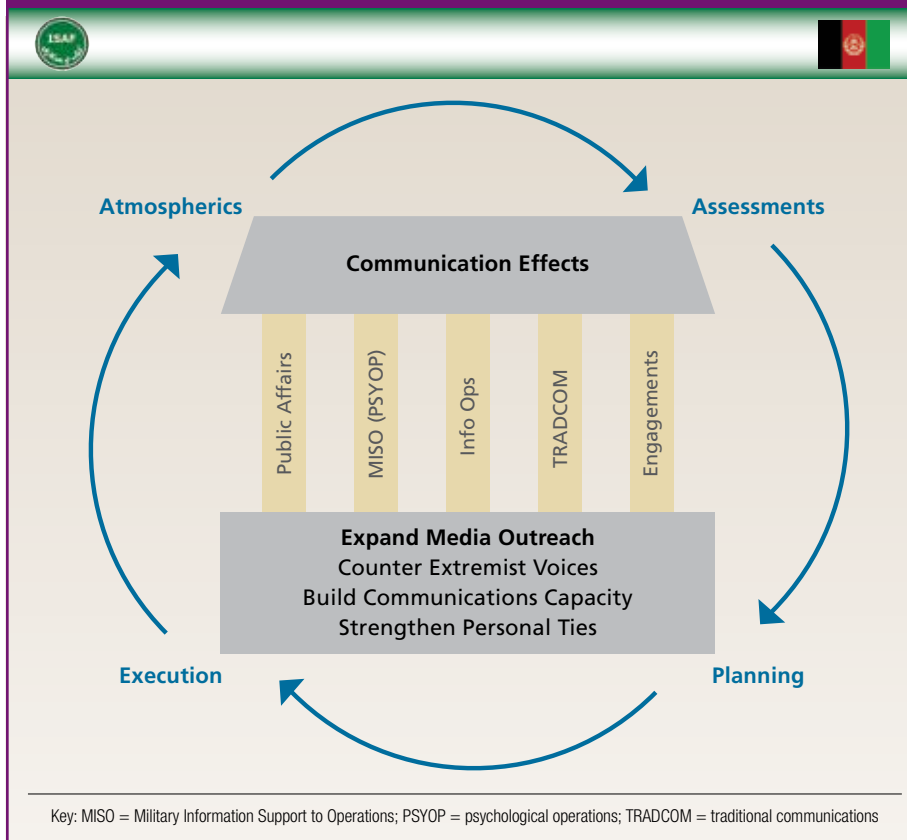
our partnership efforts have taken longer to implement, in large part because it has required lengthy socialization with the international community, the North Atlantic Treaty Organization, and the U.S. Government. There is no question that in countries such as Afghanistan—in which religion informs political, social, and legal institutions and processes—working with a ministry like MoHRA is crucial to reaching the people in ways that resonate with their worldview, ingrained customs, and community makeup.

One of the greatest challenges facing MoHRA is that a considerable number of religious leaders are naïve concerning many aspects of Islam. Many are illiterate and teach by rote what they have been taught. To help broaden their understanding, the MoHRA plans to conduct a series of religious seminars over the coming year that will offer a standardized curriculum of religious teaching. The United Arab Emirates (UAE) has also offered substantial support in this area and hosted the first of five planned 2-week seminars in late September 2010. These seminars focus on Koran-based teachings of peace and tolerance and welcome up to 20 Afghan mullahs per seminar. The next four seminars in the UAE, one of which will be dedicated exclusively to women, will be conducted once per quarter in 2011.

MoHRA will also undertake a significant effort to establish and expand a national religious leader (mullah) network by which and through which moderate and responsible religious instruction and pronouncements can reach the people. This includes dramatically increasing the registration of mosques as a means of accountability and mutual support. Registered mosques will eventually be eligible for a range of government incentives that make their inclusion in the network worthwhile.

TRADCOM's newest line of effort is outreach to Afghan youth through its partnership with the MoIC and its Deputy Minister of Youth Affairs (DMoYA). Youth in Afghanistan, defined by the Asian standard as males and females between 14 and 30 years old, constitute more than 65 percent of the population. Unfortunately, this youth majority is routinely excluded from participation in Afghanistan's traditionally hierarchical decisionmaking processes. The MoIC and DMoYA intend to empower Afghan youth by publically recognizing their importance, establishing an environment that fosters the exchange of ideas,

Figure 2. ISAF Deputy Chief of Staff for Communication Structure



and providing opportunities for the youth to serve as community leaders.

On October 30, 2010, the MoIC/DMoYA hosted Afghanistan's first National Youth High Council General Assembly in which 106 elected male and female representatives from every province and Kabul City discussed and ratified the General Assembly's platform. This platform codified the purpose and responsibilities of the National High Council and its respective provincial, district, and village youth councils across seven lines of effort: coordinate youth policy and strategic plan, encourage sport and cultural activities, support local governance and community development, encourage volunteerism, strengthen democracy, promote youth leadership, and promote gender mainstreaming.

TRADCOM is currently advising/assisting the DMoYA in the development and execution of a comprehensive follow-up shura plan to the General Assembly. The deputy minister intends to travel to each of Afghanistan's 34 provinces to conduct provincial youth shuras that will serve as a foundation on which to establish district- and village-level youth councils. Each provincial shura will strive to ensure equitable male and female rep-

resentation, address province-specific needs, and offer standardized training in the areas of governance, volunteerism, counternarcotics, and employment.

The goals of these ministries for the coming year are aggressive, even lofty, but demonstrate a genuine commitment to achieve results. TRADCOM will be in the background, quietly but actively advising and supporting with funding and logistics.

In hindsight, TRADCOM seems utterly intuitive. The fact that it took 8 years to recognize its unique ability to address the multiple challenges that confronted us speaks to our tendency to overvalue our own perspectives and then overengineer solutions based on our notions of how things should and ought to work.

TRADCOM is a unique kind of influence that leverages trusted and credible channels of indigenous communication to connect the government to the people. While not addressed specifically in doctrine, TRADCOM merits consideration as a distinct and essential component of a commander's arsenal of information/communication capabilities. This is what we have done at ISAF. Although resourcing for TRADCOM

is a fraction of other capabilities, its impact was sufficient to warrant making it a coequal pillar in the ISAF Deputy Chief of Staff for Communication structure (see figure 2). We believe that the all-important coming year will validate our thinking and prioritization of effort and resources to TRADCOM.

Indigenous people everywhere are savvy people; they can read sincerity and authenticity well. We must get out of our skin and into theirs. We must help energize and enable credible and responsible voices, both within the government and among the people, to make sense of and then shape their destiny for the better. TRADCOM is like a pebble thrown into water; it only actually impacts a tiny space of the human ocean into which it is tossed. But the ripple effect it creates, compounded by the effects of other selectively thrown pebbles, can be powerful and enduring. **JFQ**

For their contributions to this article, the author thanks Lieutenant Colonel Maria Metcalf, USA; Lieutenant Colonel Chad McGougan, USA; and Lieutenant Colonel Kelly Brown, USARNG.

NOTES

¹ William B. Gudykunst and Yuko Matsumoto, "Cross-Cultural Variability of Communication in Personal Relationships," in *Communication in Personal Relationships Across Cultures*, ed. William B. Gudykunst, Stella Ting-Toomey, and Tsukasa Nishida (Thousand Oaks, CA: Sage Publications, 1996).

² Greg Mortenson and David Oliver Relin, *Three Cups of Tea* (New York: Penguin Books, 2006).

³ Sarah Chayes, *Comprehensive Action Plan for Afghanistan*, January 2009.

⁴ William Cronon, "A Place for Stories: Nature, History, and Narrative," *The Journal of American History* 78, no. 4 (March 1992), 1347-1376.

⁵ Karl E. Weick, Kathleen M. Sutcliffe, and David Obstfeld, "Organizing and the Process of Sensemaking," *Organization Science* 16, no. 4 (July-August 2005), 414.

⁶ Robert Chia, "Discourse Analysis as Organizational Analysis," *Organization* 7, no. 3 (2000), 517.

⁷ Weick et al., 410.

⁸ Ibid., 416.

⁹ Ibid., 415.

¹⁰ John Milton, *Areopagitica*, ed. J.W. Hales (London: Clarendon Press, 1894), 42-43.

The Future of National Security, By the Numbers

By P.W. SINGER

“Figures often beguile me,” Mark Twain wrote in his autobiography, “particularly when I have the arranging of them myself; in which case the remark attributed to Disraeli would often apply with justice and force: ‘There are three kinds of lies: lies, damned lies, and statistics.’”¹



Secretary Gates and Admiral Mullen brief press on efficiencies in DOD reform agenda

U.S. Air Force (Jerry Morrison)



Most of those who work in the realm of international security would tend to agree with Twain. We have all seen academics spit out statistics and models in a way that was of no actual use to those who cared about the real world. Similarly, we have watched politicians run fast and loose with all sorts of numeric data. The result is that we often more agree with the witty Scottish statesman who said, “You might prove anything by figures.”

And yet, as much as those of us who despised calculus back when we were in school hate to admit it, numbers do matter. The unadulterated cleanness of a number does have a certain way of driving home the truth of a matter, most importantly in cutting through the rhetoric and the often intentional confusion that surrounds complex matters. Figures can show a cold, hard reality that we often want to ignore. As Aristotle wrote, “Numbers are intellectual witnesses.”²

Today, we are entering a period in national security that various strategic documents ranging from the Pentagon’s Quadrennial Defense Review (QDR) to the new British Security Strategy have entitled “an age of uncertainty.” We have been left grasping for some type of certainty in everything from threats to resources. So, if looking through the mathematical lens offers “the poetry of logical ideas,” as Albert Einstein claimed, what are the key numbers that we should be paying attention to in trying to understand where we might be headed next in the realm of national security?

\$13.7 Trillion

In October 2010, Prime Minister David Cameron issued a new British national security strategy that entailed a wave of cutbacks, including 17,000 fewer soldiers and 25,000 fewer civilians in the British military. Also left on the cutting room floor were all its Harrier jets, several ships including an aircraft carrier, and 40 percent of the army’s tanks. Cameron’s government made this decision not because it wanted to (conservative governments in the United Kingdom have traditionally been defense hawks when it comes to budgets), but because it felt that it was the only way to stave

off short-term currency and fiscal crises and a long-term economic security collapse.

While many commentators have focused on what these cuts mean for the British military role in the world, the numbers underlying the report illustrate the type of tough decisions that are also likely looming in American policy circles moving forward. That is, a quick run of the numbers shows that the British conservative government felt obligated to act when facing a fiscal

the British conservative government felt obligated to act when facing a fiscal environment that pales in comparison to the U.S. predicament

environment that pales in comparison to the U.S. predicament. The United Kingdom had a roughly \$242 billion budget deficit and (more useful for comparative purposes) was running almost to a 60 percent debt-to-gross domestic product (GDP) ratio. By comparison, the U.S. debt stands at \$13.7 trillion and an 89 percent debt ratio, with the Office of Management and Budget showing the deficit coming in at another \$1.3 trillion in fiscal year 2011. In essence, Britain’s nightmare scenario remains America’s blissful normality. If action is not taken to rein this in, the Congressional Budget Office estimated that in 2050, the U.S. gross debt will have reached about 344 percent of GDP.

At some point, these numbers’ growth will become unsustainable for both U.S. economic and national security, and thus the British experience may well be looked to for guidance by American policymakers, either by fellow conservatives or liberals. As in the United Kingdom, most of the savings will have to come out of reduced government spending and dealing with unfunded social welfare commitments (which in the United States are mainly driven by making social security promises that no longer reflect demographic reality), but no one should believe that the debate will spare the defense and foreign policy world. As in Britain, there will likely be an expectation that the pain of any cuts will have to be spread out. Notably, this likelihood seems to be borne out by the various bipartisan debt and deficit reduction task forces that released various reports last fall, all of which

brought up the need for tightening a Pentagon funding spigot that has been opened more and more over the last decade.

While Secretary Robert Gates has tried to preempt such cuts with efficiency measures designed to wring \$100 billion in savings across multiple years, two realities stand in the way. The first is that the current process is not about actual cuts, but is instead an attempt to shift funds internally. The second is that these measures are unlikely to yield anywhere near \$100 billion. For example, the big talk about closing U.S. Joint Forces Command should save at most \$250 million—and that is if the entire shop were closed versus the likelihood that many of the offices will emerge intact within other commands. Similarly, a substantial portion of the claimed cuts in the new Department of Defense (DOD) budget offer depends on a changed assumption on inflation figures. Shifting numbers across accounts did not work for Enron over the long term; nor will it work for the Pentagon.

Defense hawks should take solace in the fact that, much like what is likely to happen in the United States, the British number-crunchers found savings but avoided harming current operations. Moreover, the British defense cuts were far less severe (at only one-third of the scale) than those experienced by other agencies of foreign policy, such as the 25 percent level of cuts at the Foreign and Commonwealth Office. (Indeed, if the numbers in the British experience indicate tough times looming for the Pentagon, it indicates cuts to the bone for agencies such as the State Department.)

The exact size of the potential cuts will certainly be a matter of much projection and debate in the coming years (my colleague Michael O’Hanlon, who tends to have a good history at this sort of thing, predicts that DOD ultimately will be asked to find roughly \$60 billion in savings), but what is clear is that we are entering an era in which leaders will have to make some actual decisions in defense policy, not only in spending but also in fiscal and strategic priority-setting.

\$10,500 per American, \$1.3 Billion per al Qaeda

The U.S. military’s newspaper *Stars and Stripes* found that at \$747 billion spent in direct funds, each American citizen has paid \$2,435 for the Iraq War. If one includes indirect spending and broader economic consequences, it comes out to just over

P.W. Singer is Senior Fellow and Director of the 21st Century Defense Initiative at the Brookings Institution.

\$9,000 per citizen. This does not include the roughly \$500 billion that will have to be spent in medical and disability compensation for Iraq War veterans over their lifetimes, which comes out to another \$1,500, for a total of \$10,500 per U.S. citizen. When it comes to dealing with nonstate actors, our investment

attack had or might emanate, and the remaking of the government there to ensure it was no longer a terrorist organizing and recruiting ground. These responses, initially framed as counterterrorism missions, gradually shifted into counterinsurgency missions in the midst of civil wars, and U.S. forces became bogged

nance, no one contemplated anything beyond more unmanned strikes and a few covert action teams.

35 Bands, 1 Diplomat

This shift actually makes perfect sense when one looks at the other key numbers that shape this space, establishing the parameters of not just what the United States can afford or not, but also who should carry them out and how.

While counterinsurgencies and nation-building efforts are certainly tough, they are not impossible tasks. Rather, they require a deep and enduring commitment. A RAND study found, for example, that the average length of an insurgency is about 10 years; wars won by the government side (what we are fighting in Afghanistan) take an additional 2 years on average.

For the last decade there has been constant discussion of building up our capabilities to deliver engagement, stability, aid, development, and justice programs on the ground, the nonmilitary aspects so key to success in these types of operations. And yet for all the discussion in leveraging agencies other than the military, the numbers show something else: that nearly 10 years into such fights, Washington still has not faced the deep and enduring commitment part of the battle.

The State Department, for instance, has roughly 6,500 Foreign Service Officers and 5,000 Foreign Service Specialists. They are spread across 265 diplomatic missions, with the Washington, DC, headquarters housing the bulk. When it comes to the actual

these numbers are leading many to question whether an approach based on territorial seizure is the best manner for defeating a global nonstate network

ratio is even more draining. *Defense News* found that U.S. military spending on its operation in Afghanistan was just over \$1.3 billion per suspected al Qaeda member.

These numbers define the environment of another key aspect emerging in national security: not merely what to spend, but what we can afford to do operationally. That is, if we are entering an “era of persistent conflict,” as our strategy documents project, can we persistently sustain such cost ratios against our foes? Moreover, these numbers are leading many to question whether an approach based on territorial seizure is the best manner for defeating a global nonstate network, and, in so doing, driving an evolution of how the United States conducts counterterrorism.

In the wake of 9/11, when it came to responding to a real (in the case of Afghanistan), or at least publicly claimed potential (in the case of Iraq), terrorist attack, the rejoinders were preemption and “regime change,” the seizure of the territory from which the

down in local political and ethnic disputes. As David Kilcullen noted in *The Accidental Guerrilla*, the irony was that such efforts to undermine recruiting by extremists may have made it easier.

Seemingly unable to contemplate the costs for a new operation of such scale, the responses to recent plots of terrorism seem to be moving to another model, or perhaps a “back to the future” model of the cruise missile diplomacy of the late 1990s. Bob Woodward’s *Obama’s Wars* outlines that the planned U.S. response to a successful attack on American soil—tracked back to Pakistan—is not to set large numbers of boots on the ground. Instead, the response is a simple expansion of the number of unmanned airstrikes already being conducted there. This is not particularly notable, given that the undeclared U.S. air war in Pakistan has so far hit 202 targets with drones. Similarly, when a series of plots were tracked back to Yemen and Somalia in 2010, other black holes of gover-

NARA

M1A1 Main Battle Tank is Marine Corps’ leading combat armored vehicle



USS Freedom (LCS 1) and USS Independence (LCS 2) reflect Navy’s progress toward developing superior surface force



NARA

ability to deliver at the field level where it matters most, the numbers show a hard truth. Roughly 4 percent of the operational budget for Afghanistan goes toward civilian operations. The entire U.S. Government has been able to generate only 13 Provincial Reconstruction Teams (PRTs) there, each of roughly 80 personnel. Moreover, the only way to staff these PRTs has been to draw primarily from the military Services (even though the PRTs do not have a traditionally military role), most often by bringing officers from other taskings (meaning that their background and training do not match the type of aid, development, and reform advisory work the teams conduct). The PRT in Farah, Afghanistan, for example (which was ably commanded for the past year by a Navy officer with a background in helicopter operations), had one State Department civilian advisor for an area roughly twice the size of Maryland and containing 1 million Afghan citizens.

To put this in a numeric comparison, the U.S. Army alone has 35 Regular Army bands, ranging in size from 50 to 250 members. In addition, there are 18 Army Reserve bands and 53 Army National Guard bands. The numbers are on a similar scale for the other Services. These numbers show where we stand between the rhetoric of counterinsurgency and interagency planning and the reality of executing it at DOD as well as non-DOD agencies.

8 Percent of Voters

The reason for this shift in operational responses and the continued lack of capacity may be found within another set of figures: the numbers that tell us about the underlying political support for such expanded operations today, and their likely future.

Again, the important point here is not whether such operations are doable, but whether the intervening party has the long-term will necessary for them. And here, too, the numbers may be painting a different sort of message about the American body politic, one that is increasingly becoming disengaged from foreign policy issues. Indeed, in the last election, less than 8 percent of voters told CNN that their votes were determined by foreign policy issues.

When we look at future trends, the numbers grow worse. I recently completed a survey of over 1,100 young American leaders between the ages of 16 and 24 who have attended National Student Leader



PRT leaders meet with local officials in Diyala, Iraq

Department of State

conferences and expressed an interest into going into politics and policy. While not all will achieve this goal, it is interesting that in this set of would-be future Barack Obamas and John McCains, 58 percent believed that the “United States is too involved in global affairs,” roughly twice that of older generations. The polling shows there is a strong emerging narrative of isolationism, shaped by their formative experiences of 9/11, Iraq, and Katrina (comparable to the impact of Pearl Harbor or the Kennedy assassination and Vietnam for prior generations). Notably, this is not a trend being driven by the new Tea Party movement, but rather one occurring among young leaders who identify as Democrats or Independents, who are 20 percent more likely to have such isolationist attitudes than young Republicans.

These are just attitudes, which may change or even reverse in the future; the isolationist youth of the 1920s and 1930s, of course, ended up having to fight World War II in part because of such attitudes. But whether it is the strange coalition-building between the left and right wing on withdrawing from Afghanistan or declining new commitments in Yemen, Pakistan, Somalia, or elsewhere, the American public and its policy leaders seem to be steering away from any mission of scale. Indeed, the changing appetite is even illustrated by recent actions

in our own hemisphere. In 1994, the fear of a failed state in Haiti led to the deployment of more than 20,000 military personnel, with a broad mandate to uphold democracy. By comparison, after the 2010 earthquake created an actual collapsed state in every sense of the term, the United States sent just over 4,000 troops, with a mandate to get aid in quickly and then get out as rapidly as possible.

18 Months, 1 Billion Times as Powerful

The prime numbers of national security’s future lie not only in dollars, voters, terrorists, or diplomats, but also in how we handle an emerging wave of “killer applications.”

It used to be that an entire generation would go by without one technologic breakthrough that altered the way people fought, worked, communicated, or played. By the so-called age of invention in the late 1800s, these breakthroughs were coming once every decade or so. Today, the ever-accelerating pace of technological development is best illustrated by Moore’s Law, the finding that, over the last 40 years, microchips—and related developments in computers—have doubled in both power and capability every 18 months or so. The total amount of computing power that the entire U.S. Air Force had in 1960, for example, is now contained in a single Hallmark greeting card that plays a little song when you open it.

Moore's Law predicts that such technologies will be one billion times more powerful within 25 years. While the historic pace of change does not have to hold true (but note that even with a pace one-thousandth as fast as it has historically been, we will still see technologies one million times more powerful within 25 years), it is inarguable that wave after wave of new game-changing inventions are bursting onto the scene with an ever-increasing pace. From robotic planes that

7 Degrees of Security and 1493

But new discoveries do not just affect the tools at our disposal and how we choose to use them; they also can lead to entirely new realms of commerce and conflict that national security leaders must wrestle with. As one Air Force general told me, "The greatest change moving forward is the changing of domains."

Historically, whenever humans have discovered something of value, they often have fought over it. For example, in past

new discoveries can lead to entirely new realms of commerce and conflict that national security leaders must wrestle with

strike targets 7,000 miles away to "synthetic life," manmade cells born out of laboratory chemicals, these astounding technologies grab today's headlines with such regularity that we have become almost numb to their historic importance.

Looking forward, the range of technologies already at the point of prototyping is dazzling in potential impact. Directed energy weapons, "smart" improvised explosive devices, nanotech and microbotics, bio-agents and genetic weaponry, chemical and hardware enhancements to the human body, autonomous armed robots, and electromagnetic pulse weaponry all may seem straight from the realm of science fiction but are on track to be deployable well before most of us have paid off our mortgages.

This raises two sets of questions: how has our national security structure changed in light of these massive changes in the tools at our disposal (answer: not enough), and how will we deal with the massive changes looming? What makes such technologies notable is not just the new possibilities they open up, but also the difficult issues they raise for policy. Even the first generation of unmanned systems today (the Predator may seem advanced, but it is actually the Model T of the field, already obsolete) has raised deep military, political, moral, and legal questions that touch on everything from when our nation goes to war (the air war campaign in Pakistan that has achieved over 6 times the number of airstrikes as the Kosovo war's opening round) to the individual experiences of soldiers themselves (many remote warrior units have levels of combat stress and fatigue that are as high as their counterparts physically deployed to the battlespace).

periods of political landscape shift in European history, the discovery of gold and silver in the New World in the 1500s and the scramble for African gold and diamonds in the late 1800s were greater catalysts for diplomatic and then armed conflict among the rising and established powers than was intracontinental behavior.

Similarly, new technologies also shaped the very battlespaces where such powers contended. Through most of human history, for example, we only fought on the land and on top of the sea. Then, at the turn of the last century, technologies that had only recently been the stuff of science fiction (Jules Verne's *20,000 Leagues Under the Sea* and A.A. Milne's "The Secret of the Army Aeroplane") allowed powers to fight in entirely new domains, under the sea and in the air, which required entirely new forces to be created to carry out these battles and new laws to regulate them.

Today, the numbers show how a series of 21st-century parallels are emerging. While we are no longer filling in the blank spaces in the world's map, we are discovering immense value in locales that previously either were not accessible or did not exist, and, in turn, gearing up to fight there.

For example, the white space on the map of the Arctic region has always been a harsh, inaccessible area that no one particularly cared about in policy circles—until today. As a result of the changes that our technologies have wrought upon the global climate itself, the Arctic is warming up and opening up, and thus creating new issues for global security that cannot be ignored. Indeed, global warming appears to be playing out far more dramatically in the Arctic than elsewhere due to two key numeric factors: the sharper angle

at which the sun's rays strike the polar region, and the faster rate at which retreating sea ice is turning into open water, which absorbs far more solar radiation. Thus, the Arctic is seeing temperature increases in the 7-degree range rather than the 2- to 3-degree rises seen elsewhere. As a result, this part of the globe is yielding new and valuable navigable trade routes, as well as potential drilling spots for significant energy and mineral resources (some believe there may be as much oil and natural gas at stake as Saudi Arabia has).

But opening up a new part of the globe yields new security questions; indeed, there has not been such a geographically large area-of-sovereignty issue to solve since 1493, when Pope Alexander VI divided the New World between Spain and Portugal (which, of course, prompted wars with powers left out of this deal for the next few centuries). Thus today, while conflict is by no means inevitable, various players are preparing for a polar scramble. An advisor to Vladimir Putin declared, "The Arctic is ours and we should manifest our presence," while Canada, Norway, the United States, and even noncontiguous states such as China have started to build up their capabilities to operate in this once forbidding space (the United States has no nuclear-powered icebreakers, while China has two and plans for several more).

947 Satellites, 80 Percent of Communications

Outer space is another domain that was once inaccessible but that is increasing in commercial and military value. Technology has allowed us to turn this place of science fiction into a realm populated by 947 operational satellites.³ Through these systems now runs the lifeblood of global commerce and communication, as well as (arguably) U.S. military operations. About half of the 175 dedicated military satellites orbiting the world are U.S. military systems. But this only tells part of the story. Over 80 percent of U.S. Government and military satellite communications travel over commercial satellites. As General Lance W. Lord, commander of Air Force Space Command, explains, "Space is the center of gravity now."

To give an example of the importance of space, global positioning system (GPS) satellites are used to direct the movement of 800,000 U.S. military receivers, located on everything from aircraft carriers to individual bombs and artillery shells. A "glitch" in GPS

in early 2010 left almost 10,000 of these receivers unable to log in for days, rendering them useless and their systems directionless.

The result is that starting with the 2001 Rumsfeld Space Commission, which served as the springboard for the former Secretary of Defense's return to government, the Pentagon has conducted at least 21 studies of space warfare. Of course, as senior colonel Dr. Yao Yunzhu of the Chinese Army's Academy of Military Science has warned, if the United States believes that it is going to be "a space superpower, it's not going to be alone . . . it will have company." The Chinese have aggressively moved into the satellite and launch sectors, with plans to add more than 100 civilian and military satellites in the next decade.⁴ They also have a manned program on pace to pass the United States, hoping to place a taikonaut on the Moon's surface by 2020.

More important to conflict scenarios is that China has demonstrated antisatellite capabilities repeatedly over the past 3 years, with Russia and India and even a few nonstate actors also at work in the field, indicating that the future of conflict back on Earth will not stop at the edge of the atmosphere for long.

90 Trillion Emails, 90,000 Cyberwarriors

Unlike underwater, the air, the polar cold, or outer space, cyberspace is a domain that not only was inaccessible, but also literally did not exist just a generation ago, which perhaps explains why the current crop of senior leaders seems so flummoxed by it.

The centrality of cyberspace to our entire global pattern of life is almost impossible to fathom, as the numbers involved are so high as to sound imaginary. Almost 90 trillion emails were sent in 2009, at a pace of roughly 47 billion a day. The Internet is made up of some 234 million Web sites, with the number growing at a 25 percent annual rate.⁵ The military use is equally astounding. DOD operates 15,000 computer networks across 4,000 installations in 88 countries. While a substantial portion are kept in their own classified version of cyberspace, the Secret Internet Protocol Router Network, DOD computers access the broader Internet over 1 billion times a day.⁶ Indeed, former Director of National Intelligence Admiral Michael McConnell estimated that 98 percent of U.S. Government communications, including classified communications, travel over civilian-owned and -operated networks.



United Launch Alliance (Carlleton Baillie)

Air Force Global Positioning System IIR-21 satellite is launched aboard United Launch Alliance Delta II rocket

But with so much value being located in this new space, it is also becoming a locale for crime, contestation, and even conflict. Symantec identified more than 240 million distinct new malicious programs in 2009, a 100 percent increase over 2008.⁷ Many of these are various types of spam and low-level annoyances or criminality, but there is a serious undercurrent. More than 100 foreign intelligence organizations have been reported trying to break into U.S. systems, and known cyber attacks against U.S. Government computers rose from 1,415 in 2000 to 71,661 in 2009.⁸ Indeed, the Federal Bureau of Investigation described cybersecurity as the third most important national security threat—a notable designation, considering that its director did not even have a computer in his office until 2001.

While the majority of the focus in public discussion has been on mostly overblown

scenarios of "electronic Pearl Harbors" or "cyber Katrinas" (the vast majority of these attacks on U.S. Government Web sites are actually nuisance defacements, the equivalent of cybergraffiti), the numbers show how the real national security danger may lie in the gradual undermining of the U.S. economic and national security edge, especially in innovation and intellectual property. It is estimated that U.S. firms lose approximately \$1 trillion a year in business, wasted research and development investment, employee downtime, and added spending due to cyber attacks. The Joint Strike Fighter program, for instance, lost several terabytes of data related to design and electronics systems to a cyber attack. To put this amount of lost information into context, the overall size of the Internet did not reach a single terabyte until around 1997. Such numbers represent not only lost bytes and billions of investment dollars in research, but

also 10 to 20 years of lost technological edge in the battlefield and marketplace.

As a result, much as what happened in other new domains, security in the cyber domain is drawing a skyrocketing amount of policy attention, organization, and budget dollars. Much as Marines consider November 10, 1775 (the Corps' birthdate), as the most important day of the year, future cyberwarriors may well celebrate May 21, 2010, the date that U.S. Cyber Command stood up. Non-existent just a few years ago, this new entity now has 90,000 personnel and acts as the coordinator of over \$3 billion in DOD spending on information security.

What these numbers tell us is that war confined to the real world may be passé.

70 Percent Living in the Volcano

The shift in domains is not just a matter of the changes technology has wrought on the world around us; it is also about where we are. And here, too, the numbers show a monumental shift under way, with huge resonance for the future of national security.

To many, the U.S. military has rounded an intellectual corner in the last few years. From the writings of the QDR to the training given to Army captains, there has been an increased emphasis on the ability to navigate the complex geographic and social patterns of simultaneously defeating a guerrilla army while winning tribal elders' hearts and minds in the midst of perhaps the most rural, remote, and mountainous part of the world.

Yet the rest of the world seems to be going in a different direction than the type of villages we are training for, which remain essentially unchanged from the time of Alexander the Great's invasion to our own operations in rural Afghanistan. Rather than its rural history, the future of humanity lies in the cities.

In 1800, only 3 percent of the world's population lived in urban zones. By 2008, it crossed the 50 percent mark and is on pace to reach the 70 percent mark within the next 25 to 30 years, the same period our strategies claim to plan for.

But as we add 3 billion new souls to the planet, 99 percent of them in the developing world, it is not only a move to the cities that is afoot, but a move to cities of ever-increasing size and scale. More than 40 percent already live in cities with populations of more than 1 million. These staggering statistical trends are driving the evolution of the "megacity," an

urban agglomeration of more than 10 million people. Sixty years ago, there were only two: New York and Tokyo. Today there are 22 such megacities—the majority in the developing countries of Asia, Africa, and Latin America. By 2025, there will be another 30 or more.

Most importantly, each of these cities is characterized less by its glittering skyline than by its "megaslums," the miles upon miles of shantytowns and squatter communities that house millions of young, urban poor, the angry losers of globalization. As Mike Davis writes in *Planet of Slums*, the city that was once the capstone of civilization and wealth creation is increasingly surrounded by "stinking mountains of shit" that are "volcanoes waiting to erupt." What this means is that despite our understandable current focus on how to deal with tribal elders in the mountains of Afghanistan, the numbers tell us that the future focus of global security will most likely be an urban one.

This shift occurs not just because of the mass movement into the cities, but also because the city is increasingly where the anger that causes insurgency, terrorism, and war originates. Historically, rebellion and conflict usually started in the rural regions and, only if successful, spread to the city. But as analyst Ralph Peters notes, the 21st century has seen the reversal of that trend: "Cities are now center[s] of rebellion . . . because the city is dehumanizing, breaking down traditional values and connections."⁹ And for the young citizens of this place,

despite our understandable current focus on how to deal with tribal elders in the mountains of Afghanistan, the numbers tell us that the future focus of global security will most likely be an urban one

"Habituated to violence, with no stake in civic order . . . there is only rage."¹⁰

Moreover, these broken cities are their home turf, the more likely Sherwood Forest to any future insurgent or terrorist than a village or forest itself. Describing a scene that could be straight out of Mogadishu, Fallujah, Freetown, Gaza, Grozny, or Sadr City, Peters notes that cities are where professional forces tend to face more problems, and thus the "future of warfare lies in the streets, the sewers, high-rise buildings, industrial parks, and the sprawl of houses, shacks, and shelters that form the broken cities of our world."¹¹

3 Times the Size

The final change lies within the very people who will increasingly staff the military and will be making the decisions that shape how the United States and its allies react to these changing numbers.

From 1980 to 2005, the U.S. population experienced a historic demographic shift. The generational cohort born in this period—known as the Millennials, Generation Y, or the Facebook and 9/11 Generation—came in at slightly larger than the Baby Boomers in numbers and *three* times the size of the preceding Generation X. Indeed, these comparative ratios were what propelled Barack Obama into the White House.

This generation has already produced the young voters, soldiers, and diplomats of today, who will in turn be the leaders of tomorrow (and given their numbers, at faster rates and of greater power than the X-ers who now fill middle management roles). Thus, any national security policymaker (and, arguably, boss, teacher, coach, or pastor) who wants to succeed in this future will need to understand this new generation.

The numbers show how this emerging generation brings different perspectives to everything from historic experiences to political and strategic values. They grew up in a world in which there was no divided Germany, cameras lacked film, and the Internet is a primary news source. For instance, Vietnam has been a touchstone experience for American policymakers for the last few

decades, creating a lens through which they view the world even today (*Newsweek*, *The New York Times*, and *Washington Times* have all led with stories as to whether Afghanistan is "Obama's Vietnam"). And yet to a Millennial, the Vietnam War is as distant as World War II is to the Obama White House. Polling has found that young leaders coming of age in the post-9/11 world have far more mixed views of traditional allies such as Israel, Pakistan, or Saudi Arabia, while the shifting demographics of America (becoming over 30 percent Latino, for instance) may well bode changes to the idea that the U.S. focus can be either

transatlantic or transpacific only. Indeed, the U.S. population is expected to rise by roughly 142 million over the next four decades, but most of this growth would not be domestic. Newly arriving immigrants would account for 47 percent of the rise, and their U.S.-born children and grandchildren would represent another 35 percent.

Perhaps most importantly, the emerging generation that will shape national security brings its own way of doing things. For example, nearly every business and government agency is now wrestling with the recruitment and management of young workers who have different sets of career goals, who seem to be looking for shorter-term jobs rather than long-term careers, and who are focusing more on “finding their passion” than did previous generations. Has our 1950s-era personnel and benefits system similarly changed?

Having grown up as “digital natives” in a world in which computers always existed and 97 percent regularly use them, this new generation brings vastly different expectations of the technologies that stress our systems and bureaucracies. Indeed, perhaps no organization has faced this in tougher terms than the U.S. military, which has struggled with everything from whether to allow social networking (the Pentagon spokesperson set up Facebook and Twitter accounts at the very same time it was banned at many U.S. military bases) to the slow acquisitions system, which particularly annoys this young and very impatient generation. A young Soldier in Afghanistan, for example, who has yet to get his Joint Tactical Radio System (a multibillion-dollar defense contractor radio system first funded in 1997 but still undelivered) can buy an application for his personal iPhone that tracks sniper bullet flights for 99 cents.

This generation also brings in a different approach to how it uses, processes, and shares information itself. Prior generations had information pushed to them and were taught to hoard it, whether they were students taking a test or policymakers shaping a nation’s foreign policy. By contrast, Millennials tend to have a “Google mindset.” Information’s value lies not in its limitation, but in its distribution. Knowledge is valued not in terms of ownership, but rather in accessibility, how easily it can be “pulled” and applied to rapidly changing problems.

The outcome of this is different patterns of thinking. As an example, this generation

is amazingly adept at multitasking; I once watched a young Airman sitting behind a bank of computer screens at a Combined Air Operations Center in the Middle East simultaneously working within 36 different Internet chatrooms, each an airstrike mission. But as any parents who have had the experience of speaking with their children at dinner while they text under the table could attest, this multitasking sometimes comes at the price of reflection and long-term problem-solving.

knowledge is valued not in terms of ownership, but rather in accessibility, how easily it can be “pulled” and applied to rapidly changing problems

Unfortunately, what psychologists are calling this “continuous partial attention syndrome” could describe not only our young men and women, but also perhaps our nation as a whole. We are getting very good at multitasking, but it is hard to see much strategy in terms of directly facing the realities that the above numbers raise. And for that our nation could pay a tragic price.

One could draw differing lessons and conclusions from the key numbers above of national security, and indeed how to face them should lie at the heart of any policy debate moving forward. And they will surely evolve and change. But as Stendhal once wrote, the beauty of numbers lies in the fact that they “allow for no hypocrisy and no vagueness.” No one seriously wrestling with understanding, planning, and preparing for the national security world of today and tomorrow can afford to ignore the cold, hard reality that each of these statistics and figures underscores about the deep challenges we face in our rapidly changing world. **JFQ**

NOTES

¹ Mark Twain, “Chapters from My Autobiography,” available at <www.gutenberg.org/files/19987/19987.txt>.

² Aristotle, *The Metaphysics* (10f–1045a).

³ Union of Concerned Scientists Satellite Database, available at <www.ucsusa.org/nuclear_weapons_and_global_security/space_weapons/technical_issues/ucs-satellite-database.html>; and the United Nations Convention on Registration of Objects Launched into Outer Space, available

at <www.unoosa.org/oosa/en/SORegister/regist.html>.

⁴ Peter Brookes, “The Not-So-Final Frontier,” *Armed Forces Journal*, June 2008.

⁵ See “Internet 2009 in Numbers,” January 22, 2010, available at <http://royal.pingdom.com/2010/01/22/internet-2009-in-numbers/>.

⁶ Eric T. Jensen, “Cyber Warfare and Precautions against the Effects of Attacks,” *Texas Law Review* (June 1, 2010), available at <www.allbusiness.com/government/government-bodies-offices/14878449-1.html>.

⁷ “Symantec Report Shows no Slowdown in Cyber Attacks,” available at <http://h30458.www3.hp.com/us/us/smb/974594.html>.

⁸ Jensen; Gary McAlum, “U.S.-China Economic and Security Review Commission, Hearing on China’s Proliferation Practices, and the Development of its Cyber and Space Warfare Capabilities,” hearing before the U.S.-China Economic and Security Review Commission, 110th Congress, 2^d sess., May 20, 2008; author telephone interview with staff member, U.S. Strategic Command, August 28, 2009; author email interview with staff member, U.S. Cyber Command, August 17, 2010.

⁹ Author interview with Ralph Peters, Washington, DC, March 29, 2007.

¹⁰ As quoted in Christopher Coker, *Waging War Without Warriors? The Changing Culture of Military Conflict*, IISS Studies in International Security (Boulder, CO: Lynne Rienner, 2002), 10.

¹¹ Ralph Peters, “Our Soldiers, Their Cities,” *Parameters* (Spring 1996), 43.

Transformation Achieved?

Revisiting the 1997 National Defense Panel

By RICARDO A. MARQUEZ



Secretary Rumsfeld briefs press on Operation *Iraqi Freedom*

It was going to be a journey. In the recollection of one 1997 National Defense Panel (NDP) member, transformation was supposed to be “evolutionary,” not the revolutionary upheaval advocated by some. The NDP report’s theme—transformation—signaled an audacious undertaking, but the only urgency demanded by the panel was the need to act in the *present* if the United States were to be transformed and prepared to meet the national security challenges of the 2010–2020 period. Indeed, the principal conclusion of the 1997 NDP report was that transformation was a priority only because the factors influencing the 2010–2020 period were unfolding in the present

day, and transformation would provide the Nation with “options” in the future.

The report readily conceded that the journey to 2010–2020 would be arduous because while tremendous capabilities existed in the Department of Defense (DOD), transformation could only begin there. Under the rubric of transformation, DOD would institutionalize change while the entire Federal Government would reform its approach to national security. As the United States enters the decade for which the NDP planned, the principal questions remaining are whether transformation has been achieved and whether the country is prepared. While the NDP is to

be praised for its prescient conclusions, panel members contend, in retrospect, that America remains unprepared for 2010–2020, primarily because transformation remains incomplete.

This article revisits the conclusions of the National Defense Panel, offers a brief history of transformation at DOD, and examines the extent to which the United States is prepared for the 2010–2020 period. As part of the review, the article includes the perspectives of the original panel members as to whether the conclusions and recommendations submitted in 1997 remain valid and applicable in the current international security environment.¹

Ricardo A. Marquez is a Senior Analyst for Defense Capabilities and Management at the U.S. Government Accountability Office.

Conceiving the NDP

In 1995, the Commission on the Roles and Missions of the Armed Forces recommended establishing a “quadrennial strategy review.”² Congress embraced the proposal and passed legislation mandating DOD to undertake such a review. While considered the third of six full-scale assessments of defense policy since the end of the Cold War, the 1997 Quadrennial Defense Review (QDR) was the first such examination subsequent to congressional direction.³ At the same time, Congress authorized a separate, independent effort to conduct a corresponding comprehensive review.⁴

the panel concluded that transformation was an immediate priority because the factors influencing the 2010–2020 period were already unfolding

The subsequent National Defense Panel would be composed of nine “recognized experts” appointed by the Secretary of Defense, in consultation with the Senate and House Armed Services committees. The final panel was chaired by Philip A. Odeen and composed of the following individuals (in alphabetical order): Ambassador Richard L. Armitage; General Richard D. Hearney, USMC (Ret.); Admiral David E. Jeremiah, USN (Ret.); Ambassador Robert M. Kimmitt; Andrew F. Krepinevich; General James P. McCarthy, USAF (Ret.); Janne E. Nolan; and General Robert W. RisCassi, USA (Ret.). The legislation required the panel to submit the report to the Secretary of Defense and mandating committees by December 1997. From this mandate emerged the premise of transformation.

When the panel previewed its findings in the August 1997 issue of *Joint Force Quarterly*,⁵ the article characterized transformation as a challenge and concluded that the need for “a transformation strategy . . . to get beyond today’s security structures” was becoming “increasingly apparent.” When the panel released its report the following December, the context was no longer just challenges, but also opportunities.⁶ The military may have done a superb job of protecting national interests in the past, but it might not be as able to in the future without significant change. Transformation would entail a “comprehensive reshaping of the skills and capabilities” and would begin immediately.

The Basis for Transformation

The panel concluded that transformation was an immediate priority because the factors influencing the 2010–2020 period were already unfolding. Transformation would provide future options across a range of military capabilities, which would then provide the Nation with the capacity either to dissuade potential competitors or, if dissuasion failed, to exercise one or more of those options in order to prevail in a conflict.

A transformation strategy, however, did not stipulate a new mission for DOD. The panel readily acknowledged that the missions

enumerated by the report did not constitute a radical departure from existing missions; indeed, DOD missions would remain largely unchanged. What would be different was the increasing complexity involved in executing them and the corresponding need for greater integration with other governmental agencies and international partners.

Before elaborating further on how DOD missions would change, the panel addressed a key QDR conclusion. The QDR report described the ability to conduct wars in two major theaters as a prerequisite construct; in contrast, the NDP saw that construct as an impediment. From the panel’s perspective, it left DOD postured too conservatively when more risk could be assumed to undertake transformation. Jettisoning the construct of conducting wars in two major theaters would allow DOD to adapt appropriately.

The panel identified six missions requiring attention:

- defending the homeland
- countering weapons of mass destruction
- maintaining space superiority
- developing information capabilities
- projecting military power
- preserving regional stability.

The panel acknowledged that the American military had always performed these missions, but the new era promised only more complex tasks as the one-dimensional threat of the Cold War was succeeded by

multifaceted and overlapping vulnerabilities and challenges.

The panel declined to propose revisions to existing legacy organizations and structures (that is, Army divisions), but instead urged the Services to emphasize new attributes: stealth, speed, greater range, leaner logistics, smaller footprints, and precision strike. Additionally, it observed that such future capabilities would be enhanced if the military applied new systems architectures and information technologies. In more audacious terms, the NDP contended that such advances would allow U.S. forces to “establish less manpower-intensive forces,” “see the battlespace in near real time,” and “dissipate the fog of war.”

Applying this perspective to specific acquisition plans, the panel’s assessment was blunt; it did not “follow the logic of several of the services’ procurements.” The panel questioned planned acquisitions and essentially counseled the Services go back and redo their homework. It acknowledged that proposed systems had potential—and endorsed some purchases as a risk-mitigation step—but advocated that each Service continue exploring new concepts and, above all, test them rigorously before initiating new acquisitions.

The Core of Transformation

In broad terms, the twin focuses of overall transformation would be institutionalizing change and reforming the approach to national security.

Engineering change as an inherent function would be achieved only by establishing entities that would undertake experimentation as an objective. To this end, the panel proposed the establishment of U.S. Joint Forces Command (USJFCOM) with the resources, authorities, and forces necessary to examine and test operational concepts and doctrinal innovations under realistic conditions. The panel warned that experimentation was absolutely critical because the advantage currently possessed by the Nation’s military could not be sustained without it.

The existing approach, born of the 1947 National Security Act, was simply no longer adequate. Establishing the foundation for an integrated and responsive interagency process would be imperative. Decisionmakers needed to synchronize the Defense and State Departments and to incorporate the perspectives of other Cabinet departments. The government needed to cultivate an interagency cadre of



Soldiers review mission details before departing in mine-resistant vehicles on route-clearing operation near Tikrit, Iraq

“national security professionals.” All facets of intelligence would have to be revitalized. The Unified Command Plan would have to be updated to reflect new priorities such as homeland defense and power projection by establishing an Americas Command and Logistics Command, respectively. Regional stability would be the overriding priority, and alliances would remain vital, but the ally would vary depending on the mission or might even be a nongovernmental organization.

In the end, the National Defense Panel submitted 85 recommendations⁷ and had its first opportunity to testify before Congress less than 8 weeks later on January 28, 1998.⁸

Just the week prior, however, the Monica Lewinsky scandal exploded, convulsing the Clinton administration and turning the American political environment upside down. National security matters remained in the headlines, but the opportunity for a substantive examination of defense transformation was lost. NDP members testified en masse again in March 1998, but they did not return to the Hill for the remainder of the year.

Transformation on Hold

The future of transformation turned on the outcome of the upcoming 2000 Presidential election. While both Vice President Al Gore and Texas governor George W. Bush promoted “transformation,” Bush was a forthright advocate. In a September 1999 speech, Bush pledged to “[create] the military of the next century” and echoed the panel’s recommendations.⁹ More fatefully, he promised to give his Secretary of Defense a broad mandate “to challenge the status quo.”

Bush won and selected Donald Rumsfeld to be his Defense Secretary. Rumsfeld had held this position before from 1974 to 1977 and had helmed the 1998 Commission to Assess the Ballistic Missile Threat, but was not necessarily recognized as a proponent of transformation as described by the panel. Rumsfeld’s priorities reflected his experience on the commission—missile defense—and in the private sector—improving management and undertaking Bush’s mandate to reform DOD.

Rumsfeld advocated change throughout his first year and, in a memorable speech to assembled Pentagon employees, warned that the enemy posing a “serious threat” to the

United States was not an adversary overseas, but DOD bureaucratic processes.¹⁰ The date of the speech was September 10, 2001; the very next day, al Qaeda executed its massive terrorist attack against the country. One month later, American forces were in Afghanistan.

The Rumsfeld Era

The attacks and stunning victory achieved by U.S. Special Forces on horseback calling in precision-guided munitions against Taliban and al Qaeda formations afforded Rumsfeld a second opportunity. He followed his September 10 speech with an even more audacious address on January 31, 2002, entitled “21st Century Transformation.”¹¹ He laid out six transformational goals for the United States—homeland defense, power projection, denying sanctuary to enemies, protecting information networks, achieving enhanced jointness via information connectivity, and achieving space superiority—all of which evoked original NDP conclusions.

On many fronts, Rumsfeld appeared to endorse the panel’s transformation strategy. He dismissed the two-major-theater construct as a hindrance. He advocated improving mili-

tary capabilities by becoming more joint and capitalizing on digital networks. He asserted that the development and possession of new capabilities would dissuade aspiring competitors. Lastly, he promoted a “culture of creativity and intelligent risk taking.”

Between 2001 and 2006, Rumsfeld emerged as the champion of the transformation the panel had advocated, and he implemented a number of changes.¹² He established the Office of Force Transformation and issued the first ever Transformation Planning Guidance in 2003. He accelerated missile defense development and deployment and initiated a comprehensive review of overseas posture. At his direction, the roles and responsibilities of functional commands increased vis-à-vis the geographic combatant commands, facilitating global interoperability. Rumsfeld initiated the reorganization of the Army force structure. He created U.S. Northern Command (USNORTHCOM) to coordinate defense of the homeland. Additionally, he established U.S. Africa Command (USAFRICOM) in recognition of that region’s growing importance. Furthermore, he directed USAFRICOM and U.S. Southern Command (USSOUTHCOM), responsible for Latin America, to be prototype interagency commands in which State Department and other key non-defense agency personnel are integrated into the command structure.

Despite these accomplishments, by the time Rumsfeld left the administration in 2006, transformation as an objective had been discredited. Why? While the obvious answer is frustration with difficulties in Iraq, Rumsfeld’s interpretation of transformation was salient in terms of its fate for three key reasons.

First, Rumsfeld asserted that transformation could not wait, insisting that the September 11 attacks and war on terror necessitated immediate action. In contrast, the NDP envisioned changes that would bear results in 2010. Second, Rumsfeld argued that his approach was necessary to prepare for conflict with future adversaries even if greater risk was being incurred in the present. The panel made a similar calculation, but not one countenancing comprehensive change while fighting two wars simultaneously overseas. Third, Rumsfeld equated transformation with the revolution in military affairs. He promoted networked forces and advanced weaponry even in the face of a “long, hard slog” because, as noted, he was prepared to accept greater

risk. The consequences became painfully apparent as the military scrambled to properly armor their vehicles amidst an increasingly deadly Iraqi insurgency. At a December 2004 town hall meeting with Servicemembers, Rumsfeld responded to comments about the

by the time Rumsfeld left the administration in 2006, transformation as an objective had been discredited

lack of armor with the now infamous statement, “You go to war with the Army you have. They’re not the Army you might want or wish to have at a later time.”¹³

With that statement, the future of transformation was sealed. Rumsfeld persisted for 2 more years, whereupon dissatisfaction with his leadership eventually lapsed into opposition against his entire agenda, including transformation.

After the Republican Party lost Congress in 2006, due in part to the stalemate in

Iraq, President Bush replaced Rumsfeld with Robert Gates, former director of the Central Intelligence Agency. Secretary Gates immediately established himself as the “un-Rumsfeld” and focused completely on implementing Bush’s surge strategy in Iraq. Nearing the end of Bush’s term, Secretary Gates began defining his priorities, railing against the “next-war-itis” rampant in the Pentagon, and signaled he would prepare more for present-day threats and less for hypothetical future adversaries. To this end, over initial Service objections he expedited the production of Mine-resistant Ambush Protected vehicles, which were armored fighting transports designed to survive roadside bomb attacks, and cancelled several major weapons programs, including the F-22 fighter.

President Barack Obama ended up retaining Secretary Gates. During the transition, Gates declared his intent to craft a “balanced” defense strategy.¹⁴ In February 2010, DOD released the 2010 QDR Report,¹⁵ which echoed Gates’s call for focusing on the current fight, rebalancing the force, and reforming business practices.



Airmen conduct postattack reconnaissance sweep during operational readiness exercise, Osan Air Base, South Korea

U.S. Air Force (Evelyn Chavez)

Transformation in Retrospect

After a purposeful attempt at transformation and 9 years of war, America now enters the 2010–2020 period that the National Defense Panel hypothesized about and planned for, and the principal question is whether the Nation is indeed prepared. Has America's security posture changed for the better? Does the Nation possess sufficient "options?" In discussing whether America is

Invariably, though, a panel member's assessment of America's preparedness for the next decade and the degree of transformation depended on whether the report's recommendations had been implemented. Members expressed pride that the group's efforts had succeeded in producing insights that have generally been validated by ensuing events. However, this pride was tempered when members conceded these insights remained

dum obtained by InsideDefense.com, the joint force training and experimentation functions would be transferred to the Joint Staff, with support roles going to the Services and other components as appropriate.)¹⁷

Reform the Broader National Security Approach. Panel members cited examples of progress, but they generally acknowledged that efforts to bolster interagency capacity are still in their infancy. Several members stressed the need for longer-range planning at civilian agencies. General RisCassi singled out Secretary of State Hillary Clinton for her leadership on this front, but he and others recognized that long-range planning remains a foreign concept. Moreover, panel members conceded that the government (and public) will remain predisposed to enlisting DOD resources until interagency capabilities mature. Panel members contended that enhancing civilian agency capabilities will require more resources and appropriate authorities, which in turn will require coordinated action from the executive branch and Congress. A few panel members grimly expressed the fear that only another catastrophic terrorist attack would prompt decisionmakers to act.

Separately, other members blamed the lack of progress on bureaucratic inertia. General Hearney asserted that incoming appointees and new hires have always been receptive to interagency collaboration; the resistance comes from lifelong employees. As long as the bureaucratic workforce—unlike the military—does not face penalties for shirking such guidance, it will continue to impede progress. Nolan agreed, blaming "pernicious" incentives at civilian agencies, and lamented that the government does not cultivate cross-disciplinary thinkers, "the George Marshalls of the world." Ambassador Armitage agreed, asserting that the Office of Personnel Management could accelerate change by making promotion dependent on interagency service. (On September 30, 2010, former House Armed Services Committee Chairman Ike Skelton and Representative Geoff Davis introduced the Interagency National Security Professional Education, Administration, and Development System Act of 2010. The measure is designed to provide incentives for national security professionals to undertake interagency training, education, and rotational assignments.)¹⁸

The Two-major-theater War Construct. DOD did not formally discard this construct until the 2010 QDR Report, and

invariably, a panel member's assessment of America's preparedness depended on whether the report's recommendations had been implemented

prepared for the 2010–2020 period as a result of efforts taken to transform, only one panel member responded yes. Four responded no, and the remainder characterized American preparedness for the next decade as mixed. Nevertheless, panel members identified a number of positive changes.

For example, every member of the panel praised the priority placed on homeland defense as evidence of positive transformation. Nearly every member applauded DOD for naming homeland defense as a primary mission and establishing USNORTHCOM to coordinate defense support of civil authorities. Furthermore, a number of panel members lauded steps taken to address information and cyber warfare, as well as critical infrastructure vulnerabilities. Furthermore, every panel member agreed that the Armed Forces have adapted to new missions and are better prepared for the types of conflicts likely to occur over the next decade. Janne Nolan noted that the extent to which the military has evolved can be inferred by recognizing how operations other than war are now deemed equally important. Panel members agreed that the military now places stability operations on par with combat operations, but also that substantial work remains.

Panel members conceded that technology would not completely "dissipate the fog of war"—especially when the battlefield includes "human terrain"—but contended that the employment of information technologies and architectures has inarguably improved overall military capabilities. Precision munitions are now the norm, and space- and terrestrially based intelligence, surveillance, and reconnaissance capabilities provide increasingly persistent battlefield coverage.

valid only because the corresponding recommendations had not been implemented. The dearth of follow-through on the part of the Clinton and Bush administrations and Congress frustrated a number of members.

This subtext is readily evident when the assessment turned to specific elements of the report.

Institutionalize Change. Regarding experimentation, panel members proudly pointed to the establishment of USJFCOM, as per the NDP report's recommendation, in 1999. While some expressed frustration that the wars in Afghanistan and Iraq had obligated the command (and the military in general) to focus somewhat exclusively on counterinsurgency doctrine, they enthusiastically endorsed broader and deeper experimentation.

General Hearney commended the leadership of the former USJFCOM commander, Marine Corps General James Mattis, characterizing him as a "real change agent." When asked which was more important—experimentation or doctrinal innovation, as exemplified by current General David Petraeus—General Hearney replied that the military should be stressing both.

Krepinevich articulated the need for more realistic experimentation, citing the shortcomings of Millennium Challenge 2002, where senior U.S. commanders overseeing the exercise called for a "do-over" to validate preferred operational concepts.¹⁶ (On August 9, 2010, Secretary Gates announced he would eliminate USJFCOM. In follow-up communications, panel members generally declined to comment because DOD has not yet identified how USJFCOM missions would be allocated. According to a September 1, 2010, memoran-

Marines offload from MV-22B Osprey at Camp Price, Helmand Province, in support of ISAF



U.S. Marine Corps (Christopher Matt)

panel members agreed that its passing was overdue. In revisiting this critique, a number of panel members admitted the construct was less about strategic considerations than about preserving existing budget allocations. One member anecdotally recalled how then-Secretary of Defense William Cohen was typically receptive to the panel's findings except when they concerned adjustments to the construct—underscoring the “sacrosanct” nature of the defense budget.

Panel members acknowledged that force structure planning can be difficult in such an environment. Admiral Jeremiah captured the sentiment by noting that planners have to contend with a security environment dominated by “lots of littles.” Nevertheless, the final report declined to outline a specific force structure for this reason: transformation would instead provide future decisionmakers with options amidst strategic uncertainty.

General RisCassi recommended that decisionmakers revisit the 2006 QDR Report “quad chart” to understand the kind of options required for the next decade. Similarly, Admiral Jeremiah asserted that future

force structure planning would have to be informed by a wider range of scenarios—for example, the implosion of nuclear-armed Pakistan, a veritable “Pakistani Missile Crisis”—far more complex than major theater war.

Adaptability as an Organization.

While the report outlined how DOD could become a more flexible organization, more than one panel member admitted DOD is capable of only so much change. Members acknowledged that Rumsfeld and Gates demonstrated DOD can change course, but asserted the static nature of Service budget allocations remains a stark reminder of just how difficult it is to bring about greater organizational flexibility.

Odeen praised the lead taken by the combatant commands in regard to innovation, citing USSOUTHCOM for fashioning a coordinated political-military approach and U.S. Central Command (USCENTCOM) for successfully introducing new doctrine and pioneering the use of unmanned technologies. However, he acknowledged the success and influence achieved by the combatant commands (such as USCENTCOM) reflect an

endorsement that will lapse once operations end. Alternatively, if the future does entail “persistent conflict,” then DOD should be prepared to extend this sanction, especially

more than one panel member admitted DOD is capable of only so much change

regarding acquisition, which Mr. Odeen characterized as “too cumbersome, too slow.”

When asked whether recent acquisition reform would facilitate broader organizational reform, Odeen responded only if it spurs less “rigidity” in requirements generation. He endorsed the recommendations contained in the October 2008 Defense Business Board report and strongly urged DOD to revise its requirement development process.¹⁹ He argued more oversight will not result in the responsiveness modern warfighters need, so they will instead continue looking for “workarounds.”

Technology as Force Multiplier. Most panel members remained proponents of

U.S. Navy (Kilho Park)



Aircraft director guides F/A-18C Hornet onto catapult aboard USS Harry S. Truman

capitalizing on opportunities offered by technology, even though recent operations against insurgents have demonstrated the limits of a technologically enhanced revolution in military affairs. Panel members asserted the salient risk lies in becoming overly reliant on technology. Digital connectivity may have facilitated wider, more distributed operations, but greater emphasis should be placed on training units to operate when the network is degraded or nonexistent. Krepinevich asserted the Services are increasingly aware of this risk and are taking steps to mitigate it, but General Hearney feared that the United States is already too dependent on technology. If DOD fails to prepare units to operate without existing technological tethers, it runs the greater risk of units micromanaged by “tactical generals” and incapable of exercising initiative.²⁰

Homeland Defense. As already noted, every panel member considered the report’s conclusions on the mark. However, when asked whether the panel had considered recommending a Cabinet-level department, virtually every member answered no. In retrospect, General RisCassi stated that the

panel could have recommended a sub-Cabinet agency dedicated to homeland defense within DOD.

In discussing the Department of Homeland Security (DHS), a number of members asserted that every organization will endure “growing pains.” In general, integrating entities with similar objectives should generate efficiencies, but the history of such mergers, especially within the government, should have induced caution. Ambassador Armitage commented that any entity tasked with such an enormous responsibility should not have been created overnight. Odeen and McCarthy considered the establishment of DHS an unnecessarily accelerated attempt to combine unlike organizations. McCarthy observed that an entity like the Coast Guard remained effective only because it retained its original culture and mission.

Ambassador Armitage argued that homeland security should have been distributed across and made the principal mission of multiple agencies. He characterized challenges on the U.S. border with Mexico as a virtual “narco-insurgency” in need of

dedicated attention, and asserted DHS is simply too cumbersome to address the matter effectively. Moreover, he argued the National Guard is “ready-made” for the homeland defense mission and has been “underutilized” on this front.

Regional Stability. Every panel member also stood by the report’s characterization of regional stability as an “overriding priority.” All members stressed that the United States needs to remain engaged globally and present in every region. Numerous members reiterated how access will remain a challenge and, therefore, securing the global commons, maintaining a forward presence, and developing sea-basing capabilities remain priorities.

In discussing regions aside from Asia, Odeen criticized the Bush administration for letting commitments in Afghanistan and Iraq undermine meaningful engagement with Latin America. The dearth of American attention has allowed Chinese influence and the rising profile of anti-American Venezuelan dictator Hugo Chavez to grow unchecked. He also contended that Africa would become

more critical to global economic and security considerations over the next 10 to 15 years.

Nolan commented that the focus on regional stability and specific countries reflected a traditional state-centric view of affairs that precluded fully anticipating the rise of transnational networks or substate actors such as al Qaeda and Hizballah. In retrospect, the panel did not fully appreciate how such entities possessed an agility that defies a strictly regional approach. The panel could not have predicted the speed with which these entities would accrue capabilities to prepare for and wage war—virtually comparable to those once exclusively held by states, but without the encumbrance of strictures or norms that constrain sovereign governments.

Importance of Diplomacy and Alliances. Panel members also unanimously reaffirmed the criticality of diplomacy and alliances. Odeen asserted the panel's conclusion is "still valid" and "even more so" in the present day; in his view, the experience in Iraq underscore the perils of acting unilaterally. Krepinevich acknowledged an investment in an alliance will "plateau" over time, but explained that diplomacy and alliances remain fundamental components of the Nation's security portfolio. Going forward, America should be exploring opportunities for bilateral and multilateral arrangements in Asia and be prepared to employ nontraditional cooperative arrangements. Ambassador Kimmitt echoed the point by urging the United States to capitalize on the opportunities presented by the Group of 20. Matters such as the global economy are best addressed through multilateral diplomatic forums, and success in this arena would enhance the prospects for diplomatic initiatives in other areas.

Unified Command Plan. While most panel members commended the establishment of USNORTHCOM and U.S. Cyber Command as belated validation of the report's focus on defending the homeland and information networks, some signaled their dissatisfaction with the current Unified Command Plan. For example, Admiral Jeremiah and General RisCassi recommended that all national security agencies operate from a uniform map. Reviewing Defense and State Department "area of responsibility" maps reveals that the Indian Ocean is under the jurisdiction of seven entities.²¹ Coordinating across three combatant commands is difficult enough without having to coordinate with four additional stakeholders in the State

Department.²² If diplomatic and military capabilities are to be wielded harmoniously, then their geographic perspectives should be synchronized at a minimum.

Other members lamented the continuing emphasis on arbitrary (and sometimes inexplicable) geographic divisions. Homeland defense and regional stability are valid objectives, but organizing according to functional missions will benefit the warfighter—as more adversaries operate transnationally and in

the proficiency with which the military now addresses challenges other than war underscores the failure of diplomats to initiate missions "other than diplomacy"

cyberspace, the less effective geographically organized commands will be. Citing the old adage that "amateurs talk strategy, while professionals talk logistics," General Hearney commented that "lines on a map" can be an unfortunate distraction from focusing on what should be military leadership's foremost priorities—enhancing global projection and acting with agility and speed.

America remains unprepared for the next decade because transformation as outlined by the panel remains incomplete, as DOD efforts to prepare for the upcoming decade have not been matched by equivalent transformation in the nondefense components of the government.

DOD has changed significantly over the past 13 years—while executing two major wars for more than half that period. Indeed, the challenges arising from operations in Afghanistan and Iraq are what have led DOD to encourage and promote similar adaptation by nondefense government agencies. DOD guidance is replete with provisions describing how it is ready (and prefers) to work in conjunction with civilian "partners." Secretary Gates has even taken the unprecedented step of advocating more resources for State.²³ Nonetheless, a comparable level of effort on the part of the civilian departments to envision possible futures and adapt accordingly has not occurred until recently. DOD just completed its fourth quadrennial review, while State and Homeland Security have just undertaken their first. The National Security and Homeland Security Councils only merged in the last year, and they still lack representatives from Treasury and other agencies that have stakes in the conduct of

security affairs.²⁴ Successive administrations have missed opportunities to improve whole-of-government decisionmaking and preparedness for the next decade and have suffered as a consequence.

The impetus for an enhanced inter-agency approach received renewed momentum when the Project on National Security Reform (PNSR) formed in 2006. Many hoped that it would define how "jointness" could be achieved across the entire government.

PNSR's final report was well received, and numerous stakeholders went on to prominent positions in the current administration, but its impact has been minimal.²⁵ PNSR's 28 recommendations constituted the basis for a redesign of the U.S. national security system, but the report cautioned against incremental implementation, warning that compromises would only delay the emergence of problems, would shift them from one place to another, or worse, would not even work.

To recall, the National Defense Panel saw the opportunity for transformation differently. Instead of wholesale change, transformation constituted incremental change via new missions, approaches, and experimentation. If the opportunity for meaningful transformation is minimal, then perhaps the more practical approach would be to place greater attention on improving the frontline national security practitioner, the likeliest engine for eventual reform. Observations from three panel members stand out in this regard.

General RisCassi declared that joint professional military education is the "soul" of the Armed Forces and that deployment policies practiced during the past decade have "emasculated" it. He denounced steps such as postponing educational enrollments and reducing terms at Fort Leavenworth from 1 year to 6 months. He argued such disruptions would have long-term consequences and asserted educational commitments should be upheld, even during times of war. If constructing a "balanced" force is a priority, a Servicemember's education would remain a critical building block.

Nolan posited if Soldiers and Marines can simultaneously wage war, enforce peace,

and oversee development, the time has come for State and related agencies to cultivate diplomats prepared to undertake similar missions and deploy overseas. More pointedly, the proficiency with which the military now addresses challenges other than war underscores the failure on the part of diplomats to initiate missions “other than diplomacy.” Nolan argued diplomacy in the future would not entail presiding over negotiations or tours at Embassies, but serving in the field—supervising agricultural production and evaluating local police forces—in the same fashion as Soldiers and Marines. Until diplomats meet the military halfway in becoming “hybrid” warrior-diplomats, the Nation will never bring to bear a fully whole-of-government approach to future challenges.

Bolstering military education may not inspire the same zeal as reforming America’s national security structure, but making such a commitment is equally necessary to prepare for the challenges awaiting the country. An expeditionary stability corps may never achieve the same level of acclaim as the 82^d Airborne, but establishing one will probably be just as critical in the next decade.

According to General Hearney, the last best opportunity to achieve meaningful change may be with the imminent close of operations in Iraq and Afghanistan: “If we miss this opportunity, then shame on us.” He asked would-be agents of change to hold fast and asserted that “we should . . . always be prepared to blow things up.”

In the final analysis, lasting change will emerge from the souls of the Nation’s future warrior-diplomats.

Epilogue

On July 29, 2010, a bipartisan panel led by former National Security Advisor Stephen J. Hadley and former Secretary of Defense William J. Perry released a report entitled “The QDR in Perspective: Meeting America’s National Security Needs in the 21st Century,”²⁶ featuring a congressionally mandated critique of DOD’s 2010 Quadrennial Defense Review. The Perry-Hadley Panel issued stark warnings about the state of the All-Volunteer Force and recommended that the United States embrace a *whole-of-government* approach that would rebalance civilian and military capabilities within the Government and a *comprehensive approach* that would enhance the Nation’s ability to collaborate with select partners,

international organizations, and nongovernmental and private voluntary organizations when possible.

The journey continues. **JFQ**

NOTES

¹ The author interviewed the nine members of the National Defense Panel (NDP) between December 2009 and June 2010.

² The Commission on the Roles and Missions of the Armed Forces of the United States, *Directions for Defense* (Washington, DC: Department of Defense, May 1995).

³ Department of Defense (DOD), *Report of the Quadrennial Defense Review* (Washington, DC: DOD, May 1997).

⁴ National Defense Authorization Act for Fiscal Year 1997, Public Law 104–201, Title IX, subtitle B, sections 921–926.

⁵ NDP, “National Security in the 21st Century: The Challenge of Transformation,” *Joint Force Quarterly* 16 (Summer 1997), 15–19.

⁶ NDP, “Transforming Defense: National Security in the 21st Century, Report of the National Defense Panel,” December 2007, available at <www.dtic.mil/ndp/FullDoc2.pdf>.

⁷ *Ibid.*, “Specific Recommendations,” available at <www.dtic.mil/ndp/comments/specrec.pdf>.

⁸ Senate Committee on Armed Services, Hearing on the National Defense Panel Report, 105th Cong., 2^d sess., 1998.

⁹ George W. Bush, “A Period of Consequences,” speech given at The Citadel, Charleston, SC, September 23, 1999, available at <www.citadel.edu/pao/addresses/pres_bush.html>.

¹⁰ Donald H. Rumsfeld, “DOD Acquisition and Logistics Excellence Week Kickoff—Bureaucracy to Battlefield Remarks,” speech given at the Pentagon, Arlington, VA, September 10, 2001, available at <www.defense.gov/utility/printitem.aspx?print=http://www.defense.gov/speeches/speech.aspx?speechid=430>.

¹¹ Donald H. Rumsfeld, “21st Century Transformation of U.S. Armed Forces,” speech given at the National Defense University, Fort Lesley J. McNair, Washington, DC, January 31, 2002, available at <www.defense.gov/utility/printitem.aspx?print=http://www.defense.gov/speeches/speech.aspx?speechid=183>.

¹² Robert D. Kaplan, “What Rumsfeld Got Right: How Donald Rumsfeld Remade the U.S. Military for a More Uncertain World,” *Atlantic Monthly* 302, no. 1 (2008), available at <www.theatlantic.com/magazine/print/2008/07/what-rumsfeld-got-right/6870/>.

¹³ Donald H. Rumsfeld, “Town Hall Meeting in Kuwait,” Camp Buehring, Kuwait, December 8, 2004, available at <www.defense.gov/utility/printitem.aspx?print=http://www.defense.gov/speeches/speech.aspx?speechid=183>.

¹⁴ Robert M. Gates, “A Balanced Strategy: Reprogramming the Pentagon for a New Age,” *Foreign Affairs* (January–February 2009), 28–40.

¹⁵ DOD, *Report of the Quadrennial Defense Review* (Washington, DC: DOD, February 2010).

¹⁶ In 2009, Dr. Krepinevich published “Seven Deadly Scenarios,” in which he argued for revitalizing USJFCOM. He recommended extending the USJFCOM commander’s tenure, requiring at least one major joint field exercise a year, establishing a standing joint opposing force at each training center, and granting USJFCOM major force program budgetary authority.

¹⁷ “OSD Memo on JFCOM Disestablishment Working Group,” October 14, 2010, available at <<http://insidedefense.com/201010132341518/Defense-Plus/File-Document/osd-memo-on-jfcom-disestablishment-working-group/menu-id-77.html>>.

¹⁸ House Committee on Armed Services, “Skelton, Davis Introduce Groundbreaking Interagency Reform Legislation,” news release, September 30, 2010, available at <http://armedservices.house.gov/apps/list/press/armedsvc_dem/SkeltonPR093010.shtml>.

¹⁹ Defense Business Board, Report to the Secretary of Defense, *Capability Requirements Identification and Development Processes Review*, Report FY09–2, *Recommendations to Improve Joint Capability Requirements Identification and Development Processes*, Washington, DC, October 2008.

²⁰ P.W. Singer, “Essay: The Rise of the Tactical General,” *Armed Forces Journal*, June 2009, available at <www.armedforcesjournal.com/2009/06/4036660/>.

²¹ “Department of Defense—Department of State Areas of Responsibility,” *Joint Force Quarterly* 53 (2^d Quarter 2009), 131.

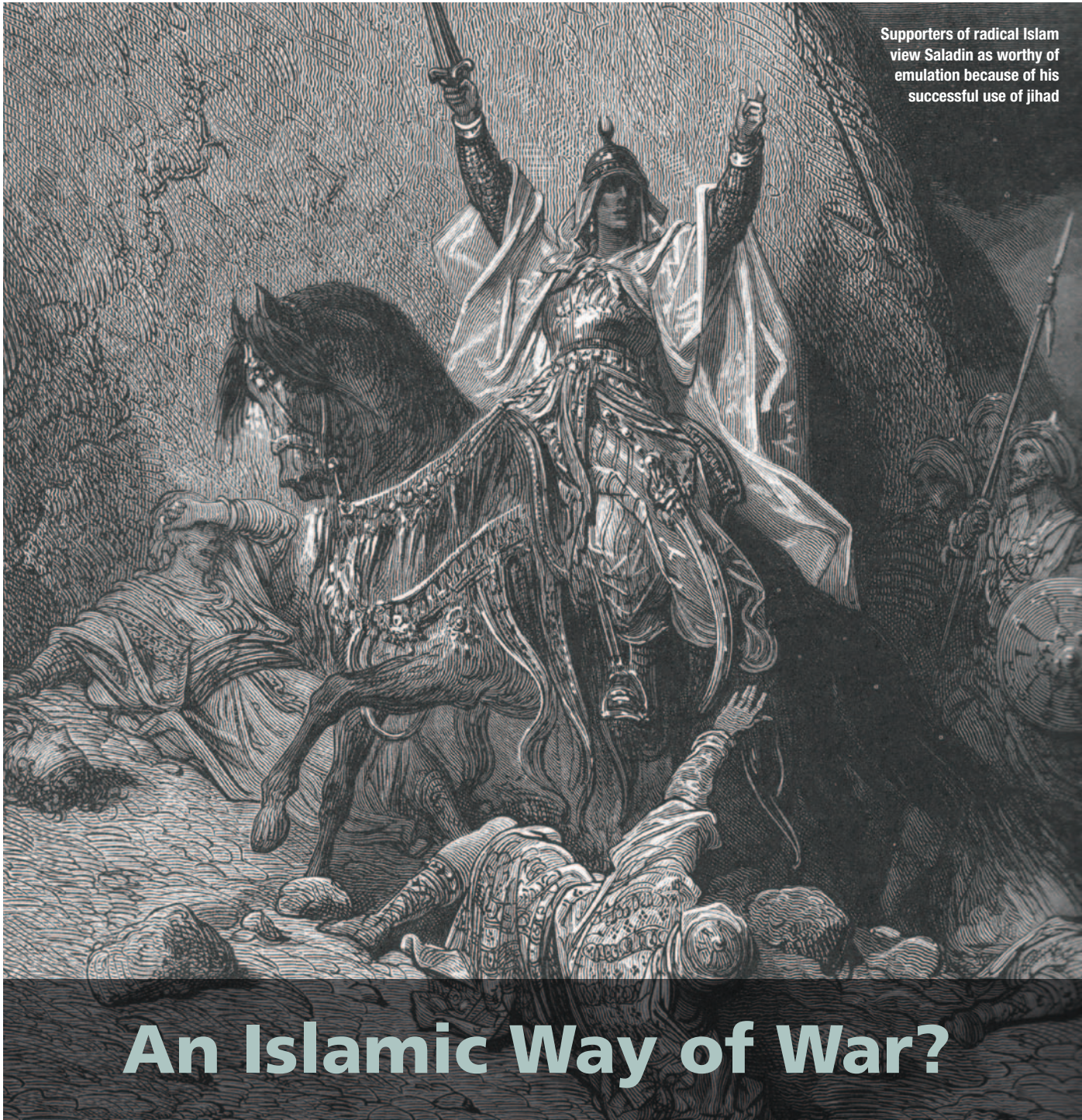
²² R. Jordan Prescott, “Indian Ocean Command,” House of Marathon, July 27, 2009, available at <<http://houseofmarathon.blogspot.com/2009/07/090731indianoceancommand-printer.html>>.

²³ Robert M. Gates, “Landon Lecture,” Kansas State University, Manhattan, KS, November 26, 2007, available at <www.defense.gov/speeches/speech.aspx?speechid=1199>.

²⁴ Presidential Study Directive 1, “Organizing for Homeland Security and Counterterrorism,” February 23, 2009, available at <<http://www.fas.org/irp/offdocs/psd/psd-1.pdf>>.

²⁵ Project on National Security Reform (PNSR), *Forging a New Shield* (Washington, DC: PNSR, December 2008), available at <<http://pnsr.org/data/files/pnsr%20forging%20a%20new%20shield.pdf>>.

²⁶ Quadrennial Defense Review Independent Panel, *Meeting America’s National Security Needs in the 21st Century* (Washington, DC: U.S. Institute of Peace, July 29, 2010), available at <www.usip.org/files/qdr/qdrreport.pdf>.



Supporters of radical Islam view Saladin as worthy of emulation because of his successful use of jihad

Wikipedia (Gustave Dore)

An Islamic Way of War?

University of Texas Library



By ADAM OLER

Great Islamic conquests occurred during reigns of Four Rightly Guided Caliphs

Is one to assume that there is an Islamic mode of war different, say, from Christian warfare?¹

—Edward Said

Well before Saddam's final defeat, others, less stupid, began to develop alternative means of what they called "resistance." This new Islamic Way of War evolved over a period of decades not only in the Arab world but beyond.²

—Andrew J. Bacevich

I sincerely believe, and my belief is borne by historical facts, that just as there is no Christian Chemistry or Jewish Physics or Hindu Ballistics, there is no such thing as Islamic Warfare.³

—Mehtar Omar Kahn

The trio of quotations in the epigraph reflects an important debate over whether there is such a thing as "an Islamic way of war." The question surfaced 32 years ago when Edward Said published his celebrated and controversial book *Orientalism*. Several years earlier, *The Cambridge History of Islam* made reference to a "manner of warfare which can be described, in a meaningful sense, as Muslim."⁴ Said took offense and added the Cambridge History's assertion to a long list of what he considered ill-informed generalizations about the Islamic world.⁵ The matter remained largely dormant until 9/11 made topics regarding Islam critical to U.S. policy-makers. The question is certainly no longer academic as the West struggles with Islamist terrorists and wars in Iraq and Afghanistan. If there is an Islamic way of war, the United States needs to recognize it in order to plan

Colonel Adam Oler, USAF, is a Student at the National War College and a Member of the Judge Advocate General's Corps.

effectively. If not, care must be taken to avoid the invention of a false paradigm that could lead to flawed assumptions. Fortunately, by analyzing key periods of Muslim military history, and by carefully considering each side's arguments, one can clearly discern where the truth lies. Simply put, there is no such thing as an Islamic way of war.

For purposes of this article, the term *way of war* refers to an institutionalized approach to warfare that is essentially unique, definable, and therefore recognizable. That societies can possess such an approach to warfare is not a new concept. The late historian Russell Weigley defined an "American Way of War" 35 years ago, describing it as one tending toward "annihilation" of the enemy.⁶ More infamously, the Nazis created their own distinct way of war premised on ultranationalist, racist principles carried out through mass murder.⁷

So where should one look for an Islamic way of war? Three key periods in Muslim military history—the early Islamic conquests, the Crusader and Mongol era, and the gunpowder empires through the postcolonial age—lend great insight to the question at hand. Scrutinizing arguments made by proponents of an Islamic way of war definition further helps resolve this important query. Finally, it is

erence works provided some coverage,¹³ for a long time key details remained obscure.¹⁴

Fortunately, Islamic military events of the pre-Crusader period are becoming more accessible, and it is possible to draw some conclusions about their character.¹⁵ The latest histories reveal that the Muslim soldiers who exploded out of the Arabian Peninsula conducted brilliant campaigns, capturing territory extending 7,000 kilometers.¹⁶ Although tremendous in scale, there is nothing exceptionally "Islamic" about why the early Muslim armies proved so successful. That is, their achievements resulted from circumstances and actions seen in similar periods of great conquest. First, the Muslim generals exploited the fact that their two enemies, the Byzantines and Sassanids, had just exhausted themselves¹⁷ in what proved to be the last great war of antiquity.¹⁸ In the decades leading to Mohammed's death in 632, the Sassanids conquered most of the Levant, only to have it retaken by the great Byzantine general Heraclius.¹⁹ During the war, the Byzantines and Sassanids suffered tremendously from plague, exhausting them further still.²⁰ Eventually, the two superpowers' borders returned to the status quo ante,²¹ but when the great Islamic conquests began, the Muslims found themselves filling a power vacuum much like

there is nothing exceptionally "Islamic" about why the early Muslim armies proved so successful

essential to examine why this issue is far more than an academic exercise. Rather, it is a topic of immense importance to U.S. strategists.

The Great Conquests

When searching for evidence of an Islamic way of war, a fitting point of departure is Islam's first century. After the Koran and examples set by the Prophet (*Sunnah*)⁸ as recorded in the *Hadith*,⁹ the most important source of moral guidance for Muslims comes from the "combined reigns" of the four Rightly Guided Caliphs (*Rashudin*).¹⁰ Ruling between 632 and 661 CE, their accomplishments proved instrumental to the foundation of Sunni Islam.¹¹ Because the great Islamic conquests largely occurred during *Rashudin* rule, these campaigns are central to Islam's earliest epoch. Until relatively recently, however, early Islamic military history received minimal attention from Western authors.¹² Although a few comprehensive ref-

the Macedonians after the Peloponnesian War.²² The Muslims likely knew of their enemies' weakness, since Arab frontier forces actively participated in the conflict along the Byzantine-Sassanid border.²³ The Muslims then exploited this weakness maximally.

Although Muslim forces fought with inspiration garnered from their new faith, the role of religious zeal should not be overstated. When the second Caliph, Umar, broke out of Arabia, he did so without a perceived "divine mandate to conquer the world."²⁴ In fact, his concerns were "pragmatic," echoing his army's motivation, which hinged on financial and territorial gain.²⁵ Success also stemmed from a number of other factors. For example, the Caliph's highly mobile forces traveled without a supply caravan, fought skillfully at night, and selected leaders based on merit.²⁶ Because of their small size and awareness of their own managerial limits, they left the local government bureaucracies in place.²⁷

Additionally, they did not billet their forces among the conquered population,²⁸ but chose to build garrison cities from which they could maintain order.²⁹ Furthermore—and this point is key—they did not forcibly convert the local population to Islam.³⁰ Instead, they afforded a type of protected (*dhimmi*)³¹ status to the conquered population, which had to pay a poll tax (*jizya*)³² and recognize Muslim authority over their territory in exchange for protection from external invaders and excusal from military service.³³ Because of contemporary schisms within the Christian segment, the conquered populations in the West frequently disdained Byzantine rule,³⁴ resulting in a lack of support for Byzantine forces³⁵ and, occasionally, outright support for the invaders.³⁶

The Arabs' comparatively enlightened approach toward conquered populaces proved instrumental to success as well, particularly the decision allowing Jews and Christians to keep their houses of worship.³⁷ Massacres of defeated forces refusing to surrender occurred, but not wholesale slaughter of civilians.³⁸ And although Western authorities once argued that Muslim operations at this time were "of an unsophisticated kind,"³⁹ this conclusion is undermined by the work of more recent scholars.⁴⁰ In fact, on close examination, little distinguishes early Arab armies from other medieval forces.⁴¹ Indeed, their applied use of archers, infantry, and cavalry approximated English tactics of the 14th century.⁴²

What, then, does this review of the military events during Islam's most formative period reveal? In short, it shows nothing intrinsically "Islamic" about the great Muslim conquests from which one could discern a uniquely Islamic way of war. On the contrary, the remarkable achievements of the Muslim armies resulted from the same combination of factors that other successful states have used throughout history. Astute leadership, an ideologically (in this case religiously) motivated force, vastly weakened enemies, and clever interaction with conquered peoples brought Islam its tremendous victories. No doubt strategic lessons can be gleaned from this period, but a unique, identifiable Islamic approach to warfare cannot.

Crusader and Mongol Periods

Searching for evidence of an Islamic way of war during the era of early conquests is important because of the period's seismic meaning for Muslims everywhere. Undeni-



Mongol destruction of Baghdad in 1258 ended over 500 years of continuity under Abbasid Caliphate

ably, Muslims view the great conquests as "miraculous proof of historic validation" for their faith.⁴³ Therefore, if a distinctly Islamic approach to warfare had developed during this period, it may well have become part of Islamic culture. The next era, that of the Crusades and Mongol invasions, is also important, but for different reasons. During this period, three giant figures in Muslim history emerged, each with his own relevance for Islam today. The first, Saladin, is closely associated with the Crusades. The second, Abu Hamid Al Ghazali, is Islam's most important philosopher. The third is Taqi al-Din Ibn Taymiyya, whose interpretation of jihad laid the foundation for today's radical Islamists.

Saladin's invocation of jihad merits examination given the significance placed on

the Crusades by a number of Muslim leaders⁴⁴ and Islamists.⁴⁵ Jihadis in particular exhort Muslims to see the Crusades as part of an ongoing "cosmic war"⁴⁶ pitting Christianity against Islam.⁴⁷ They view those wars, which began in the 11th century, as a struggle that will not end until Islam's final victory.⁴⁸ Among supporters of radical Islam, Saladin is seen as a figure most worthy of emulation because of his successful use of jihad,⁴⁹ a view unquestionably held by Osama bin Laden.⁵⁰

By invoking jihad against the Crusaders, did Saladin create a uniquely Islamic approach to warfare? Although he instilled a heightened resolve in his forces by calling upon them to wage holy war, the notion of fighting for a religious purpose is hardly unique to Islam. Consider, for instance, the early example of

Joshua's capture of Canaan in the 13th century BCE. Israeli historian (and former President) Chaim Herzog concludes that victory was ultimately "vouchsafed" because the ancient Israelites "were imbued with the belief that Canaan was theirs by injunction of their god."⁵¹ For more corroboration, one need only reflect on the European wars of religion

was already decaying. Today, Al Ghazali is viewed as a leading agent of this decline, and some blame him for what they call the "closing of the Muslim mind."⁶³ Whether true or not, it would be hard to overstate Al Ghazali's importance to the Muslim world, where his personal sobriquet has long been "Reviver of the Faith."⁶⁴ Even his detractors

Ibn Taymiyya promulgated a revolutionary philosophy that transformed the concept of jihad

during the 1618–1648 Thirty Years' War, the most destructive war on that continent between the Mongol invasions and the Napoleonic era.⁵² Clearly, the impact of Saladin's victories would be hard to exaggerate, especially since the Ayyubid state that he created stopped advancing Mongol forces before they could reach the Mediterranean and conquer Egypt.⁵³ That said, nothing Saladin did can be fairly described as a distinct, uniquely Islamic method of warfare.

Although Saladin and the Crusades receive far more attention in the West,⁵⁴ the Mongol invasions had a greater impact on Islam. While World War II is often described as the most devastating in history,⁵⁵ the destruction wrought upon the Muslim world by the Mongols is comparable. A new Islamic history describes the Mongol invasions as "genocide," and with good reason.⁵⁶ The Mongols razed countless cities, many never to be rebuilt,⁵⁷ and may have slaughtered as many as 18 million people.⁵⁸ In 1258, they destroyed Baghdad and killed the last Abbasid Caliph, ending a period of continuity that had endured for 508 years.⁵⁹ So total was the destruction that parts of the vanquished area never completely recovered.⁶⁰ From this terrible age emerged two key philosophers, Abu Hamid Al Ghazali and Taqi al-Din Ibn Taymiyya. Because of their tremendous influence today, their teachings are well worth considering when searching for an Islamic way of war.

During the pre-invasion period, the Muslim world experienced what is often called its Golden Age. Significantly, Muslim society preserved and largely adopted Hellenistic thought, to include rationalist interpretations of the Koran.⁶¹ Islam's contributions to the world during this epoch range from the invention of algebra to the creation of musical notes.⁶² However, by the time the Mongols appeared, this enlightened period

recognize him as a "titanic figure" and "the second most important person in Islam, next only to Muhammad."⁶⁵ Because of the trauma that engulfed the Muslim world shortly after his death, Al Ghazali's conservatism came to dominate Sunni Islam,⁶⁶ a domination it has yet to yield.⁶⁷

Al Ghazali's writings incorporated comments on military matters, including the role of the army in society. He envisioned a three-tier social caste, placing soldiers in the second, and believed they should be paid by the state's central treasury.⁶⁸ He placed tremendous value on maintaining order⁶⁹ and described government service—to include soldiering—as the highest profession.⁷⁰ Because avoidance of intra-social civil war (*fitna*)⁷¹ was paramount to him, he believed that so long as a sultan controlled the army, he needed to be obeyed no matter how "evil-doing and barbarous."⁷² Al Ghazali also wrote on the subject of military necessity, explaining that it was only legitimate to kill Muslims taken hostage if a matter was so vital that "all or nearly all Muslims [would otherwise face] extinction."⁷³ He was far less concerned for non-Muslims; for example, he prescribed very poor, even abusive treatment for those with *dhimmi* status.⁷⁴ Nonetheless, nothing exists in Al Ghazali's teachings that prescribes a uniquely Islamic way of war. Perhaps the best evidence for this conclusion rests in the fact that he is apparently without influence among modern Islamist extremists.⁷⁵ At least in this sense, Ibn Taymiyya is his complete opposite.

Al Ghazali had a tremendous and unrivalled impact on Islam. By comparison, Ibn Taymiyya's influence was marginal for centuries.⁷⁶ He was considered dangerous and was frequently jailed,⁷⁷ and his teachings on jihad all but disappeared until the 20th century.⁷⁸ Because of their recent resurgence in the hands of Islamists, however, Ibn Taymiyya's thoughts warrant close consideration.⁷⁹

Unlike Al Ghazali, who predated the Mongol occupation, Ibn Taymiyya lived through it.⁸⁰ What Ibn Taymiyya witnessed had a profound impact on him, and, during his long life, he wrote hundreds of books on Islamic jurisprudence.⁸¹ Most importantly for our purposes, he promulgated a revolutionary philosophy that transformed the concept of jihad from a predominantly spiritual, reflective, and defensive concept into a metaphorical sword aimed at the region's Mongol occupiers.⁸² Although the Mongols converted to Islam shortly after they arrived, and even though they governed the region where he lived, Ibn Taymiyya nonetheless deemed them apostates.⁸³ Under his aggressive interpretation of jihad, he concluded that the population had an obligation—to rebel against Mongol rule or risk being declared apostates (and thus killed) themselves.⁸⁴ Nothing in Islamic jurisprudence or philosophy to that time supported his position.⁸⁵ On the contrary, his notion of jihad was antithetical to virtually all interpretations that had gone before.⁸⁶

Ibn Taymiyya's influence on radical Islam is unmistakable,⁸⁷ and he is cited as its "favorite" philosopher—including by those who believe there is an Islamic way of war.⁸⁸ He definitely promulgated a concept of war that was unique, definable, and therefore distinguishable, but it was only applicable within Islam itself. At its root, his concept of jihad undermined a central tenet of Islam that forbade the killing of fellow Muslims, and thus many today consider his teachings heretically un-Islamic.⁸⁹ By "plant[ing] a seed of revolutionary violence in the heart of Islamic thought,"⁹⁰ however, he introduced a legal justification for rebellion that Islam had been missing. Ibn Taymiyya's teachings do not represent a concept of war that is unique to Islam. Rather, they represent a fundamental incongruity with a key pillar of Islamic jurisprudence.

Erosion of Distinctions

The gunpowder empires that emerged in Turkey, Persia, and India following the Mongol cataclysm brought a renaissance to Islam's ravaged lands. Each created astonishing societies, perhaps represented best by the great edifices of Istanbul, Isfahan, and Agra.⁹¹ Arguably, the period's most important legacy was Muslim expansion into East Asia, bringing Sunni Islam to Indonesia and beyond.⁹² Yet because this immense expansion occurred peacefully,⁹³ it offers little to consider in terms of an Islamic way of war.

Of course, wars did occur among these Muslim states and between Ottoman Turkey (in particular) and its Western neighbors. Beginning in 1317, at least 29 major engagements took place between Ottoman and Christian forces, culminating in the Ottomans' 1683 high water mark at Vienna.⁹⁴ An additional seven significant engagements transpired between them prior to Napoleon's invasion of Egypt in 1798⁹⁵ and the start of the colonial era.⁹⁶ Unlike the great Islamic conquests, military developments of these periods customarily receive a great deal of attention. What is most remarkable is the extent to which the armies of the Muslim and Europeans empires tended toward similarity and away from meaningful distinction.

When the Ottomans first established their standing army, Byzantine influence was already quite strong.⁹⁷ After gunpowder and artillery made their way into the Ottoman armies in the 14th century, the Europeans followed suit.⁹⁸ Then, as the European powers strengthened, weaponry began to flow in the other direction. Indeed, Bernard Lewis concludes that "[b]y far, the most important contribution of the West to life—and death—in the Islamic world" was in the form of weapons.⁹⁹ Once the military fortunes of the gunpowder states declined, both the Ottoman Turks¹⁰⁰ and the Qajar Persians¹⁰¹ strove to emulate their Christian counterparts by hiring advisors from across Europe. Although they did not abandon Islamic symbols or trappings, from the 18th century onward, Muslim armies strove to recreate themselves exclusively on European models.¹⁰² As a result, during the gunpowder and colonial periods, there was a steady march *away* from a distinctively Islamic way of war. Even *The Cambridge History of Islam* that so offended Edward Said concluded, "[t]he manner of warfare which can be described, in a meaningful sense, as Muslim" became obsolete and ceased to exist after this period.¹⁰³

The march toward symmetry continued beyond the colonial period and into the modern era. Kenneth Pollack's *Arabs at War* is replete with examples of Soviet aid to Muslim armies, which ran the gamut from equipment to training to doctrine.¹⁰⁴ Pollack also provides numerous examples of like support from the United States, and smaller instances of assistance from Great Britain and France.¹⁰⁵ What is particularly telling about Pollack's work is the apparent irrelevance of Islamism for these forces. Instead, national-

ism, far more than religion, motivated Arab armies as they went into battle.¹⁰⁶ By the end of the 20th century, the militaries of the Middle East, including their overall approaches to warfare, had developed into near-mirror images (even if far less capable images) of their Western sponsors. It was only with the start of a new century that some Islamic forces began to pursue an asymmetric approach, one that promoters of a definable Islamic way of war think supports their position.

Proponents

Those who believe there is an Islamic way of war can be fairly placed into one of two categories. The first argues that Islam is by its very nature a religion of war. The second focuses on Islamist radicalism, arguing that the methods used present an approach to warfare that is sufficiently definable to be labeled Islamic. The views of each school merit scrutiny.

the militaries of the Middle East developed into near-mirror images of their Western sponsors

One well-known representative of the first group is Robert Spencer, author of the mass media publication *The Politically Incorrect Guide to Islam (and the Crusades)*.¹⁰⁷ His book contains chapter headings such as "The Qur'an: Book of War"¹⁰⁸ and "Islam: Religion of War."¹⁰⁹ Although Spencer has his detractors,¹¹⁰ his *Guide to Islam* spent 15 weeks on the *New York Times* bestseller list¹¹¹ and is one of the best-selling books on Islam ever to appear in the United States.¹¹²

In making his argument, Spencer focuses on Koranic verses that promote war, and then argues that many Muslims today feel inherently bound to follow them.¹¹³ He dismisses the obvious comparison of similarly "violent" verses from the Old Testament by saying the latter were only directed at distinct, long disappeared tribes.¹¹⁴ He also dismisses established scholars of Islam such as Bernard Lewis, whom he describes as "disingenuous about Islamic radicalism,"¹¹⁵ and Karen Armstrong, whom he considers a "Western apologist for Islam" and "[o]ne of the people most responsible" for "the fog of misinformation that surrounds Islam and the Crusades today."¹¹⁶ Although he concedes there are moderate Muslims who want

nothing to do with terrorism, he argues there is no such thing as moderate Islam and that, at its core, "Islam is unique among the religions of the world in having developed a doctrine, theology, and legal system that mandates warfare against unbelievers."¹¹⁷ He also insists that under Islam's tenets, there can be no peace until Islam controls the world, and that once a place falls under Islamic control, "peaceful coexistence as equals in a pluralistic society isn't one of the choices."¹¹⁸ Finally, he argues the early Islamic conquests only succeeded because Muslim soldiers received a promise of forgiven sins and insists the notion that local populations welcomed the Muslims is "a PC myth."¹¹⁹

The problem with Spencer's Islam-is-war theory is that it obfuscates inconvenient facts. For example, his arguments rely on militaristic verses from the Koran without mentioning that religious scholars have innumerable disagreements about what they really mean.¹²⁰ Spencer similarly fails to address evidence showing the great Islamic conquests succeeded primarily due to enemy exhaustion, oppressive Byzantine rule, and the decision to leave existing bureaucracies in place.¹²¹ Likewise, he overlooks Islam's grand expansion into Indonesia, which occurred peacefully.¹²² Nor does he examine the Andalusian communities of Cordoba and Toledo, where Muslims and Jews, coexisting under Islamic leadership, produced the likes of Averroes and Maimonides.¹²³ Perhaps above all, his theory disregards centuries of warfare similarly waged by Christians and others in the name of their religions.¹²⁴ Nowhere, for example, does Spencer contrast the spread of Islam with the brutal spread of Christianity in, for instance, Central and South America.¹²⁵

A second argument suggesting there is an Islamic way of war depends less on sweeping if flawed generalizations and focuses on events of the past several decades. Consider Andrew Bacevich's article "The Islamic Way of War."¹²⁶ He argues that Muslims realize they cannot defeat the West with conventional means and instead have learned to fight asymmetrically. He describes this Islamic way of war as:

a panoply of techniques employed to undercut the apparent advantages of high-tech conventional forces. The methods employed do include terrorism—violence targeting civilians for purposes of intimidation—but they also incorporate propaganda, subversion, popular

agitation, economic warfare, and hit-and-run attacks on regular forces, either to induce an overreaction or to wear them down. The common theme of those techniques, none of which are new, is this: avoid the enemy's strengths; exploit enemy vulnerabilities.¹²⁷

In truth, what Bacevich brands as an Islamic way of war is simply an application of Sun Tzu's indirect approach to warfare,¹²⁸ and the methods he describes are indistinguishable from those used by resistance movements around the world.¹²⁹ Additionally, in his critique of Bacevich's definition, David Kilcullen sagely notes that this supposedly Islamic approach to warfare is wholly consistent with the "unrestricted warfare" theory promulgated by Chinese colonels Qiao Liang and

although terrorism is the method chosen by al Qaeda, there is nothing inherently Islamic about terrorism itself

Wang Xiangsui a decade ago.¹³⁰ Simply put, implying that these methods are somehow Islamic is erroneous. Perhaps Bacevich is simply trying to point out that some elements in the Muslim world are resorting to asymmetric warfare, but it is hard to imagine labeling, for example, Jewish resistance movements that fought asymmetrically in World War II as waging a "Jewish way of war."¹³¹

Although terrorism is the method chosen by al Qaeda to confront its enemies,¹³² there is *nothing inherently Islamic* about terrorism itself. For example, high-profile terrorist attacks began in the Middle East in the late 1960s, often in the form of hijackings.¹³³ Although he was an Arab, the pioneer of this method was George Habash, the *Christian* founder of the Popular Front for the Liberation of Palestine.¹³⁴ Islamists who attack civilians are hardly the first groups to employ that approach. For example, the Irish Republican Army killed over 600 civilians through terror tactics;¹³⁵ the Irgun, led by future Prime Minister Menachem Began, deliberately targeted British civilians in the years leading up to Israeli independence;¹³⁶ and today, radical Israeli terrorist elements aim to prevent peace between Israel and the Palestinians.¹³⁷ Although al Qaeda—a viciously anti-Shi'ite organization¹³⁸—employs suicide bombers, Robin Wright notes that Shi'ites, not Sunni Islamists, began the modern practice in the early 1980s.¹³⁹ Wright estimates that 3,400 Americans died

in suicide attacks between 1983 and 2008.¹⁴⁰ However, as an indirect approach to warfare, suicide attacks are hardly new. Japanese Kamikaze pilots killed 4,900 Americans and wounded 4,800 between the fall of 1944 and the following August.¹⁴¹ Many other organizations, including the Marxist Kurdish Workers Party and the Black Tigers of Sri Lanka (just to cite two), frequently used suicide bombers as well.¹⁴² Terrorism is regrettably ubiquitous. It is not, however, an Islamic way of war.

Something eerily familiar permeates the debate over whether there is an Islamic way of war, and it can be found in historian John Dower's *War without Mercy*.¹⁴³ Dower described how Hearst newspapers portrayed the war against Japan as "cultural and religious," while warning that a victorious Japan would cause a "perpetual war between Oriental ideals and Occidental."¹⁴⁴ He further noted how popular writers of the day described the war with Japan differently from the one in Europe because the former was seen as "a holy war, a racial war of greater significance than any the world has heretofore seen."¹⁴⁵ For Dower, there was an underlying "Pan-Asian unity myth" that it took the war to destroy.¹⁴⁶ Ultimately, he showed how racism and the creation of the less-human "other" helped turn the war into one of unspeakable horror.¹⁴⁷

The specter of Said's *Orientalism* also comes to the fore with the question of whether there is an Islamic way of war. Said indicted Western scholarship of Islam by demonstrating how it simultaneously was shaped by and promulgated imperialism.¹⁴⁸ He described "Orientalism" as akin to anti-Semitism, but this time directed at people and cultures in Islamic lands.¹⁴⁹ Although assailed by some,¹⁵⁰ *Orientalism* germanely and poignantly described how creation of the "lesser other" negatively shaped outlooks and perceptions of Middle Easterners for generations.¹⁵¹

Thus, defining an Islamic way of war would yield tangible risks. The first involves the definition's potential to dehumanize. Arguing that Muslims have an institutionalized approach to war that is unique, definable, and therefore recognizable as a stand-alone concept helps establish that Muslims are different from non-Muslims in the West; they risk becoming the other. In an ideological sense, what Robert Spencer does in *Guide to Islam* is paint Muslims as an apocalyptic enemy, implying war or submission are the only two options at hand. Unfortunately,

Western thought has displayed a disturbing willingness to brand Islam as "irrational" and declare the Muslim mind "closed,"¹⁵² thereby further propagating Muslims as the other.

Perhaps the second risk is subtler, but it is also dangerous. Defining an Islamic way of war generates a paradigm, a set of blinders. If U.S. strategists believe there is an institutionalized Islamic approach to war that is unique, definable, and recognizable, their assumptions will be made accordingly. By adopting the arguments of Spencer and others, Americans risk falling prey to an ideological "pathology" capable of "blinding us irreversibly."¹⁵³ In short, Americans must steadfastly avoid placing themselves in a nonexistent box.

Unmistakably, an Islamic way of war does not exist. Studying key periods of Islamic military history, considering Islam's most important philosophers, placing current events in their proper global context, and questioning opposing views mandate this conclusion. Whenever the theory of an Islamic way of war surfaces, it must be rejected unequivocally. Otherwise, the minds that end up being closed may well be our own. **JFQ**

NOTES

¹ Edward W. Said, *Orientalism*, 1st ed. (New York: Vintage Books, 1979), 304.

² Andrew J. Bacevich, "The Islamic Way of War: Muslims Have Stopped Fighting on Western Terms—and Have Started Winning," *The American Conservative*, September 11, 2006, available at <www.amconmag.com/article/2006/sep/11/00007/>.

³ Mehar Omar Kahn, "Is There an Islamic Way of War?" *Small Wars Journal*, March 8, 2010, available at <<http://smallwarsjournal.com/blog/journal/docs-temp/381-khan.pdf>>.

⁴ Peter Malcolm Holt et al., *The Cambridge History of Islam, 2B, Islamic Society and Civilization* (Cambridge: Cambridge University Press, 1977), 847.

⁵ Said, 304.

⁶ Russell Frank Weigley, *The American Way of War: A History of United States Military Strategy and Policy* (New York: Macmillan, 1973), xxii.

⁷ Michael Geyer, "German Strategy in the Age of Machine Warfare, 1914–1945," in *Makers of Modern Strategy: From Machiavelli to the Nuclear Age*, ed. Peter Paret, Gordon Alexander Craig, and Felix Gilbert (Princeton: Princeton University Press, 1986), 566.

⁸ John L. Esposito, *Islam: The Straight Path*, 3rd ed. (New York: Oxford University Press, 1998), 12.

⁹ *Ibid.*, 13.

¹⁰ Bernard Lewis, *The Middle East: A Brief History of the Last 2,000 Years* (New York: Scribner, 1995), 62.

- ¹¹ Karen Armstrong, *Islam: A Short History* (New York: Modern Library, 2000), 21.
- ¹² See Jeremy Black, *The Seventy Great Battles in History* (London: Thames & Hudson, 2005); Elmer C. May, Gerald P. Stadler, and John F. Votaw, *The West Point Military History Series: Ancient and Medieval Warfare* (Wayne, NJ: Avery Publishing Group, 1984); and Michael Lee Lanning, *The Military 100: A Ranking of the Most Influential Military Leaders of All Time* (Secaucus, NJ: Carol Publishing Group, 1996).
- ¹³ One of the most comprehensive single volume military history compendiums, R. Ernest Dupuy and Trevor N. Dupuy, *The Encyclopedia of Military History from 3500 B.C. to the Present*, 2^d rev. ed. (New York: Harper & Row, 1986), includes battle summaries from the entirety of recorded human history, those in the Near East included. In that work, however, much of the analysis is reserved for events traditionally important to Western historians.
- ¹⁴ Perhaps one reason for this dearth of coverage represents a Western (possibly "Orientalist") perspective on the value of studying Islamic history.
- ¹⁵ Hugh Kennedy, *The Great Arab Conquests: How the Spread of Islam Changed the World We Live In* (Philadelphia: Da Capo, 2007), 12–33.
- ¹⁶ *Ibid.*, 371.
- ¹⁷ *Ibid.*, 67–70.
- ¹⁸ *Ibid.*, 368.
- ¹⁹ *Ibid.*, 69.
- ²⁰ *Ibid.*, 68.
- ²¹ *Ibid.*
- ²² Thomas R. Martin, *Ancient Greece: From Prehistoric to Hellenistic Times* (New Haven: Yale University Press, 1996), 174.
- ²³ Malise Ruthven and Azim Nanji, *Historical Atlas of Islam* (Cambridge: Harvard University Press, 2004), 24.
- ²⁴ Armstrong, 35.
- ²⁵ *Ibid.*
- ²⁶ Kennedy, 372.
- ²⁷ *Ibid.*, 97.
- ²⁸ *Ibid.*, 373.
- ²⁹ Lewis, *The Middle East*, 433.
- ³⁰ *Ibid.*, 57.
- ³¹ Esposito, *Islam: The Straight Path*, 38.
- ³² Lewis, *The Middle East*, 210–212; Esposito, *Islam: The Straight Path*, 38.
- ³³ Esposito, *Islam: The Straight Path*, 38.
- ³⁴ Kennedy, 369.
- ³⁵ *Ibid.*, 68.
- ³⁶ Esposito, *Islam: The Straight Path*, 38.
- ³⁷ Kennedy, 372.
- ³⁸ *Ibid.*, 373.
- ³⁹ Holt et al., 825.
- ⁴⁰ David Nicolle, *Yarmuk, 636 AD: The Muslim Conquest of Syria* (London: Osprey, 1994).
- ⁴¹ David Nicolle and Angus McBride, *Armies of the Muslim Conquest* (London: Osprey, 1993), 10.
- ⁴² *Ibid.*
- ⁴³ Esposito, *Islam: The Straight Path*, 38.
- ⁴⁴ Geoffrey Hindley, *A Brief History of the Crusades* (London: Robinson, 2004), 256.
- ⁴⁵ Christopher Catherwood, *A Brief History of the Middle East: From Abraham to Arafat* (New York: Carroll & Graf Publishers, 2006), 260.
- ⁴⁶ Reza Aslan, *How to Win a Cosmic War: God, Globalization, and the End of the War on Terror* (New York: Random House, 2009), 5–6, 11.
- ⁴⁷ Catherwood, 106.
- ⁴⁸ Lawrence Wright, *The Looming Tower: Al-Qaeda and the Road to 9/11* (New York: Knopf, 2006), 171.
- ⁴⁹ Daniel Benjamin and Steven Simon, *The Age of Sacred Terror: Radical Islam's War Against America* (New York: Random House, 2003), 167.
- ⁵⁰ Bruce B. Lawrence, *Messages to the World: The Statements of Osama Bin Laden* (London, New York: Verso, 2005), 213–214.
- ⁵¹ Chaim Herzog and Mordechai Gichon, *Battles of the Bible* (New York: Random House, 1978), 62.
- ⁵² Dupuy and Dupuy, 533.
- ⁵³ Bertold Spuler, *The Mongol Period: History of the Muslim World*, trans. F.R.C. Bagley (Princeton: Markus Wiener, 1994), 20.
- ⁵⁴ Muhammad Mojlum Khan, *Muslim 100: The Lives, Thoughts and Achievements of the Most Influential Muslims in History* (Markfield, Leicestershire, UK: Kube, 2008), 65.
- ⁵⁵ See, for example, George Melloan, "World War II's Do-good Offspring are Flagging," *The Wall Street Journal*, September 20, 2005, A17.
- ⁵⁶ Mir Tamim Ansary, *Destiny Disrupted: A History of the World through Islamic Eyes* (New York: PublicAffairs, 2009), 143–145.
- ⁵⁷ *Ibid.*
- ⁵⁸ Aslan, *How to Win a Cosmic War*, 106.
- ⁵⁹ *Ibid.*
- ⁶⁰ Michael Axworthy, *A History of Iran: Empire of the Mind* (New York: Basic Books, 2008), 341.
- ⁶¹ Robert R. Reilly, *The Closing of the Muslim Mind: How Intellectual Suicide Created the Modern Islamist Crisis* (Wilmington, DE: ISI Books, 2010), 35–39, 233–234.
- ⁶² Michael Hamilton Morgan, *Lost History: The Enduring Legacy of Muslim Scientists, Thinkers, and Artists* (Washington, DC: National Geographic, 2007), 56–57, 241.
- ⁶³ Reilly, 119.
- ⁶⁴ Lewis, *The Middle East*, 240.
- ⁶⁵ Reilly, 93.
- ⁶⁶ Ansary, 115.
- ⁶⁷ Reilly, 119.
- ⁶⁸ Antony Black, *The History of Islamic Political Thought: From the Prophet to the Present* (New York: Routledge, 2001), 102.
- ⁶⁹ *Ibid.*, 104.
- ⁷⁰ *Ibid.*, 102.
- ⁷¹ Armstrong, 172.
- ⁷² Black, 102.
- ⁷³ Sohail H. Hashmi, "Saving and Taking Life in War, Three Modern Muslim Views," in *Islamic Ethics of Life: Abortion, War, and Euthanasia*, ed. Jonathan E. Brockopp (Columbia: University of South Carolina Press, 2003), 147–148.
- ⁷⁴ Andrew G. Bostom, "Sufi Jihad," *American Thinker*, May 15, 2005, available at <www.americanthinker.com/printpage/?url=http://www.americanthinker.com/2005/05/sufi_jihad.html>.
- ⁷⁵ William F. McCants et al., "Militant Ideology Atlas Executive Report," Combating Terrorism Center, available at <www.ctc.usma.edu/atlas/Atlas-ExecutiveReport.pdf>.
- ⁷⁶ Aslan, *How to Win a Cosmic War*, 110.
- ⁷⁷ *Ibid.*
- ⁷⁸ *Ibid.*
- ⁷⁹ According to Ansary, "Ibn Taymiyya reputedly wrote about four thousand pamphlets and five hundred books. With these, he planted a seed. The seed didn't flourish at once, but it never died out either. It just lay there, under the surface of Islamic culture, ready to bud if circumstances should ever favor it. Four and half centuries later, circumstances did" (164).
- ⁸⁰ Benjamin and Simon, 44.
- ⁸¹ Ansary, 164.
- ⁸² Catherwood, 114.
- ⁸³ *Ibid.*
- ⁸⁴ Ansary, 162.
- ⁸⁵ Benjamin and Simon, 48.
- ⁸⁶ *Ibid.*, 50.
- ⁸⁷ John L. Esposito, *Unholy War: Terror in the Name of Islam* (New York: Oxford University Press, 2002), 62.
- ⁸⁸ Robert Spencer, *The Politically Incorrect Guide to Islam (and the Crusades)* (Washington, DC: Regnery Publishing, 2005), 39.
- ⁸⁹ Aslan, *How to Win a Cosmic War*, 110.
- ⁹⁰ Benjamin and Simon, 50.
- ⁹¹ Bernard O'Kane, *Treasures of Islam: Artistic Glories of the Muslim World* (London: Duncan Baird, 2007), 138–147, 163–169, 200–203.
- ⁹² Robert Day McAmis, *Malay Muslims: The History and Challenge of Resurgent Islam in Southeast Asia* (Grand Rapids, MI: W.B. Eerdmans Publishing Company, 2002), 24.
- ⁹³ *Ibid.*, 24–25.
- ⁹⁴ T.P. Schwartz-Barcott, *War, Terror & Peace in the Qur'an and in Islam: Insights for Military & Government Leaders* (Carlisle, PA: U.S. Army War College Foundation Press, 2004), 370–372.
- ⁹⁵ *Ibid.*, 372–374.
- ⁹⁶ Albert Hourani, *A History of the Arab Peoples* (Cambridge: Belknap Press of Harvard University Press, 1991), 265.
- ⁹⁷ David Nicolle, *Armies of the Ottoman Turks, 1300–1774* (London: Osprey Publishing, 1983).
- ⁹⁸ Dupuy and Dupuy, 403.
- ⁹⁹ Lewis, *The Middle East*, 275.
- ¹⁰⁰ Caroline Finkel, *Osman's Dream: The Story of the Ottoman Empire, 1300–1923* (New York: Basic Books, 2006), 390–396.
- ¹⁰¹ Axworthy, 195.



for the
Africa Center for Strategic Studies

NEW
from **NDU Press**

ACSS Research Paper No. 2

Africa's Evolving Infosystems: A Pathway to Security and Stability

Political instability and violence in Africa are often the products of rumor and misinformation.

Against this backdrop, Steven Livingston shows that the emergence of new information and communication technologies—together with new democratic institutions—is noteworthy. In the past 5 years, the annual growth rate for mobile telephones in Africa has been 65 percent—more than twice the global average. Linked by these new technologies and geographical information systems, civil society networks in Africa now are able to monitor security, provide health care information, create banking services, and provide marketing information to farmers. Mobile communications has helped to create new institutions that promote transparency, accountability, and security. This research paper traces the remarkable development of these infosystems and their effects in Africa. The paper recommends supporting African innovation centers as well as basic research on the political, economic, and security implications of local networks created by mobile telephony and related technologies.



Forging Partnerships for Africa's Future

The Africa Center offers a variety of resources that keep readers abreast of the Africa-related news and research published on this site.

<http://africacenter.org/>

To subscribe to Africa Center's Daily Media Review and/or Africa Security Briefs, go to <http://africacenter.org/subscribe/>, enter email address, check the box next to the name of the newsletter(s) desired, and click the "Submit" button.

Visit the NDU Press Web site
for more information on publications
at ndupress.ndu.edu

FEATURES | An Islamic Way of War?

¹⁰² David Fromkin, *A Peace to End All Peace: Creating the Modern Middle East, 1914–1922* (New York: Holt, 1989), 109, 218–219.

¹⁰³ Holt et al., 847.

¹⁰⁴ Kenneth M. Pollack, *Arabs at War: Military Effectiveness, 1948–1991* (Lincoln: University of Nebraska Press, 2002).

¹⁰⁵ Ibid.

¹⁰⁶ Ibid., 569.

¹⁰⁷ Spencer.

¹⁰⁸ Ibid., 19.

¹⁰⁹ Ibid., 33.

¹¹⁰ Karen Armstrong, "Balancing the Prophet: Four Books about Muhammad Shed as Much Light on the Authors—and Their Convictions—as They Do on the Man Himself," *Financial Times*, April 28, 2007.

¹¹¹ This information is from Spencer's publisher and can be found at <www.regnery.com/bestsellers.html>.

¹¹² Amazon lists *The Politically Incorrect Guide to Islam* as its 14th best selling book on Islam.

¹¹³ Spencer, 45.

¹¹⁴ Ibid., 29.

¹¹⁵ Ibid., 221.

¹¹⁶ Ibid., xv.

¹¹⁷ Ibid., 43.

¹¹⁸ Ibid., 37.

¹¹⁹ Ibid., 53–54.

¹²⁰ Reza Aslan, *No God but God: The Origins, Evolution, and Future of Islam* (New York: Random House, 2005), 84–85.

¹²¹ Kennedy, 366–375.

¹²² McAmis, 24.

¹²³ David L. Lewis, *God's Crucible: Islam and the Making of Europe, 570 to 1215* (New York: Norton, 2008), 367–379.

¹²⁴ Spencer fervently rejects comparisons between the spread of Islam and the expansion of Christianity as misguided, illegitimate attempts at "moral equivalency." Spencer, 116.

¹²⁵ Paul Johnson, *A History of Christianity* (London: Weidenfeld & Nicolson, 1976), 402. Johnson describes the Christian conversion process as "an extraordinary mixture of force, cruelty, stupidity and greed, redeemed by occasional flashes of imagination and charity."

¹²⁶ Bacevich.

¹²⁷ Ibid.

¹²⁸ Lawrence P. Phelps, *East Meets West: A Combined Approach to Studying War and Strategy in the 21st Century* (Carlisle Barracks, PA: U.S. Army War College, 2006).

¹²⁹ Ibid.

¹³⁰ David Kilcullen, *The Accidental Guerrilla: Fighting Small Wars in the Midst of a Big One* (Oxford: Oxford University Press, 2009), 25.

¹³¹ Michael I. Karpin, *The Bomb in the Basement: How Israel Went Nuclear and What That Means for the World* (New York: Simon & Schuster, 2006), 9.

¹³² Terry McDermott, *Perfect Soldiers: The Hijackers: Who They Were, Why They Did It* (New York: HarperCollins, 2005), 269.

¹³³ "Habash Was No Role Model," *Jerusalem Post*, March 2, 2008.

¹³⁴ "For the Record," *The New York Times*, July 17, 2007.

¹³⁵ Malcolm Sutton, *Bear in Mind These Dead: An Index of Deaths from the Conflict in Ireland, 1969–1993* (Belfast: Beyond the Pale Publications, 1994). Statistics available at <www.cain.ulst.ac.uk/sutton/book/index.html#append%20CAIN:%20Sutton%20Index%20of%20Deaths%20-%20extracts%20from%20Sutton's%20book%20>. The report estimates the IRA killed 650 civilians.

¹³⁶ Charles D. Smith, *Palestine and the Arab-Israeli Conflict: A History with Documents* (Boston: Bedford/St. Martin's, 2007), 178–179.

¹³⁷ Ilana Kass and Bard E. O'Neill, *The Deadly Embrace: The Impact of Israeli and Palestinian Rejectionism on the Peace Process* (Fairfax, VA: University Press of America, 1997), 101–106.

¹³⁸ Seyyed Vali Reza Nasr, *The Shia Revival: How Conflicts within Islam Will Shape the Future* (New York: Norton, 2006), 243–247.

¹³⁹ Robin B. Wright, *Dreams and Shadows: The Future of the Middle East* (New York: Penguin Press, 2008), 170.

¹⁴⁰ Robin Wright, "Since 2001, a Dramatic Increase in Suicide Bombings," *The Washington Post*, April 18, 2008.

¹⁴¹ Richard P. Hallion, "Precision Weapons, Power Projection, and the Revolution in Military Affairs," USAF Air Armament Summit, Air Armament Center, Eglin Air Force Base, FL, May 29, 1999, available at <www.airforcehistory.hq.af.mil/EARS/hallionpapers/precisionweaponspower.htm>.

¹⁴² Leonard Weinberg, Ami Pedahzur, and Daphna Canetti-Nisim, "The Social and Religious Characteristics of Suicide Bombers and their Victims," *Terrorism and Political Violence* 15, no. 3 (October 2003), 140, available at <www.informaworld.com/10.1080/09546550312331293167>.

¹⁴³ John W. Dower, *War without Mercy: Race and Power in the Pacific War* (New York: Pantheon Books, 1986).

¹⁴⁴ Ibid., 7.

¹⁴⁵ Ibid.

¹⁴⁶ Ibid.

¹⁴⁷ Ibid., 77–93.

¹⁴⁸ Said, 12–15.

¹⁴⁹ Ibid., 27–28.

¹⁵⁰ Robert Irwin, *Dangerous Knowledge: Orientalism and its Discontents* (Woodstock, NY: Overlook Press, 2006).

¹⁵¹ Said, 12.

¹⁵² Reilly, 127.

¹⁵³ Terry L. Deibel, *Foreign Affairs Strategy: Logic for American Statecraft* (New York: Cambridge University Press, 2007), 118.


Why Unmanned

By PAUL SCHARRE

It is almost a cliché these days to speak of an unmanned revolution in war, and yet with literally thousands of unmanned vehicles on the ground and in the air supporting U.S. troops overseas, it is clear that something special is happening. Ten years ago, unmanned aerial vehicles (UAVs) such as the Predator were a niche capability that existed only in small numbers. Today, U.S. forces overseas cannot get enough of them. Wartime necessity has driven the deployment of unmanned ground vehicles (UGVs) to defuse bombs and UAVs to provide persistent overhead surveillance to track insurgents and protect troops. The utility—and limitations—of unmanned versus manned systems for future weapons, however, such as combat UAVs or robotic ground vehicles, is a continuing source of debate.

Pitting manned and unmanned vehicles (UxVs) directly against one another for the same tasks misses the point of building such vehicles. The utility in UxVs is not that they are cheaper or necessarily better than equivalent manned systems (compare, for instance, the Global Hawk and U-2 aircraft), but that *they can be designed to do things that manned systems cannot do*. Unmanned systems can be designed with performance characteristics and risk profiles that, for some missions, simply would be not feasible or acceptable for manned vehicles. Innovative unmanned systems can be designed to operate on land, at sea, and in the air in larger quantities, taking greater risks, and with range, endurance, speed, and maneuverability not possible with manned systems.

The result is that unmanned systems offer the potential for a new paradigm for U.S. warfighting. Since the end of World War II, the United States has generally fought from a position of numerical inferiority and relied on superior quality weapons. Unmanned systems offer the potential to untether U.S. forces from the relatively small personnel base of a professional military. Instead, the United States could unleash large quantities of attritable unmanned weapons on the battlefield, leveraging both quality *and* quantity. These weapons could provide a range of capabilities, including reconnaissance, decoy, jamming, and strike. As the computer processing power that enables autonomy increases exponentially, even more capable systems will be possible in the future.



United Kingdom's Taranis prototype will test possibility of developing unmanned combat vehicle with long-range precision strike capabilities

BAE Systems

Paul Scharre is a former Infantryman in the 75th Ranger Regiment who has served in Iraq and Afghanistan. He currently works in the Office of the Secretary of Defense.

Performance

Removing the person from the cockpit, driver's seat, or tiller yields two immediate benefits: commanders can take more risk with the asset; and in some situations, performance advantages are achieved. Performance advantages can include less weight, greater payload, smaller size, longer endurance, more maneuverability, and greater speed, although these advantages become less significant for larger vehicles.

The Predator UAV is a shining example of exploiting the performance advantages of removing a person from the cockpit, thus enabling an aircraft that can loiter for 24 hours providing continuous overhead surveillance. A manned aircraft with similar endurance would be hindered by both pilot weight and pilot fatigue. Smaller UAVs such as the Scan Eagle and Raven go even further by enabling concepts of operation that would literally be impossible with manned aircraft, such as an infantry squad carrying a hand-launched Raven UAV on foot patrol. To achieve the same effect by stationing numerous manned aircraft continuously over each and every infantry patrol would be prohibitively expensive and unfeasible.

Even greater performance advantages in the areas of range and endurance are anticipated with future UxVs. The BAE Taranis, Northrop Grumman X-47B, and Boeing X-45 combat UAVs are expected to have greater endurance and longer ranges than equivalent manned aircraft. Concept surveillance aircraft and airships aim for endurances of months and years, a scale clearly impossible with manned aircraft. Similarly, glider unmanned underwater vehicles can stay at sea for months or years at a time, monitoring critical areas or shadowing enemy submarines.¹ Performance advantages diminish and the weight and size of a person on board become negligible as a vehicle gets larger.² Significant gains might not be made by, for example, removing a person from a large bomber or a warship. For a variety of applications, however, UxVs can fill roles manned systems cannot.

Risk

UGVs like the iRobot Packbot are used for hazardous missions, such as defusing bombs, where commanders would prefer not to put soldiers at risk. While war necessarily involves risk, the U.S. military does not (nor should it) treat its Servicemembers as expend-

able assets. UxVs, provided they are cheap enough, could be expendable, opening up new concepts of operation.

UxVs can enable radically new concepts for accomplishing missions by decoupling force protection from combat performance. The proliferation of improvised explosive devices (IEDs) drives Soldiers and Marines into heavily armored vehicles such as the Mine Resistant Ambush Protected (MRAP) vehicles, which are correspondingly cumbersome. Building a next-generation ground combat vehicle that is fast, maneuverable, light enough to traverse unimproved roads and bridges, well armed, and survivable against IEDs is a nearly impossible task. Unmanned systems offer the potential to disaggregate the fighting and surviving roles, however. Lightly armored reconnaissance UxVs could scout ahead to discover enemy positions and relay

tage. UxVs can be used to flood an enemy's defenses. Combined with the performance advantages of greater speed, maneuverability, range, and endurance, UxVs can enable power projection and persistence not possible with manned assets. (This is especially the case if networked UxVs lead to significant coordination and synchronization advantages, such as intelligent swarming.⁴)

Because they are able to take more risks in survivability, UxVs could be built for special purposes. Mission tasks could be disaggregated. By optimizing for a single task, cheaper UxVs could be fielded in larger quantities. The result would be a family of special purpose vehicles that together accomplish the mission previously done by a single multimission platform. The resulting increased quantity and diversity of U.S. assets complicates an adversary's decisionmaking.

concept surveillance aircraft and airships aim for endurances of months and years, a scale clearly impossible with manned aircraft

their data to troops safely ensconced in survivable platforms in the rear. Then, attributable UxVs (such as smart missiles) could be sent forward to strike enemy positions.

Next-generation unmanned tanks could be designed to emphasize speed and maneuverability over survivability. Air-mobile swarms of UxVs could leapfrog behind enemy lines and provide reconnaissance for precision indirect fires. At sea, unmanned surface vehicles (USVs) could be used to help U.S. Navy warships defend against swarming small boat attacks, providing a buffer between threatening surface vessels and U.S. ships. USVs and ship-launched UAVs could extend the range of a ship's sensors, moving beyond the crow's nest to an over-the-horizon concept for situational awareness.³ Using UxVs to remove the person from the leading edge of the battlefield could not only reduce risk, but also enable faster, more maneuverable forces.

Numbers Matter

Broadly speaking, the American way of war since the end of World War II has been to focus on superior technology to counter the numerical superiority of adversaries. The ability to send unmanned vehicles to the front means that the U.S. military's smaller all-volunteer force may no longer be forced to fight from a position of numerical disadvan-

For instance, the miniature air launch decoy (MALD) offers the ability to confuse an enemy's integrated air defenses by flooding the skies with relatively cheap unmanned decoys. Clearly, this concept would not be possible with a manned asset. While a decoy is not even comparable to an actual aircraft in terms of capability, the MALD is relatively inexpensive compared to the asset it is protecting, allowing the proliferation of a large number of decoys that multiplies the effectiveness of existing aircraft. Every MALD in the skies drawing fire from enemy defenses enhances the survivability of U.S. strike aircraft. Similarly, other MALD-like attributable unmanned vehicles could perform reconnaissance and surveillance, battle damage assessment, electronic attack (like the MALD-Jammer), or close-in strike such as traditional precision-guided munitions. As autonomous capabilities grow, the difference between attributable unmanned vehicles and loitering munitions will become increasingly hazy. The Tactical Tomahawk and Harpy UAV, for example, blur this distinction.

Unmanned vehicles could also act as force multipliers for offensive systems. Unmanned floating weapons pods, for example, which would be little more than remote-controlled barges loaded with missiles, could be used to deepen the magazine

of the destroyers that would control them. The result would be a dramatic multiplying of the offensive capability of a destroyer at relatively low cost. Moreover, because weapons pods distribute the fighting capability of a single ship across a wider area, an enemy's targeting problem is significantly complicated compared to a hypothetical large, densely packed warship with the same offensive capability. With a distributed network, any single pod or group of weapons pods is attritable. Combat power may decline as pods are attrited, but provided that the command and control node (and sensors) at the center of the network survives, the U.S. battle network could continue to fight.

The performance advantages of UxVs (speed, maneuverability, and endurance) could lead to offensive advantages, while the ability to take risks in a single asset could, paradoxically, enable a more robust system of weapons and sensors. A distributed network of UxVs operating as a *reconnaissance-strike swarm* could project more survivable and more capable power further, faster, and with greater persistence than small numbers of more costly multimission manned platforms. Swarms that instantly communicated and autonomously coordinated their actions without human input would be able to achieve even greater speed of decisionmaking and synchronization of fire and maneuver than manned or remotely piloted systems.

These advantages may be essential in the emerging antiaccess and precision strike regime. Other nations are investing in precision strike capabilities designed to target traditional U.S. means of projecting power—aircraft carriers and land bases—necessitating both improvements in resiliency and defense as well as new concepts for power projection. From global positioning system-guided mortars and precision antitank rockets, to advanced antiship cruise missiles and DF-21 antiship ballistic missiles, the increasing precision of munitions is altering the character of warfare. Leveraging attritable UxVs to reconnoiter deep into enemy territory and then relay data back to standoff strike assets may be a cost-effective strategy for competing in an era where large quantities of precision munitions are proliferated widely to state and nonstate actors alike.

Cost, Quantity, and Expendability

In order for attritable UxVs to be truly expendable, they must be relatively low cost.



Soldier launches RQ-11 Raven UAV near Taqqadum, Iraq

U.S. Army (Michael J. MacLeod)

The cost threshold for a given UxV to be considered “expendable” is relative to the mission, the asset it is protecting, and the marginal cost to the enemy of producing more of their own weapons to counter the UxV.⁵ A \$500,000 unmanned lead truck in a convoy is expendable relative to the cost of the \$1 million MRAP vehicle that it saves. In other situations, such as in missile defense, the cost-exchange ratio between U.S. and enemy weapons may be paramount.

To be affordable enough to be expendable, UxVs must be protected from the Department of Defense (DOD) death spiral of rising costs and production cuts that can lead to small numbers of extremely expensive “baroque” weapons.⁶ While performance advantages could translate into increased cost-effectiveness, there is no reason to believe that the simple act of removing a person from a vehicle in and of itself saves significant costs. Many weapons programs, manned and unmanned alike, have fallen victim to the trap of rising costs and unaffordability. Unfortunately, one of the drivers of cost increases in many acquisition programs is often the same high-end information technology that UxVs seek to leverage. High-risk information technology projects can turn into nightmarish monstrosities, with cost overruns, schedule slippage, and millions of lines of snarled code.⁷ Autonomous systems need not be expensive, however. The price of raw computing power is falling at an exponential rate. As a result, greeting cards that play musical jingles now carry throwaway microprocessors that

would have been considered supercomputers decades ago. Computing power *can* be purchased at low costs.

Affordable and effective UxVs can be built by focusing on specialization, “good-enough” capabilities, and modular design. The Predator is a perfect example of the cost efficiency possible when a UxV aims to fill a specialized niche. While the Predator is nowhere near as capable as a multirole F-16 fighter for a whole host of missions, it is preferable for long-duration surveillance in permissive environments. It is also cheaper for 24/7 surveillance than an equivalent manned aircraft that might perform long-loitering airborne surveillance, such as the Super Tucano or MC-12 airplane. With endurances of 6 and 8 hours, respectively, both manned options would require more total aircraft on hand to support one airborne “orbit” on station 24/7 than the Predator, with its 24-hour endurance.

Modularity can enable incremental upgrades, employing affordable autonomy that is good enough given existing technology, rather than breaking the bank stretching for experimental technology. Incremental upgrades that leverage existing code can reduce technology risk and lower costs. For example, while the robust autonomy needed to operate fully autonomous ground combat vehicles on unimproved roads, around civilians, and against adaptable enemies is not quite mature enough for 100-percent-reliable, error-free operation, relatively modest semiautonomous technology is currently available.⁸ “Robotic appliqué kits” can, for a cost of tens of thousands of dollars rather

than millions, convert existing Humvees and trucks to semi-autonomous or tele-operated UGVs. These unmanned vehicles could save lives by becoming “sacrificial vehicles” that lead convoys in dangerous areas, while the troops who control them follow safely behind. As computer technology improves, these vehicles can continue to be upgraded incrementally for more autonomous operation.

UxVs should be built with modularity as a fundamental design concept, so that they can harness the potential of accelerating computer technology while remaining affordable. With a modular design, a range of stealthy and nonstealthy vehicles and munitions in various sizes could be upgraded and modified as needed by swapping out payloads and sensors within the same vehicle frame. Such an approach would save costs on developing vehicle frames and propulsion, while leaving room to upgrade the “brains” of the machine on a regular basis, so U.S. systems could remain at the leading edge of computer development.

Computer processing power is doubling roughly every 18 months, meaning that a military system, just like a personal computer or cell phone, risks obsolescence within a short time. Waiting decades for modernization initiatives to bear fruit, which is the traditional timeline for new military hardware, is not a winning strategy for competing in the precision-weapons arms race fueled by the information revolution. Moreover, developing custom DOD-unique solutions, while necessary in many cases, is orders of magnitude more expensive than modifying commercial solutions that allow piggy-backing off of previous development. The information revolution is being driven by the private sector, and U.S. adversaries are not shy about exploiting commercial technologies. Hedging and flexibility must be a significant part of U.S. strategy for coping with the continued evolution of information technologies.⁹

Degraded Communications

In order for UxVs to be capable war-fighting assets on the battlefield, they must be more than simply missile sponges. Large numbers of dumb drones sent forward to soak up enemy defenses are not nearly as innovative as intelligent, synchronized, swarming maneuverable UxVs. Communication links are the Achilles’ heel of remote-controlled UxVs, however.

UxVs must either rely on communications links back to human operators or depend on autonomous programming to carry out missions. Today’s UxVs are largely remote controlled, although some tasks use human-automation teaming, such as UAVs flying point-to-point or taking off and landing autonomously. A spectrum exists between remote control and full autonomy, and as a system moves further down this spectrum toward greater autonomy, less bandwidth is required for mission execution. The vulnerability of remote-controlled UxVs to potentially crippling communications disruptions will drive unmanned vehicles to greater autonomy, particularly if U.S. adversaries continue to invest in counter-communications abilities.

Even if reliable backup communications could be assured, in a communications-degraded environment, autonomy could free up precious bandwidth for other tasks. Onboard automated video processing technology, for example, like the commercially available Archerfish security camera that monitors an area and alerts a human only when a person or vehicle enters the frame, has the potential not only to free up humans from having to watch thousands of hours of video footage but also to significantly reduce satellite communications demands.¹⁰ The bandwidth required for full motion streaming video is roughly an order of magnitude more than the command and control functions required of a UAV.¹¹ Automated video processing onboard a UxV would significantly reduce the bandwidth demands that the UxV places on the network, increasing resiliency in the event of degraded communications.

Autonomy and Use of Force

As UxVs shift from a remote-control form of operations to a human-automation teaming concept of operations, defense policymakers, military leaders, and weapons designers will need to determine what kinds of decisions are appropriate for automation and which require human input.¹² Autonomy in combat may be desirable in two situations: if a UxV loses its communication link, and if the speed of engagements is too quick for human reaction times. As computers become more capable, more autonomy will be possible and defense leaders will have to consider when it is appropriate. In some situations, autonomy may be necessary to succeed in an engagement, such as defense against an incoming missile barrage, presenting defense

leaders with the difficult choice of delegating autonomy or risking losing an engagement.

Delegating weapons use to autonomous systems raises a host of difficult ethical, moral, legal, and policy questions. The fact that DOD has had automated systems for decades that defensively engage aircraft and missiles—the ship-based Aegis and land-based Patriot—belies the notion that it will be easy to draw clear, stark lines on the use of force. The track record of those systems, on the other hand, suggests that additional policy guidance on autonomy is needed. Flaws in the Patriot’s autonomy played a role in the downing of two coalition aircraft—killing the pilots—and the targeting of a third aircraft in 2003.¹³ Similarly, although the actual engagement decision was made by a person, human-machine interaction failures led to confusion within the USS *Vincennes* command center that caused Iran Air Flight 655 to be improperly identified as a hostile Iranian F-14 fighter in the Persian Gulf in 1988. The *Vincennes* subsequently engaged the civilian airliner with two surface-to-air missiles, downing the aircraft and killing all 290 passengers onboard.¹⁴ Clearly, existing DOD operational testing and evaluation procedures do not adequately ensure that autonomous weapons are sufficiently fault-tolerant and safe for use, including ensuring that human-automation interfaces provide digestible information for informed decisionmaking.

Restraints on autonomous weapons to ensure ethical engagements are essential, but building autonomous weapons that *fail safely* is the harder task. The wartime environment in which military systems operate is messy and complicated, and autonomous systems must be capable of operating appropriately in it. Enemy adaptation, degraded communications, environmental hazards, civilians in the battlespace, cyber attacks, malfunctions, and “friction” in war all introduce the possibility that autonomous systems will face unanticipated situations and may act in an unintended fashion. Because they lack a broad contextual intelligence, or common sense, on par with humans, even relatively sophisticated algorithms are subject to failure if they face situations outside of their intended design parameters.¹⁵ The complexity of modern computers complicates this problem by making it difficult to anticipate all possible glitches or emergent behavior that may occur in a system when it is put into operation.¹⁶

Safeguards and control measures will be necessary to ensure that autonomous systems, in the event of failure, revert to safe modes of operation and do not lead to unintended consequences, such as fratricide, civilian casualties, or unintentional escalation. Rigorous operational testing and evaluation, including tests with dynamic Red teams, will be essential to ensuring that all of the potential weaknesses and failure points of autonomous systems are fully understood before they are deployed to a real-world operation. Operators must be confident that they can accurately predict behavior and that systems are failsafe if they are to “trust” autonomous weapons for use.

The Future of UxVs

There is a natural hesitancy on the part of military leadership to embrace autonomy. This will be challenged by the widespread future proliferation of adversary autonomous UxVs. While the United States enjoys a lead in UAV technology today, other nations are experimenting with novel concepts of operation and may be more accepting of autonomy. A number of countries already possess fully autonomous antiradiation UAVs that self-target enemy radar installations.¹⁷ Moreover, the underlying technology behind autonomy is driven not by the U.S. defense industry, but by the exponentially advancing pace of computer processing power in the private sector, making the barriers to entry in developing UxVs extremely low.¹⁸ Whether UxVs bring about a true revolution in war remains to be seen, but it is clear that scores of countries—and even some nonstate actors—are racing ahead to develop them.¹⁹ As computer technology continues to evolve, so too will the potential of autonomous systems.²⁰ The final chapter on the capabilities and military utility of unmanned and autonomous systems remains to be written. **JFQ**

NOTES

¹ Robert W. Button et al., *A Survey of Missions for Unmanned Undersea Vehicles* (Santa Monica, CA: RAND, 2009).

² Brien Alkire, RAND, unpublished briefing, 2009.

³ Author correspondence with Captain Keith Wheeler, USN.

⁴ John Arquilla and David Ronfeldt, *Swarming and the Future of Conflict* (Santa Monica, CA: RAND, 2000), available at <www.usaraf.army.mil/

documents_pdf/READING_ROOM/Swarmng_and_the_Future_of_Conflict.pdf>.

⁵ Noah Shachtman, “Why Bomb-Proofing Robots Might Be a Bad Idea,” September 2, 2010, available at <www.wired.com/danger-room/2010/09/why-bomb-proofing-robots-might-be-a-bad-idea/#more-30222>.

⁶ Robert M. Gates, “A Balanced Strategy,” *Foreign Affairs* (January–February 2009), available at <www.foreignaffairs.com/articles/63717/robert-m-gates/a-balanced-strategy>.

⁷ Alec Klein, “The Complex Crux of Wireless Warfare,” *The Washington Post*, January 24, 2008, available at <www.washingtonpost.com/wp-dyn/content/article/2008/01/23/AR2008012303695.html>; Government Accountability Office (GAO), *Significant Challenges Ahead in Developing and Demonstrating Future Combat System’s Network and Software*, GAO–08–409 (Washington, DC: GAO, March 2008), available at <www.gao.gov/new.items/d08409.pdf>.

⁸ Autonomous vehicle technology is improving by leaps and bounds, however. See John Markoff, “SMARTER THAN YOU THINK: Google Cars Drive Themselves, in Traffic,” *The New York Times*, October 9, 2010, available at <www.nytimes.com/2010/10/10/science/10google.html>; and Elaine Kurtenbach, “Without Driver or Map, Vans Go from Italy to China,” Associated Press, October 28, 2010, available at <http://hosted.ap.org/dynamic/stories/A/AS_CHINA_EU_DRIVERLESS_VEHICLE?SITE=ORBEN&SECTION=HOME&TEMPLATE=DEFAULT>.

⁹ P.W. Singer, “How the U.S. Military Can Win the Robotics Revolution,” *Popular Mechanics*, May 13, 2010, available at <www.popular-mechanics.com/technology/military/robots/how-to-win-robot-military-revolution>.

¹⁰ “Archerfish: The Video Monitoring System that Thinks,” available at <www.myarcherfish.com/>.

¹¹ Brien Alkire et al., *Applications for Navy Unmanned Aircraft Systems* (Santa Monica, CA: RAND, 2010), 30–32, 38–39.

¹² For more on human-automation teaming, see M.L. Cummings, Andre Clare, and Christin Hart, “The Role of Human-Automation Consensus in Multiple Unmanned Vehicle Scheduling,” *Human Factors: The Journal of the Human Factors and Ergonomics* 52, no. 1 (2010), draft version available at <http://web.mit.edu/aeroastro/labs/halab/papers/Cummings_Clare_Hart_2010_draft.pdf>.

¹³ Rebecca Leung, “The Patriot Flawed? Failure to Correct Problems Led to Friendly Fire Deaths,” *60 Minutes*, June 27, 2004, available at <www.cbsnews.com/stories/2004/02/19/60minutes/main601241.shtml>.

¹⁴ Gene I. Rochlin, *Trapped in the Net: The Unintended Consequences of Computerization* (Princeton: Princeton University Press, 1997), 156–165, available at <http://press.princeton.edu/books/rochlin/chapter_09.html>.

¹⁵ Mary L. Cummings, “Automation and Accountability in Decision Support System Interface Design,” *Journal of Technology Studies* 32, no. 1 (Winter 2006), available at <http://scholar.lib.vt.edu/ejournals/JOTS/v32/v32n1/cummings.html>.

¹⁶ Charles Fishman, “They Write the Right Stuff,” *Fast Company*, December 31, 1996, available at <www.fastcompany.com/magazine/06/writestuff.html>; Charles Perrow, *Normal Accidents: Living with High-Risk Technologies* (New York: Basic Books, 1984); Robert N. Charette, “This Car Runs on Code,” *IEEE Spectrum*, February 2009, available at <http://spectrum.ieee.org/green-tech/advanced-cars/this-car-runs-on-code>.

¹⁷ “Harpy Air Defense Suppression System,” *Defense Update*, March 3, 2006, available at <http://defense-update.com/directory/harpy.htm>.

¹⁸ “Moore’s Law: Made Real by Intel Innovation,” available at <www.intel.com/technology/mooreslaw/>; “Excerpts from *A Conversation with Gordon Moore: Moore’s Law*,” Intel, available at <ftp://download.intel.com/museum/Moores_Law/Video-Transcripts/Excerpts_A_Conversation_with_Gordon_Moore.pdf>.

¹⁹ “Hezbollah Mirsad-1 UAV Penetrates Israeli Air Defenses,” *Defense Industry Daily*, April 20, 2005, available at <www.defenseindustrydaily.com/hezbollah-mirsad1-uav-penetrates-israeli-air-defenses-0386/>. Computer scientist Bob Mottram argues that the application of robots for terrorist or disruptive purposes is far more likely than a “Terminator scenario”: “Unlike conventional fighter planes or tanks, telerobots capable of delivering deadly force will not be expensive to manufacture and so will inevitably fall into the hands of non-state actors which may include criminal gangs and cults. As a near term scenario, imagine a cult consisting of a few tens of followers building a hundred telerobots equipped with firearms, then driving them into a city center, under supervisory control similar to a real time strategy game. All of the technology needed for such a dastardly plan exists today, and will only get cheaper and less complex with time.” See “POLL: Is a Terminator Scenario Possible?” available at <www.hplusmagazine.com/articles/ai-poll-terminator-scenario-possible>.

²⁰ Gordon Moore: “I can see the next two to three generations of technology will be likely to proceed, so we have 10 to 20 years before we reach a fundamental limit, and even then that’s not the end of the progress as by then engineers will have a budget of literally millions of transistors on a chip for their designs,” as quoted in “Moore’s Law: At Least 10 to 20 Years Before the Limit Is Reached,” available at <www.engineerlive.com/Electronics-Engineer/Interview_Opinion/Moores_Law_at_least_10_to_20_years_before_the_limit_is_reached/13295/>. Doubling every 18 months for 20 years results in a net 10,000-fold increase ($2^{(20/1.5)} = 10,321.27$).

DOD (Jeremiah Erickson)



SECURITY COOPERATION, SECURITY ASSISTANCE, AND BUILDING PARTNER CAPACITY

Enhancing Interagency Collaboration

By SHARIF CALFEE, JOSEPH LEE,
PETER CRANDALL, and YOUNG ROCK AN

I am a great believer that strength and diplomacy go together; it is never one or the other. Today foreign policy is a unified diplomatic, military, and intelligence effort that must be tightly integrated—a team approach.¹

—George P. Shultz

The United States has been in the business of Building Partner Capacity (BPC) of nations and allies for over 60 years, to include significant efforts during World War II, the Korean War, the Vietnam War, and throughout the Cold War in Europe. Current Department of State United States Code (USC) Title 22 Security Assistance (SA) authorities, such as Foreign Military Financing (FMF), Foreign Military Sales (FMS), and International Military Education and Training (IMET), eventually evolved from the initial forays into formalizing BPC efforts legislatively in the 1960s.

Following the September 11 terrorist attacks, the Bush administration determined gaps existed with traditional SA authorities that hindered U.S. ability to address certain counterterrorism and stability operations funding, capacity, and capability shortfalls of key partner nations. To address these shortfalls, a new set of Department of Defense (DOD) USC Title 10 BPC authorities, which eventually became known as Security Cooperation (SC) programs, were developed by DOD and State, enacted in legislation by Congress, and signed into law by the President starting in 2006.

Unlike their SA counterparts, SC programs were appropriated (that is, funded) through and managed by DOD and designed to be more agile to support geographic combatant commanders in their responsibilities to conduct BPC in pursuit of national security objectives as directed initially in Security Cooperation Guidance and later in the Guidance for the Employment of the Force.² Some programs included legislative provisions, so-called dual-key, that required the Secretary of State's concurrence on military training and equipping programs approved by DOD (typically by the Secretary of Defense himself).

The 2006 National Defense Authorization Act (NDAA), Section 1206 (Global Train and Equip program) has become the flagship DOD authority for dual-key. From the outset of their enactment, SC programs, epitomized by Section 1206, have generated substantial controversy within Congress, the executive branch, and various foreign relations and Armed Forces academic institutions. Despite notable counterterrorism successes in Yemen, Pakistan, trans-Saharan Africa, and the Philippines-Malaysia-Indonesia triborder region, Section 1206 and dual-key have become a source of friction between Defense and State within the overall debate over the "militarization of foreign policy."

Even with the rigorous debate that Section 1206 and dual-key mechanisms have generated with regard to roles and missions between DOD and State, this article seeks to demonstrate that they have produced substantial benefits to the advancement of U.S. national security policy. First, it reviews the evolution of BPC activities from inception in the 1940s to pre-9/11 so as to properly frame the context of the current situation. Next, it examines the creation and implementation of Section 1206, along with the benefits it has achieved through the dual-key mechanism, which underscores the necessity for its prudent expansion into all aspects of security assistance and cooperation activities. Last, it reviews the

Lieutenant Commander Sharif Calfee, USN, is an Action Officer on the Joint Staff, Strategic Plans and Policies Directorate, Partnership and Strategy Deputy Directorate. Major Joseph Lee, USMC, is the Operations Directorate Executive Officer for U.S. Joint Forces Command, Naples, Italy (North Atlantic Treaty Organization). Major Peter Crandall, USA, is assigned to Special Operations Command—U.S. Joint Forces Command. Major Young Rock An, ROKAF, is the Commanding Officer of Safety Flight in the Republic of Korea Air Force 203^d Flight Training Squadron.

Secretary of Defense's proposed BPC Shared Responsibility, Pooled Resources (SRPR) fund and considers how this proposal could establish a mutually beneficial architecture for enhanced collaboration between Defense and State in future SA and SC activities.

Evolution

According to Secretary of Defense Robert Gates:

Helping other countries better defend themselves or fight beside us—by providing equipment, training, or other forms of support—is something the United States has been doing in various ways for nearly three-quarters of a century. It dates back to the period before America entered World War II, when Winston Churchill famously said, "give us the tools, and we will finish the job."³

In the 1960s, these BPC activities were codified legislatively under the Foreign Assistance Act (FAA), which provided for the creation of SA authorities. These authorities, which eventually evolved into FMF and IMET, were appropriated through the State Department budget. Following bilateral negotiations between the United States and partner nations, these authorities provided program budget lines for training, educating, and equipping those partner militaries. They employed a model whereby State personnel assigned to U.S. Embassies abroad proposed (with Chief of Mission approval) assistance programs/budgets to improve the capabilities and capacity of these militaries, to include their professionalization. DOD (specifically the combatant commands, Services, Joint Staff, and Office of the Secretary of Defense) then assessed and made recommendations on those proposals, with State providing the final decision on the program selections, to include funding level and composition. Subsequently, State forwarded the approved programs to DOD for execution and implementation. Proposals, once approved by State during a current fiscal year, would typically not be implemented for approximately another 3 fiscal years.

Following the September 2001 terrorist attacks, pursuing BPC activities designed to directly enhance a partner nation's military counterterrorism and military stability operations capability and capacity assumed a more urgent priority. However, the pre-9/11 SA architecture, which relied on a slower process, was reexamined with a view toward their not being sufficiently agile to address

critical partner nation counterterrorism deficiencies that might suddenly arise within the traditional 3-year planning cycle. In the mid-2000s, DOD officials developed a proposal for a "Global Train and Equip" authority to increase U.S. support for foreign military and security forces in order to disrupt terrorist networks, build the capacity of legitimate states to provide security within their sovereign territory to prevent terrorists from establishing footholds, and strengthen the capacity of partner nations to participate in United Nations, regional, and U.S. coalition military missions.⁴ Under Secretary of Defense for Policy Michèle Flournoy discussed this concept in a June 2010 speech: "Nearly five years ago, the Defense Department obtained authorities enabling the military to provide training and equipment to countries with urgent security needs. This expansion of authority and funding was very helpful, adding much-needed flexibility to a creaky and slow-moving system."⁵

The creation of the Section 1206 Global Train and Equip Authority in the fiscal year 2006 (FY06) NDAA (subsequently revised in the FY07, FY09, and FY10 NDAs) would culminate several years of effort by the White House and DOD to establish new SC authorities that could meet the burgeoning need for enhancing the counterterrorism and military stability operations capacity of partner nations.⁶

Section 1206 and Dual-Key

Since its inception in 2006, the Section 1206 program has been evaluated several times. The combined DOD and State Inspector General (IG) report (2009) and Government Accountability Office (GAO) report (2010) are the most recent and relevant evaluations. They were conducted after the program had reached a level of operational maturity. The combined DOD and State team interviewed U.S. Government personnel at all levels of DOD and State, both in the field and in Washington, DC. The IG team's assessment attained buy-in since both departments' IG offices jointly conducted the evaluation and had equal input into drafting the final report. Considered a neutral and independent assessment organization, the GAO evaluation team had similar inherent credibility. Both reports issued generally positive evaluations on the Section 1206 program, to include strong endorsements about the interagency collaboration they engendered. The IG report specifically highlighted:

The synergy achieved by combining the geographical perspectives and resources of country teams . . . in Section 1206 planning and implementation is a unique strength. . . . The Under Secretary of Defense (Policy), in coordination with the Department of State, has developed a well-structured project selection process that includes vetting procedures. . . . Section 1206 projects evaluated were effective in building partner nation capacity for counterterrorism and military or stability operations. . . . Section 1206 leverages the expertise of both Departments of Defense and State. As such, Section 1206 is an excellent tool for providing corollary benefits to Chiefs of Mission.⁷

In summary, the IG report concluded that:

- DOD and State conducted the Section 1206 program in compliance with the law
- cooperation between the departments was effective
- a strength of the program is the combination of perspectives and resources of Ambassadors and combatant commanders.⁸

The April 2010 GAO report provided additional positive endorsements of Section 1206 and the dual-key mechanism:

The Section 1206 program is generally distinct from other programs. . . . DOD has demonstrated that most approved Section 1206 projects address U.S. military priorities and urgent and emergent counterterrorism and stabilization needs identified by DOD combatant commanders. Further, Section 1206 projects have done so more quickly than other programs could have—sometimes within a year, whereas FMF projects can take up to 3 years to plan.⁹

Additionally, the report concluded that:

- Section 1206 has generally been consistent with U.S. strategic priorities relating to combating terrorism and addressing instability
- the program has generally been in alignment with U.S. counterterrorism priorities
- most Section 1206 counterterrorism resources have been directed to countries the U.S. Intelligence Community has identified as priorities for the counterterrorism effort.¹⁰

Finally, the report positively endorsed the dual-key mechanism because it addressed

three key practices for interagency collaboration GAO had identified in a previous report.¹¹

Congress weighed in directly on the value of Section 1206 and dual-key when the House Armed Services Committee (HASC) commented positively on the program. In its FY10 NDAA report, the committee commented that it “regards the historical execution of this authority favorably and concludes that it is an important aspect of a combatant commander’s theater engagement strategy. The committee recognizes that it has become an important tool for building partner capacity and security cooperation.”¹²

However, one other key, unnoticed, unexpected, and unreported benefit has been the increased collaboration, integration, and coordination among the eight congressional oversight committees. Prior to the implementation of dual-key SC programs, BPC discussions with the committees were conducted in isolation from each other with authorizers separated from appropriators, HASC staffers fragmented from foreign relations/affairs

and interactions with the executive branch increased to the point where they began coordinating/integrating their respective legislative actions and even hosting joint briefings on BPC issues with the executive branch. In other words, similar to the much desired whole-of-government (that is, executive branch) objective, dual-key legislation produced a whole-of-Congress effect whereby committee members and staffers, who previously may have seldom interacted with their counterparts on other committees, now worked more closely on BPC issues.¹³ This has increased efficiency, improved the dialogue and understanding of executive and legislative points of view, and created better oversight of BPC activities by the legislative branch, to include more responsive action/replies to their inquiries.

From the outset of its enactment, Section 1206 generated substantial controversy within Congress, the executive branch, and various foreign relations and Armed Services academic institutions. It has frequently been



U.S. Air Force (Richard Simonsen)

Nuristan PRT commander discusses potential agriculture improvement projects with State Department representatives in Nangarash, Afghanistan

staffers, and Senate committees separated from House committees. This resulted in a disjointedness that both hindered the integration of legislative action on BPC issues and exasperated the executive branch in its attempts to propose BPC legislative solutions and execute programs.

With the advent of dual-key, the committees’ awareness of their peer BPC activities

labeled the leading example of the “militarization of foreign policy,” which has overridden the DOD-State balance. Such views first appeared in the Senate Foreign Relations Committee report on combatant command and Embassy activities, which was published in December 2006, less than a year after the Section 1206 authority was established by Congress. The following excerpt from the

report highlights the concern that arose before any relevant SC activity had commenced:

Such bleeding of civilian responsibilities overseas from civilian to military agencies risks weakening the Secretary of State's primacy in setting the agenda for U.S. relations with foreign countries and the Secretary of Defense's focus on war fighting. . . . As the role of the military expands, particularly in the area of foreign assistance, embassy officials in some countries question whether the Department of Defense will chafe under the constraints of State Department leadership and work for still more authority and funding.¹⁴

These reactions continue today. As Laura A. Hill and Gordon Adams (a well-respected professor in the U.S. Foreign Policy Program at American University) asserted in an article from May 2010:

Providing some of the funding through DoD committees and with one key in the pocket

this arrangement and moving to a "dual key" would undermine this balance. No amount of consultation or even concurrence requirements outweighs the influence that resources and personnel bring to policy debates.¹⁵

Other documents advance similar narratives,¹⁶ all of which make common arguments in opposition to SC authorities such as Section 1206 and the dual-key mechanism. Unfortunately, they assert hypothetical disadvantages for SC authorities but never provide any concrete supporting details or examples of how their suppositions have come to (or are coming to) fruition. However, in assessing fault with Section 1206, dual-key, and SC authorities, they must also carry the burden to prove their case with facts. Instead, they:

- relied on statements, not grounded in any established facts, that served to evoke strong emotions about the accelerated demise of State responsibilities and authorities in a manner that has not been proven

while ignoring practical questions such as whether these security cooperation authorities are producing any success in obtaining national security objectives

- warned that Section 1206 reduces congressional ability to execute its constitutional oversight duties, but are incorrect in this regard since the authority's legislation mandates oversight by eight committees that in fact vigorously exercise their prerogative for notification briefings for each train and equip program approved by the Secretary of Defense

- claimed that Section 1206 programs endanger human rights efforts within those partner nations, but failed to account for the governing legislation that requires the authority to "observe and respect human rights, fundamental freedoms, and the legitimate civilian authority within that country,"¹⁷ which is accomplished through DOD and State adherence to the Leahy Amendment,¹⁸ as well as DOD implementation of human rights and respect for civilian authority training to every partner nation military unit receiving a Section 1206 assistance¹⁹

- overlooked the outstanding inter-agency collaboration and coordination between DOD and State that has taken root and grown since the inception of SC authorities, the dual-key ones in particular.



U.S. Air Force (Sarah Brown)

Under Secretary of Defense for Policy Michèle Flournoy meets with commander of Kabul Military Training Center for Afghan National Army

of the Secretary of Defense would distort the decision making on when, where, and for what purposes such funding should be applied. . . . Traditional train and equip missions, such as those done through foreign military financing, balance these two facts by being funded as foreign assistance, overseen by the Department of State, and implemented by the Department of Defense. Creating funding outside

- ignored the positive, concrete successes that SC authorities have produced

- failed to address/consider independent evaluations, such as those conducted by the GAO and DOD/State IG offices, which positively endorsed Section 1206 and dual-key; instead, they focused on the bureaucratic/organizational disagreements that revolve around Beltway funding, authority, and status

the executive and legislative branches should expand the dual-key mechanism to other SA and SC authorities

Given the benefits of increased inter-agency collaboration highlighted in the reports, the executive and legislative branches should expand the dual-key mechanism to other SA and SC authorities. Although a detailed discussion of which authorities should be recipients is beyond the scope of this article, as a starting point, DOD and State could limit the list of authorities to those that involve BPC of military forces since both departments have equity in these endeavors.

Section 1206 authority has demonstrated its uniqueness and utility to address critical counterterrorism and military stability operations capabilities gaps of our partner nations. Furthermore, it has done it in a manner that has enhanced interagency collaboration from the field to Washington, DC, and ensured that valuable State insight

U.S. Marine Corps (Joseph M. Peterson)



Marine demonstrates firing positions to Afghan Uniform Police personnel at Forward Operating Base Jackson, Helmand Province

is incorporated into DOD SC activities while promoting human rights and civilian leadership authority over the military within partner nations and preserving congressional oversight and transparency at home. Consequently, Section 1206 and/or a follow-on program of similar type and scope should be made permanent authorities in USC Title 10.

Improving BPC Efforts

In December 2009, Secretary Gates introduced a revolutionary proposal known as the Shared Responsibility, Pooled Resources Fund to transform the future of BPC while maintaining the best aspects of the current SC authorities (namely the dual-key mechanism). Based on a British model, the SRPR would consist of three separate pools of funds dedicated to specific activities: Security Capacity Building, Reconstruction and Stabilization, and Conflict Prevention. In February 2010, Secretary Gates discussed the memorandum that he sent to Secretary of State Hillary Clinton in December 2009 outlining the SRPR proposal:

Last year, I sent Secretary Clinton one proposal I see as a starting point of discussion for the way ahead. It would involve pooled funds set up for security capacity building, stabilization, and conflict prevention. Both the State and Defense Departments would contribute to these funds, and no project could move forward without the approval of both agencies. What I found compelling about this approach is that it would actually incentivize collaboration between different agencies of our government, unlike the existing structure and processes left over from the Cold War, which often conspire to hinder true whole-of-government approaches.²⁰

only minor adjustments to implement.²¹ Each pool would have an executive agent called a “process secretariat” who would manage the function required for its operation (nominally DOD for Security Capacity Building, State for Stabilization, and the U.S. Agency for International Development [USAID] for Conflict Prevention). The SRPR would retain the dual-key feature in the three pools as it is considered one of the best aspects of SC programs. In addition to their planned funding amounts, the organizations could also contribute follow-on funding as needed.

The SRPR proposal is still under review within the executive and legislative branches.

Secretary Gates introduced a revolutionary proposal known as the Shared Responsibility, Pooled Resources Fund

On the same topic, Under Secretary Flournoy provided her thoughts on the goal of the SRPR where she explained that the proposal was a creative way to break through the current BPC impasse, which required

For this legislation to advance, Congress will have to incorporate it into the NDAA and Defense appropriations bills as well as the State Foreign Operations authorization and appropriations bills. Given the shared respon-

sibilities, Congress would likely implement legislation that maintains eight oversight committees, similar to Section 1206.

Opponents of SRPR disagreed, using the same types of arguments they previously employed against Section 1206 and dual-key. For example, Paul Clayman in *Defense News* wrote in April 2010:

*Though innovative, “pooled resources, shared responsibilities” is an inappropriate construct for conducting America’s foreign policy. For the first time, it would grant the Secretary of Defense a veto over foreign policy decisions made by the Secretary of State. That, in turn, would misalign the roles of the Defense Department in policymaking and the contribution of security assistance to America’s delicate diplomatic balance.*²²

Laura Hall and Gordon Adams noted:

[Secretary] *Gates’ shared pools proposals provide the mirage of easy money but would come with too many strings. The Secretary of State should remain the lead on foreign policy activities and maintaining control of funding ensures she, and her successors, can exercise that authority. The larger problem with these proposals is the continued perception that the role of diplomatic and development activities is supporting military operations.*²³

These authors did not propose any novel and effective recommendations that took into account the significant improvements to interagency collaboration that the SRPR forerunners, Section 1206 and dual-key, produced. Instead, they appear to support turning back the clock toward the BPC framework that existed from the Cold War to the 1990s. Given the dramatic events that have shaped the world since 9/11, it is implausible and unfeasible to return to the “good old days” and, even if it were possible, such a course of action would undoubtedly undermine the substantial interagency collaboration built through the implementation of Section 1206 and dual-key.

Furthermore, after 5 years of operation, given these authors’ arguments, there should be plenty of specific examples of how Section 1206 and dual-key activities negatively impacted U.S. national security objectives for them to cite in support their assertions. However, such examples were not provided,

and their absence profoundly undermines those arguments.

Section 1206 authority and dual-key mechanisms have proven that they enhance interagency collaboration in the pursuit of Security Cooperation activities. The Shared Responsibility, Pooled Resources fund proposal builds upon these successes and has tremendous potential to further incentivize and institutionalize interagency collaboration/coordination between the Department of Defense and Department of State, which could transcend the “roles and missions” disagreement that has simmered between the two departments for years. **JFQ**

NOTES

¹ George P. Shultz, interviewed by Rickey L. Rife, April 13, 1998, Stanford University.

² Office of the Secretary of Defense (OSD), *Guidance for the Employment of the Force* (Washington, DC: OSD, May 2008).

³ “Remarks as Delivered by Secretary of Defense Robert M. Gates, The Nixon Center, Washington, D.C., Wednesday, February 24, 2010,” available at <www.defense.gov/Speeches/Speech.aspx?SpeechID=1425>.

⁴ Nina M. Serafino, *Security Assistance Reform: “Section 1206” Background and Issues for Congress* (Washington, DC: Congressional Research Service, 2010), 3.

⁵ “Under Secretary of Defense for Policy Speech at the Center for a New American Strategy Conference as Delivered by Undersecretary of Defense for Policy Michèle Flournoy, Center for a New American Strategy, Thursday, June 10, 2010,” available at <www.defense.gov/Speeches/Speech.aspx?SpeechID=1485>.

⁶ Public Law 109–163, National Defense Authorization Act for Fiscal Year 2006, 109th Cong., January 6, 2006, 322–324, Sec. 1206, available at <www.dod.gov/dodgc/olc/docs/PL109-163.pdf>.

⁷ Inspectors General, U.S. Department of Defense (DOD) and U.S. Department of State, *Interagency Evaluation of the Section 1206 Global Train and Equip Program*, DOD Report No. IE-2009-007, Department of State Report No. ISP-I-09-69 (Washington, DC: Government Printing Office, August 31, 2009), ii–iii.

⁸ *Ibid.*, 43–44.

⁹ U.S. Government Accountability Office (GAO), *DOD and State Need to Improve Sustainment Planning and Monitoring and Evaluation for Section 1206 and 1207 Assistance Programs*, GAO-10-431 (Washington, DC: GAO, April 15, 2010), 3–6.

¹⁰ *Ibid.*, 12–13.

¹¹ GAO, *Results-Oriented Government: Practices That Can Help Enhance and Sustain Col-*

laboration among Federal Agencies, GAO-06-15 (Washington, DC: GAO, October 21, 2005).

¹² U.S. House of Representatives, *National Defense Authorization Act for Fiscal Year 2010—Report of the Committee on Armed Services, House of Representatives on H.R. 2647 Together with Additional and Supplemental Views*, 111th Cong., 1st sess., 2009, Report 111-166, 411–412.

¹³ Robert M. Gates, Memorandum for Secretary of State: Options for Remodeling Security Sector Assistance Authorities, OSD 13826-09, December 15, 2009, 6, available at <www.washingtonpost.com/wp-srv/nation/documents/Gates_to_Clinton_121509.pdf>.

¹⁴ Senate Committee on Foreign Relations, *Embassies as Command Posts in the Anti-Terror Campaign—A Report to Members of the Committee on Foreign Relations, United States Senate*, 109th Cong., 2^d sess., 2006, S. Rep. 109-52, 2.

¹⁵ Laura A. Hall and Gordon Adams, “Relying on the Kindness of Others: A Risky Partner-Building Strategy,” May 13, 2010, available at <<http://thewillandthewallet.org/2010/05/13/relying-on-the-kindness-of-others-a-risky-partner-building-strategy/>>.

¹⁶ Stephen J. Morrison and Kathleen Hicks, *Integrating 21st Century Development and Security Assistance* (Washington, DC: Center for Strategic and International Studies, January 2008), 2, 7, 10; Thomas Boyatt, *A Foreign Affairs Budget for the Future—Fixing the Crisis in Diplomatic Readiness* (Washington, DC: The American Academy of Diplomacy, October 2008), 4, 22–24; Adam Isacson, “The Pentagon’s Military Aid Role Grows,” January 26, 2010, available at <<http://justf.org/blog/2010/01/26/pentagons-military-aid-role-grows>>.

¹⁷ Serafino, 9.

¹⁸ Defense Institute of Security Assistance Management (DISAM), *The Management of Security Assistance*, 27th ed. (Wright-Patterson AFB, Ohio: DISAM, October 2007), 16–9.

¹⁹ *Ibid.*, 5.

²⁰ Gates, “Remarks.”

²¹ Flournoy.

²² Paul Clayman, “Building State Department Muscle: Link Security Assistance to Foreign Policy Priorities,” *Defense News*, April 5, 2010, available at <www.defensenews.com/story.php?i=4567294>.

²³ Hall and Adams.

A Role for NATO?

By KENNETH WEISBRODE



NATO Secretary-General Anders Fogh Rasmussen presents new NATO Strategic Concept reconfirming Alliance commitment to defend Euro-Atlantic security

NATO

The North Atlantic Treaty Organization's (NATO's) long-awaited Strategic Concept, released last November, glosses over an important topic: the collective interests of its members in the Middle East. Historically and strategically, the Middle East lies in Europe's back yard. Nearly every major security problem for Europe has an important Middle Eastern dimension. This is also true, albeit to a lesser extent, for the United States. The security that the United States purportedly provides in the Middle East has not underwritten a stable regional order; politics within and among major regional states are difficult and, in a few notable cases, hostile. Nevertheless, the security of Europe, the North Atlantic, and the Middle East is indivisible.

Dr. Kenneth Weisbrode is a historian and former defense analyst. Research for this article was conducted under the auspices of the *Stiftung Wissenschaft und Politik* and the *United States Institute of Peace*.

Regional security arrangements and policies should reflect this reality. For that to happen, strategic discussions about the region in the NATO context must take place openly, with an emphasis on overarching regional interests and well before the members of the Alliance plan to counter particular threats.

The proliferation of nuclear weapons technology is one of the region's biggest challenges. It greatly heightens the costs of potential conflict. Iran is widely believed to be on the verge of joining Israel as a de facto nuclear weapons state. Should this occur, most analysts claim, it is only a matter of time before other states—Egypt, Saudi Arabia, Syria, Turkey, and possibly Algeria and Jordan—develop their own nuclear weapons capabilities. The alternative of a nuclear weapons-free zone for the Middle East shows little sign of being adopted any time soon.

It is difficult to imagine a scenario in which a Middle Eastern nuclear arms race, however gradual, would not affect the core

interests, and therefore the strategic posture, of NATO. Yet few Alliance members want to think, let alone talk, about the subject. There may be valid reasons for keeping a discussion (and, to the extent it exists, actual planning) quiet. But silence has a price. It may cause some to conclude that NATO is giving priority to the wrong areas, or is not being as exhaustive as it ought to be in the right ones. And the silence has resulted already in mixed signals over policies such as missile defense, where differences in identifying putative aggressors have strained relations between members. The Alliance has come to appear desperate for a formula to make the necessary planning for contingencies in this critical region possible.

NATO, of course, is only as viable as its members and their own deterrents; militarily, the Alliance may not be much stronger than the sum of its parts. Yet politically, it carries a much greater weight than any single member does by itself. Accordingly, as the only multinational alliance that possesses a nuclear

deterrent and is proximate to the Middle East, NATO should consider at the earliest possible moment the nature and implications of extending a security guarantee to the territory of the region. Such a guarantee—or better put, deterrent—must be nuclear because it is the spread of nuclear weapons throughout the region that is the issue of greatest concern to NATO.

On the surface, a regional nuclear deterrent would appear to fly in the face of the global effort to curtail and roll back nuclear arsenals. However, as this moves forward, regional nuclear weapons-free zones, as well as global agreements among larger states, will probably evolve simultaneously as important means for managing a world without nuclear weapons. If the nations of the Middle East succeed in negotiating a nuclear weapons-free zone, their security would need to be guaranteed in some fashion by the Permanent Five nuclear powers both during and after the process of implementation. NATO would be in a position to contribute support and resources for this effort. Its declaratory policy, at a minimum, should include a statement of its willingness to offer such support.

Besides the negotiation of a nuclear-free zone or, conversely, an all-out regional arms race, there are only two other conceivable scenarios: the imposition of stability from the outside in the form of a semipermanent American nuclear “umbrella” over the entire region, or the emergence of an internal equilibrium or balance of power on its own.

Neither scenario is desirable. The first would place too heavy a burden on the United States and be complicated by the close U.S. relationship with Israel (whose leaders, for their part, have said that they are unenthusiastic about a U.S. umbrella). The second, as already noted, seems unlikely in the near future. The problem, therefore, should be cast more broadly as one of regional security—and the need for a credible anchor of security in the form of a deterrent—rather than as simply one of preventing an arms race or coping with one after it emerges.

Regional Context

The extent of relations between NATO and the countries of the Middle East is modest at the present time. In addition to deployments in Afghanistan and off the Horn of Africa, NATO operates two partnership programs with regional governments: the Mediterranean Dialogue, begun in 1994, and the Istanbul Cooperation Initiative, begun in 2004. The

first includes Algeria, Egypt, Israel, Jordan, Mauritania, Morocco, and Tunisia, while the second includes Bahrain, Kuwait, Qatar, and the United Arab Emirates. These programs are quite different from one another. The Mediterranean Dialogue features a multilateral policy agenda, whereas the Istanbul Initiative provides practical and technical assistance on a bilateral basis. In 2010, the Istanbul Initiative offered some 700 activities, mostly small scale, like officer exchanges and training programs in areas such as disaster relief operations. Both its efforts also include the participation of officers at the NATO Defense College.

the problem should be cast as one of regional security rather than as one of preventing an arms race or coping with one after it emerges

These efforts are useful to the extent that they build trust, familiarity, and goodwill. But they are limited by the nonparticipation of several powers, notably Saudi Arabia and Iran, as well as the persistent hostility toward Israel, making the latter’s own participation in the Mediterranean Dialogue an obstacle to its formal collaboration with the Istanbul Initiative.

Besides the limited scope of these efforts, an important impediment to having a high-level, multilateral strategic discussion in the region is the gap between declaratory and actual policy as regards nuclear weapons. To date, Israel has not publicly declared itself a nuclear power. Iran continues to insist that its nuclear ambitions are entirely peaceful, a claim backed publicly by Turkey. Saudi Arabia and the other regional powers state that they have no nuclear ambitions whatsoever. The global nuclear agenda has tended to avoid discussion of deterrence and nuclear force postures. Its emphasis has been on nuclear security, non-proliferation, and the march to zero.

Similarly, the U.S. Nuclear Posture Review, released in April 2010, noted a shift toward a more modest posture resembling a minimum deterrent. It makes only a handful of references to the Middle East and says nothing about possible roles for NATO there. Yet at the same time, former and current U.S. officials have spoken out strongly in favor of maintaining NATO’s nuclear deterrent for the foreseeable future.

Discussions about peace and security in the region, therefore, must operate somewhat surreally. Attempts to bridge the gap—such as the short-lived promotion of an alliance between Israel and Turkey about a decade ago—have done little to achieve overall security. The vision of a peaceful, stable, and secure region that was put forth at Madrid in 1991 remains a distant prospect.

Deterrence Today

It is axiomatic that no credible security guarantee can exist absent a strong deterrent. Thinking in NATO about deterrence has not advanced very far since the end of the Cold War, however. Rather than updating and refining deterrence as a forward posture, there has been a shift, led by France and certain quarters in the United States, toward thinking more conventionally about regional military balances and the marginalization—and, ultimately, the elimination—of nuclear weapons as warfighting instruments—in other words, a nuclear force in being or a more purely existential deterrent (similar to what Japan currently possesses). The problem is that there is almost no evidence that such a view has a following in the Middle East. By contrast, it appears that nuclear weapons are still seen as instruments of military superiority.

If NATO were to apply a nuclear force in being to the Middle East, it would probably do so in a manner that theorists call “pivotal deterrence,” which is a form of extended deterrence, or “collective-actor deterrence” involving multiple parties with the ultimate goal of transforming a region into a security community whereby collective security replaces fluctuating bilateral or multilateral power balances.

No deterrent is foolproof, of course. Deterrence will not succeed in every case. But this need not proscribe the value of the deterrent, which comes less from what it guarantees operationally than from the political and strategic benefits that it can bring in the middle and long term. For example, it could happen that Israel, should it launch a nuclear first strike on a neighboring state even if it were attacked first by conventional means, would see NATO come to the defense of that state. The likelihood of this ever happening in the real world is remote. The point of a deterrent, however, is that it makes such a choice even less likely while reassuring smaller powers that they need not compete in order to forestall it.

Extending deterrence to third parties whose instability poses an indirect threat to

the members of the Alliance could very well become one of the most important tasks for NATO in the coming years.

Practical Considerations

How might a Middle East deterrence regime come into effect? The members of NATO could amend the treaty to extend an Article V commitment to the entire region. This would mean, in effect, that NATO would defend any country attacked with nuclear weapons. The nature of the prescribed attack should apply in phases, although in keeping with the spirit of the treaty, the precise response need not be specified.

Alternatively, NATO members could merely issue a communiqué along these lines, or extend it only to particular countries. Or they could follow a precedent set by former Secretary of State Dean Rusk, who once proclaimed (in reference to Yugoslavia) the existence of a “gray area” where NATO might respond with armed force.

which is a U.S. formulation combining missile defense with a range of offensive and other defensive capabilities.

Of course, deterrence is as much a political as a military strategy in any instance where an outside power or group of powers provides guarantees that deter aggression while limiting the independence of those under protection. This is not easy, especially in parts of the world where any imposition of order from the outside carries the tinge of imperialism. Fluctuating relationships within the Middle East make such limitations exceedingly difficult to manage. Several governments, especially those of smaller states that would presumably be the most eager for a NATO commitment, are keen to maintain good relations with multiple parties. For example, most members of the Gulf Cooperation Council have preferred to downplay concerns about Iran, letting the United States take the lead in confronting it over its nuclear program. The reasons have to do not only with their dependence on the

the Middle East. Russian and, someday, even Chinese collaboration could make for a more broadly based deterrent. However, it would also probably be less credible, and neither Russia nor China has shown any willingness to collaborate formally with the Alliance in the region. But both have incentives to do so and ultimately would have to guarantee a nuclear weapons-free zone should it come into existence.

At the very least, a generic territorial deterrent ought to preclude talk of Alliance enlargement in the region, or the likelihood of particular Middle East states acquiring special status vis-à-vis NATO unless the members of the Alliance reach a consensus that such a relationship, as indicated above, is in their combined interest and is consistent with the extended deterrent.

There are two final considerations to bear in mind. First, NATO planners should continue to improve their familiarity with the strategic culture in this region and with the thinking of key regional actors about deterrence and other basic doctrines. This could be furthered by a reinvigoration, perhaps under NATO auspices, of the long-dormant Arms Control and Regional Security working group. Similar mechanisms may also exist bilaterally, following the model of the NATO–Russia Council; some Iranians, for example, have proposed something like it for their country.

Second, no credible deterrent in the Middle East could exist absent a clearer set of strategic priorities for NATO itself. That it has moved from a defensive to a security alliance is now repeated as a mantra, but it is still unclear what this means outside Europe, especially when NATO insists on preserving its “core” mission of defending Alliance territory. Multiple missions need not be incompatible, but some clearer articulation of NATO’s defense and security roles *a tous azimuts* is a precondition to understanding its deterrent role and allocating the right balance of forces and deployments, particularly the dual-capable aircraft and other nuclear forces that remain in Europe.

A NATO nuclear deterrent for the Middle East would help to provide the underlying stability the region requires. It might also make a regional nuclear arms race less likely. Finally, it could have the added advantage of concentrating thinking at NATO about what exactly the role of the Alliance is meant to be toward its extended neighborhood. Sooner or later, it will need to have one. **JFQ**

no credible deterrent in the Middle East could exist absent a clearer set of strategic priorities for NATO itself

NATO would have to consider the effects of such a deterrent posture on deployments, and vice versa. The presence of NATO troops could serve as a kind of tripwire that could complicate the Alliance’s own deterrent, not to mention its decisionmaking, in an unfavorable way.

With sufficient forethought and preparation, however, a strong NATO nuclear deterrent need not necessarily be inconsistent with a readiness to deploy troops in specific contingencies. Current thinking in NATO appears to be receptive to such a composite approach—that is, the so-called New Triad,

U.S. military presence and their simultaneous efforts to gain favor (or to preserve options) with Iran, but also with the need to maintain a public posture against Israel and its own nuclear status. Here, too, domestic politics matter insofar as sympathy exists in these countries for Iran and its positions.

Insofar as NATO is identified closely with the United States, some regional states may desire to have a less conspicuous American umbrella, and for this reason an Alliance deterrent could be a more palatable option.

Under ideal circumstances, NATO would not be alone in extending deterrence to



NATO’s first ever theater ballistic missile defense capability is turned over to Alliance military commanders, January 27, 2011

DECISIVENESS in War

By PHILLIP S. MEILINGER

Colonel Phillip S. Meilinger, USAF (Ret.), served in the U.S. Air Force for 30 years. He holds a Ph.D. in history from the University of Michigan. He is the author of 8 books and 90 articles on military affairs.

Decisive victory has been sought by military commanders for millennia. It is the goal to which leaders aspire, for if they achieve such victories, it means the war ends more quickly, reducing the cost in both blood and treasure.

The list of decisive victories in the long history of war is relatively short, and decisiveness in war is often confused with a battle that is merely a turning point, or, worse, that has only tactical and therefore transient impact on the course of a war. My purpose is to define the meaning of *decisive victory* and to give examples of such engagements, while also distinguishing them from battles. A relevant question is whether such decisions can still be achieved in modern war.

Roman infantry encounters Carthaginian assault at Battle of Zama

Henri-Paul Motte



Battles Won and Lost

Wars are fought for specific purposes, and these purposes should meet several criteria. They should be determined only after considerable thought by a nation’s recognized leaders—not by private or moneyed interests. The purposes for going to war should concern weighty issues of state—not matters of whim or personality. The goals for which the war is to be fought should be achievable—even though those goals may change during the course of the war. A belligerent can modify his goals during a war based on a variety of factors, and that does not necessarily mean the original goals were ill advised or unattainable; circumstances change. Finally, leaders should prepare the nation for war, both materially and psychologically. These criteria appear to be straightforward and adhere to common sense, and most countries entering a war believe they have fulfilled them. It is only later, as a nation begins to taste defeat,

not surrender, and Hannibal was never strong enough to besiege the Eternal City.

A brilliant young Roman general, Publius Cornelius Scipio, then restructured and retrained his legions and took the war to the enemy. He crossed the Mediterranean and moved on Carthage itself. Hannibal was forced to return and defend his capital. In March 202 BCE, the Romans under Scipio with approximately 35,000 men met Hannibal’s slightly larger army near Zama, south of Carthage.¹

Hannibal attacked first, releasing elephants in the hope of disrupting the Roman formation, but the flexible maniples instituted by Scipio simply parted to allow the animals to pass to the rear. The superior Roman cavalry charged next, sweeping Hannibal’s horsemen from the field. The two infantry contingents then clashed and fought desperately for the next several hours. When it appeared the Carthaginians were gaining the upper hand, the Roman cavalry returned after their rout of

the British, and neither side seemed close to victory, although, significantly, the French joined the Americans in 1777. The following year, the war shifted to the southern colonies, where the British captured the ports of Savannah and Charleston. A British army under Charles Cornwallis moved into the interior and attempted to destroy colonial resistance. Washington then sent Nathanael Greene to take command in the south. Cornwallis pushed for a conclusive victory, but Greene cleverly refused to execute anything but delaying actions. Exasperated, in April 1781 Cornwallis elected to abandon the Carolinas and move north into Virginia. Arriving at Yorktown in August, he intended to resupply and reinforce his troops by sea, but Yorktown turned into a trap.

In a crucial engagement in the Chesapeake, the Royal Navy was driven off by the French fleet, which then blockaded Yorktown from the sea. Simultaneously, Washington marched south with a large contingent of American and French troops to bolster Greene’s forces, which had invested Cornwallis by land. Washington took command of the combined allied army of 17,000 men and laid siege to Yorktown. After an abortive attempt to break free, Cornwallis realized the hopelessness of his situation, and on October 19, he surrendered his 8,000 men.³

The loss of a major army in the American colonies, combined with the active involvement of the French fleet, caused consternation in London. The war had become increasingly expensive and unpopular, and Britain sued for peace. Yorktown had won independence for the United States of America.

Yet it is also true that *great victories are often of a negative variety*: rather than overthrowing an enemy, the result is the assurance that the enemy cannot win—the victor therefore ensures his own survival. There have been several such “negative” decisions in history.

The Persians under Darius invaded Greece in 490 BCE. The army landed on the beach at Marathon, about 20 miles from Athens, and was met by a Greek force led by Miltiades. The Greeks defeated the Persians, who then retreated to Asia. Ten years later, the Persians, now led by Xerxes, returned, determined to redress their previous defeat. Checked temporarily at Thermopylae, they went on to occupy most of northern Greece, including Athens.

The Greeks did not surrender. They gathered a fleet of 350 ships with 60,000 men under the command of Themistocles and

great victories are often of a negative variety: rather than overthrowing an enemy, the result is the assurance that the enemy cannot win

that it realizes the criteria were not followed after all. At that point, it is usually too late. Kaiser Wilhelm II, Adolf Hitler, Benito Mussolini, Hideki Tojo, and countless others over the centuries thought they had fulfilled these requirements when deciding for war. The majorities of their populations and militaries acquiesced to, if not agreed with, them—at first. It is in retrospect that the decisions look ill advised and rash.

Therefore, the first requirement of decisive victory is that *it achieves the goal of the belligerent*. More to the point, that goal must be a matter of great importance, such as the conclusive destruction of a dangerous enemy. For example, in the third century BCE, two mighty empires arose in the Mediterranean area, Rome and Carthage. Both empires fronted the sea, and both viewed it with proprietary eyes, thus bringing them into conflict.

The First Punic War lasted from 264 to 242 BCE and saw Rome victorious. Tensions remained, and in 219, the Carthaginian general Hannibal renewed hostilities. With an army of 90,000 men, he secured Spain and then crossed the Alps into Italy. For the next decade, Hannibal shattered every Roman army sent against him: his most noted victories were at Trebia, Lake Trasimene, and Cannae. But Rome would

the enemy cavalry and struck the Carthaginian infantry in the rear. Most of Hannibal’s army was destroyed or captured, although he himself escaped. The war was over. Henceforth, Scipio would be known as “Africanus.”²

Zama ended Carthage as a military factor, while at the same time elevating Rome to a world power—a status it held for the next six centuries.

The next important goal that can serve as a basis for decisive victory is that of *independence*. The American colonies began to chafe under British rule after the French and Indian War. The core issue involved taxation. The late war had been expensive, and London felt justified in raising taxes to help pay the bill. The colonies disagreed, and over the next decade there were a series of demonstrations against the new taxes, such as the Boston Tea Party in December 1773.

The British tightened the screws, and in April 1775, a force of Redcoats marched out of Boston to confront the colonials at Lexington and to confiscate the military stores at Concord. Fighting broke out and blood was spilled: the American Revolution had begun.

Over the next 3 years, George Washington, commander of the Continental Army, fought several inconclusive battles against



Lord Cornwallis's forces surrender after siege of Yorktown

stationed them near the island of Salamis, directly opposite Athens. In late September 480 BCE, the Persian fleet, 700 strong, was confident of victory, and Xerxes set up his golden throne atop a hill to watch the battle that would give him mastery of all of Greece.

Themistocles wisely selected the narrow channel between the mainland and Salamis. Greek ships were heavier than Persian vessels, which were more maneuverable. The purpose of trireme warfare was to ram the enemy ship and then back out quickly while the victim foundered. In confined waters, the agility of the Persians was of no avail; instead, the heaviness of the Greek boats made them superior as rammers.

The Greeks attacked at 7:00 in the morning, and the battle lasted 12 hours. The Persians, who had rowed all the previous night to arrive at Salamis, were already fatigued and thus at a serious disadvantage from the outset. Throughout the day, the heavier Greek ships battered the Persians, and as evening fell, the invaders broke and fled. Many Persian ships were then caught from behind and sunk. Overall, the Persians lost over 200 ships and as many as 20,000 men.⁴

With the Persian fleet destroyed, Xerxes returned home in disgust, but left behind an army 70,000 strong to mop up the remains of the Greek armies. Without fleet support and far from their supply base, however, the Persians were in peril. In July 479 BCE, a Greek army of 40,000 under the command of Pausanias met the Persians at Plataea. The Persians attacked the Greek phalanx and were initially successful, but the stoutness of the Greeks, especially the Spartan contingent, turned the tide. By the end of the day the Persians, driven back against a stream, were slaughtered.⁵

Salamis and Plataea meant the end of Persian plans for the subjugation of Greece. These battles did not break up the Persian Empire—it was far too massive and powerful—but the victories ensured Greece would remain Greek. “Western Civilization” was saved by the *negative* decisive victories at Salamis and Plataea.

Another such negative victory occurred during World War II. The Treaty of Versailles that ended World War I was merely a truce. When Adolf Hitler was appointed chancellor in 1933, rearmament, combined with a more bellicose foreign policy, accelerated. In

1936, Germany reoccupied the Rhineland; in 1938, it annexed Austria and moved into the Sudetenland of Czechoslovakia. When Hitler invaded Poland in September 1939, France and Britain declared war. Poland fell, soon followed by Norway, Denmark, Belgium, and France in blitzkrieg strikes. By July 1940, Britain was alone.

Hitler intended to invade Britain, and Operation *Sea Lion* was the plan to mount an amphibious assault. Before he could attempt such an effort, however, he needed to ensure control of the English Channel, and for that, he needed air superiority *over* the channel.

The German onslaught began on August 12, 1940, when the Luftwaffe sent over several hundred bombers escorted by fighters. The intent was to bomb targets so vital to Britain that the Royal Air Force (RAF) would be required to rise and defend them. The goal was to bring Fighter Command to battle and then destroy it. Initially, German targets focused on radar sites, whose loss would pose a serious danger to the RAF. After only 3 days, however, the Luftwaffe switched targets and began concentrating on airfields. This, too, was a major concern for Fighter Command,

National Archives and Records Administration



Firemen and members of London Auxiliary Fire Fighting Services train in July 1939

National Archives and Records Administration



St. Paul's Cathedral in London survives fire raid

and over the next month “the few” found themselves “gasping on the ropes.” They were saved when Hitler, angered over the RAF’s bombing of Berlin, directed his bombers to concentrate on British cities in retaliation. On September 15, a force of 200 bombers, heavily escorted, attacked London but suffered 25 percent casualties in the process; these were unsustainable losses. This raid, which occurred on the date originally set for the invasion, was the Luftwaffe’s last major daylight attack: the blitz moved to the safety of night. This decision spelled the end of German attempts to gain air superiority for an invasion.⁶

By the end of October, the Battle of Britain was over. One of the great negative decisive victories in history had saved the island nation. When Hitler realized he could

not achieve air superiority over the English Channel, he knew an invasion was impossible. His attention now turned to the east—toward Russia—and Britain survived to become the “unsinkable aircraft carrier” for the Allied reinvasion of the Continent in 1944.

There is a time element involved in the notion of decisiveness. A smashing victory, regardless of the death toll, is not decisive if the enemy is able to raise another army and continue the war. A victory should not be reversible except in the long term—50 years would seem to be a minimum. So, for example, the iconic battle of Cannae where Hannibal annihilated 16 Roman legions in 216 BCE was a brilliant tactical victory, but the strategic results were minimal. Rome formed more legions, the war lurched on for 14 more years, and Carthage eventually lost. By the same

token, Chancellorsville was one of Robert E. Lee’s masterpieces. Heavily outnumbered by Federal forces, Lee won a crushing victory, but the Civil War continued and went badly for the South. Chancellorsville was a transient tactical advantage for the Confederates, nothing more.

This time element is important. If the defeated side uses the interlude as a truce so it can rebuild its forces and resume the war, the battle was not decisive at all. Most of Napoleon’s victories fall into this category; they merely ended hostilities temporarily while both sides regrouped before going at each other again. French triumphs over the Austrians at Ulm and Austerlitz in 1805 broke the Third Coalition, but Austria attacked again in 1809. After Napoleon’s victory at Wagram, Austria once again sued for peace—only to initiate hostilities in 1813. Similar Napoleonic battles that led to truces, not lasting peace, included Jena-Auerstadt over the Prussians in 1806 that shattered the Fourth Coalition, and the bloody decision over the Russians at Friedland, leading to Tilsit in 1807.⁷ Both Prussia and Russia rejoined the fight against Napoleon a few years later.

Smashing victories often lead to surrender and war’s end—they are the “last battle.” After the attack at Pearl Harbor in December 1941, the Japanese swept to victory throughout Asia. Much of China and Indochina fell into their hands, as did Korea, the Philippines, Singapore, Malaysia, the Dutch East Indies, and a host of islands large and small. The great naval air battle of Midway in June 1942—the opposing fleets never saw one another—was a turning point, but there

Library of Congress



Robert E. Lee surrenders to Ulysses S. Grant at Appomattox Court House

was still a long slog ahead. In August 1944, the Mariana Islands were recaptured, and airbases were built there to house long-range B-29s, which then began to hit the Japanese home islands. Even so, invasions were planned and thought to be essential: the assault on Kyushu was scheduled for November 1, 1945, and a larger one was slated for Honshu the following March. A new weapon would make these operations unnecessary.

Since early 1942, scientists had been studying the possibility of splitting the atom to release an astounding amount of energy. A major scientific endeavor, the Manhattan Project, built an atomic weapon, and the Army Air Forces formed a special B-29 unit to deliver it. The 509th Bomb Group, commanded by Colonel Paul W. Tibbets, moved to Tinian in the Marianas in May 1944 and trained to deliver the top-secret bomb.⁸

On July 26, 1945, President Harry Truman sent Japan an ultimatum: surrender or suffer destruction. The Potsdam Declaration was rejected, and orders were issued to prepare for a launch. On August 6, the *Enola Gay*, piloted by Tibbets, lifted off from Tinian and dropped an atomic bomb on Hiroshima. Crewmembers would later recall the purple cloud building upward for 10 miles, and the cauldron below that resembled a “pot of bubbling hot tar.”⁹ The center of Hiroshima was destroyed, and over 60,000 died.

Japan still resisted, and a second atomic bomb was dropped on Nagasaki on August 9. Six days later, Emperor Hirohito made a radio address to his people citing “a new and most cruel bomb” that contained a power to do “incalculable” damage. He was surrendering.

The atomic strikes on Hiroshima and Nagasaki ended World War II, representing one of the most decisive victories in history and saving millions of Japanese and American lives.¹⁰ Sixty-five years later, Japan remains one of our closest allies.

Although one generally refers to decisive *battles*, sometimes it is *wars* that are decisive. Some conflicts are attritional slugfests that kill thousands yet fail to yield conclusive battlefield decisions. The American Civil War was one such event. Although it was the bloodiest war in U.S. history and witness to several tactical gems—the Chancellorsville battle already noted as well as the Shenandoah Valley campaign of Thomas Jackson and the persistent industriousness of U.S. Grant at Vicksburg—the conflict ended in April 1865 with a whimper, not a bang. The

exhausted and depleted armies of Lee and Joseph Johnston simply gave up. Yet the war was decisive in the truest sense of the word: the Confederacy would not rise again, and the impact of the war on American society and its mythos was profound.¹¹ Similarly, World War II contained many huge battles, but the decisive defeat of Germany—and the death of German/Prussian militarism—was due to grinding and inexorable pressure on multiple fronts—massive land armies east, west, and south, a strangling naval blockade, and strategic bombing.

It is necessary, however, to differentiate between the decisive victories noted above and a *turning point*—a battle or campaign that changes the momentum in a war. Usually identified in retrospect, it is a decision where the side that had been losing sees its fortunes reversed and then moves with increasing momentum toward the attainment of victory. In modern history, such turning points include Saratoga (1777), where American colonial forces defeated a British army, thus

a turning point is a decision where the side that had been losing sees its fortunes reversed and then moves with increasing momentum toward the attainment of victory

securing crucial French support; Gettysburg (1863), whose aftermath saw the South in constant decline; Midway (1942), the battle that broke the back of the Japanese carrier fleet; Stalingrad (1943), where Soviet troops destroyed the chances of German victory in the east; and Tet (1968), when the Viet Cong, although largely destroyed as an effective fighting force, broke the will of the American people and their political leaders. All of these turning points were important battlefield decisions, but they were not decisive because they were not conclusive—the wars continued, sometimes for several years.

Key to the understanding of decisive victory is that the enemy must acknowledge defeat. He must agree to give up the fight. Battlefield success may or may not have a role in that acknowledgment. Napoleon defeated the armies of Spain, but he did not defeat the Spanish people. In 1870, the French army was crushed by the Prussians at Sedan and Metz, and Paris was surrounded. Yet the French

people refused to admit defeat, and the war continued for 5 more months. Similarly, Germany was never reconciled to its defeat in 1918. Almost immediately following the Armistice, it secretly began to prepare for a rematch. On the other hand, the United States suffered fewer than two dozen dead in the 1993 battle of Mogadishu, but the deaths of those relatively few Soldiers broke the will of American leaders. The Nation pulled out and abandoned the Somalis to their fate. In sum, an enemy’s will may be broken without breaking his military forces, and forces can be crushed without shattering the nation’s will. In this sense, *decisive victory has a human, cultural dimension that must not be ignored.*¹²

The likelihood of achieving decisive victory seems to have decreased over the past few centuries. Russell Weigley argues this was due to the emergence of the nation in arms. Not only were armies substantially larger than in the past—thereby making it more difficult to destroy them all at once—but also warfare became increasingly total. More personnel, resources, and funds were devoted to war, and this totality included a lack of concern for the impact of military operations on the civilian populace. The result was a seemingly inexhaustible supply of men and materiel combined with a heightened passion of the populace that generated a reluctance to quit. A knockout blow was almost impossible. Nations lost hundreds of thousands of men on the Western Front in 1914 and 1915, but still drafted millions more to continue the fight.¹³ This situation changed after World War II, when the deployment of thousands of nuclear weapons made nations less inclined to risk their survival in war. Limited war returned. Decisive victory has thus now become even more elusive than in centuries past. The overwhelming military triumph of the coalition in the Persian Gulf War of 1991 did not lead to a sound peace, as America’s continued involvement there attests. As always, the purpose of war must be a better condition in its aftermath, and destroying armies may have little or nothing to do with achieving a better peace.

Combining these considerations leads us to a definition of *decisive victory*: achieving major, long-term political results in war that include attaining grand strategic objectives. These results can be negative; the enemy is prevented from achieving his objectives as a result of losing a key engagement, or the victor of a battle ensures he will not lose the war.

Decisiveness Today

Decisive battles have been sought by commanders throughout history. The defeat of a powerful foe, the conquest of a rich and fertile region, the quest for freedom, and the desire to spread ideas or beliefs to other areas have all been impulses leading to conclusive and long-lasting victories. Noted above are some of these engagements, both positive and negative, that decided the outcome of major wars. These wars were in turn monumental events in world history. Key to all of them was the attainment of conclusive political objectives and, ultimately, a better peace—at least for the victor. That, after all, is the object of war.

Should decisive victory remain our goal, and is it still achievable? In my view, the answer to both questions is yes—if we adhere to the definition of achieving major, long-term political results that are attainable given the resources we are willing to commit. That, as noted, does not mean we must crush our opponent or destroy his military forces. Even Carl von Clausewitz, the foremost advocate of conclusive battle, admits an exception to his rule: “It is possible to increase the likelihood of success without defeating the enemy’s forces. I refer to operations that have *direct political repercussions*.”¹⁴ Although precisely what he meant by such alternative operations is unclear, their suggestion permits present-day strategists to consider ways of achieving decisiveness without *assuming* a bloody force-on-force engagement. B.H. Liddell Hart advanced a possible solution several decades ago: “The real target in war is the mind of the enemy command, not the bodies of his troops. If we operate against his troops it is fundamentally for the effect that action will produce on the mind and will of the commander.”¹⁵ A more recent military theorist, John Boyd, echoed this view. Boyd’s OODA Loop (observe, orient, decide, act) posits a strategy of operating within an enemy’s decision cycle—to act more quickly than the enemy and thus render his responses belated and irrelevant, to fatally confuse the mind of the enemy leader.¹⁶ Liddell Hart and Boyd are alluding to a more cultural approach to war that should inform our strategy. Regarding counterinsurgency, a form of war even more politically driven than most, this usually translates into winning the hearts and minds of the populace.

These ideas are relevant to our current situations in Iraq and Afghanistan. Decisive victory may still be possible in both countries, but our leaders must give increased thought

to exactly what type of peace they wish to achieve—and for what results they are willing to settle. In this regard, Michael Howard made the insightful comment that the “honor” of the defeated must be taken into consideration if true peace and reconciliation are to occur.¹⁷ A defeated country, even when decisively defeated, must eventually rejoin the family of nations as an equal partner. How can we ensure that occurs in Iraq and Afghanistan?

My definition of decisive victory focuses on results, and, critically, results are in the eyes of the beholder. Because war is a cultural phenomenon as much as it is a political one, it is quite possible that decisiveness for one side may be defined differently for the other, depending on what its culture is willing to accept. Nonetheless, the only sensible object of war is a better peace. Decisive victory is usually an essential if not always sufficient factor in achieving that result. More importantly, we must think through in advance what the following state of peace should look like—a difficult task that is too often ignored precisely because of that difficulty. How do we defeat our foes while at the same time allowing them to preserve their honor? That is the question now confronting us in the Middle East. **JFQ**

and the Atomic Bomb (Washington, DC: Center of Military History, 1985).

⁹ For his personal account, see Paul W. Tibbets, *Return of the Enola Gay* (Columbus, OH: Mid Coast Marketing, 1998).

¹⁰ For an excellent discussion regarding casualty figures, see D.M. Giangreco, “Casualty Projections for the U.S. Invasion of Japan, 1945–1946,” *Journal of Military History* 61 (July 1997), 521–582. Given the numbers of troops involved on both sides, and the casualty rates of the Pacific war up to that time, it is likely the invasions of the Home Islands would have resulted in well over 2 million military dead on both sides—the civilian total would have been horrendous.

¹¹ In one of his oft-quoted one-liners, Clausewitz stated that “in war the result is never final.” But of course, wars are often very final indeed, as the experience of the Confederacy, or Carthage, illustrates. See Carl von Clausewitz, *On War*, ed. and trans. Michael Howard and Peter Paret (Princeton: Princeton University Press, 1976), 80.

¹² For the idea that war is a cultural phenomenon more than it is political, see John Keegan, *A History of Warfare* (New York: Knopf, 1993); Victor Davis Hanson, *Carnage and Culture* (New York: Doubleday, 2001); and Martin van Creveld, *The Culture of War* (New York: Ballantine, 2008).

¹³ Russell F. Weigley, *The Age of Battles: The Quest for Decisive Warfare from Breitenfeld to Waterloo* (Bloomington: Indiana University Press, 1991), passim, but especially xi–xiii and 536–540.

¹⁴ Clausewitz, 92. Emphasis in original. Regrettably, Clausewitz gave little explanation of what such operations might be. Rather, he noted that splitting an alliance, paralyzing it, or gaining allies are possibilities, but he then implies that such activities are important merely because they make it more likely for a conclusive battle to take place. He gives no other way, for example, how to split an alliance other than by destroying a nation’s army and thus forcing it out of the war.

¹⁵ B.H. Liddell Hart, *Thoughts on War* (London: Faber & Faber, 1944), 48.

¹⁶ For Boyd’s life and theories, see Grant T. Hammond, *John Boyd and American Security* (Washington, DC: Smithsonian, 2004).

¹⁷ Michael Howard, “When Are Wars Decisive?” *Survival* 41 (Spring 1999), 132.

NOTES

¹ The estimates given for the numbers of troops participating in these ancient battles vary, but the totals listed are consistent with most sources.

² H.H. Scullard, *Scipio Africanus: Soldier and Politician* (Ithaca: Cornell University Press, 1970), chapters 6 and 7; and J.F. Lazenby, *Hannibal’s War* (Norman: University of Oklahoma Press, 1978), 215–227.

³ Don Higginbotham, *The War of American Independence* (New York: Macmillan, 1971), 352–388.

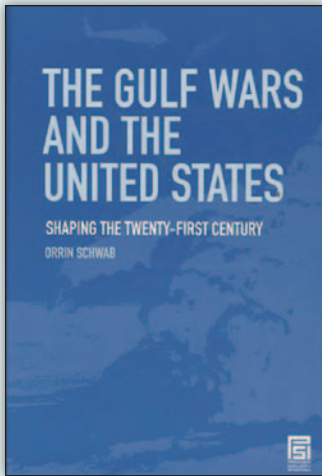
⁴ Barry Strauss, *The Battle of Salamis* (New York: Simon & Schuster, 2004), chapters 8–11.

⁵ Hans Delbrück, *Antiquity*, vol. I of *History of the Art of War Within the Framework of Political History*, trans. 4 vols. (Westport, CT: Greenwood, 1975), book I, chapters 8 and 9.

⁶ John Terraine, *A Time for Courage: The Royal Air Force in the European War, 1939–1945* (New York: Macmillan, 1985), 169–213; and Richard Overy, *The Battle* (London: Penguin, 2000).

⁷ The best account of Napoleon’s military career remains David Chandler, *The Campaigns of Napoleon: The Mind and Method of History’s Greatest Soldier* (New York: Macmillan, 1966).

⁸ For the development of the atomic bomb, see Vincent C. Jones, *Manhattan: The U.S. Army*



The Gulf Wars and the United States: Shaping the Twenty-first Century

By Orrin Schwab

Praeger Security International,
2009

180 pp. \$75

ISBN: 978-0-275-99754-0

Reviewed by

STEPHEN A. BOURQUE

A significant portion of the American population has never known a world in which the United States was not militarily involved in some way with Iraq. Many wonder how the obvious military success of Operation *Desert Storm* could digress to years of sanctions and deployments culminating in Operation *Iraqi Freedom*, the 2003 invasion ending Saddam Hussein's regime but creating a host of new problems. Misguided policy in 1991 and the coalition's failure to achieve a satisfactory political endstate wasted that superb operational victory.

The title of Orrin Schwab's book indicates that he understands this linkage and suggests that the book should provide an overarching narrative of this period. Schwab, who has written several books on the nature of civil-military relations and taught at Purdue and the University of Chicago, certainly joins these two conflicts into one story.

The first chapter, one of the book's best, lays out the relationship between this long conflict and American foreign policy. Central to Schwab's thesis is the concept of *scripts*, defined as "powerful unconscious cognitive structures that control human behavior at all levels of interaction" (p. 12). In his view, the multiplicity and complexity of these scripts have resulted in all the key actors in this conflict, to include three Presidents, talking past themselves without arriving at a regional solution. This narrative provides each participant—such as states, tribes, bureaucratic organizations, and religious groups—with its own framework for interpreting current events. The author's fundamental argument is that after defeating Saddam in 1991, the American script was flawed: "The powers of the American state and the Western liberal scientific-industrial order could not extinguish the tribal, Islamic, and anti-Western scripts of the indigenous groups that opposed them" (p. 19). In essence, three American administrations have failed in the Persian Gulf because they understood neither themselves nor the complexity of the Middle Eastern and Iraqi environment and the competing "ethnic, religious, economic, and political differences" that resulted from these varying world perspectives. As "U.S. institutions have been paragons of innovation, they have also been the epitome of bureaucratic failure" (pp. 133–134). In effect, the chaos of the last decade was almost preordained. Those who plan our foreign and military policies need to understand these narratives before they embark on military adventures in distant lands.

In general terms, Schwab's arguments are sound. The current generation of American military leaders understands the

consequences of our historic propensity for embarking on military operations without a firm understanding of the complexity of the task at hand. Much of the current curriculum at the U.S. Army Command and General Staff College's School of Advanced Military Studies focuses on the concept of design: understanding the problem, the environment, and the ways to a solution. The author's theme directly relates to what this school is teaching our planners today.

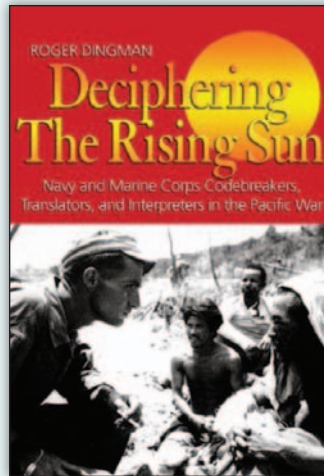
On specific issues, however, Schwab's evidence is less than convincing. His superficial discussion of Operation *Desert Storm* using dated sources, such as Michael Gordon and Bernard Trainor's *The General's War* (1995), and biased secondary sources, such as Robert Scales's *Certain Victory: The U. S. Army in the Gulf War* (1994), indicates he has not investigated this conflict too deeply. In some ways, he is depending on his own script to evaluate this conflict. He ignores the text of United Nations Security Council Resolution 660 (August 2, 1990), which demanded not only that Iraq withdraw from Kuwait but also that it "begin immediately intensive negotiations for the resolution of their differences." From the beginning, this conflict lacked the political focus required to obtain a stable regional peace. Both General Norman Schwarzkopf, commander of the American intervention, and Ambassador Chas Freeman, senior State Department representative in the region, complained to their respective leaders that they were fighting a war without clear political objectives. Rather than the U.S. administration's failure to understand scripts, it failed at the most fundamental task of war making. Ignoring Carl von Clausewitz's admonition that policy drives war, George H.W. Bush and his government never

related long-term stability to military success. At the conclusion of the conflict, there was no regional conference to ensure that the Security Council's guidance of resuming negotiations was followed. The military forces simply ended the war without consulting the coalition or imposing its will on the enemy. Essentially alone in a tent near Safwan, Schwarzkopf found himself making national policy with little guidance and a defiant Iraqi military. The results were catastrophic. Saddam would never admit defeat, no matter what Western commentators said. More important is the script that Schwab misses: the Shia uprising in March 1991 and the failure of the United States to support it, an event that would become a major part of the regional narrative and affect how the Shia responded to the American invasion in 2003.

Unfortunately, because of the details missed in his analysis of the first war, the author is unable to contribute to our understanding of what followed. Rather than a focused discussion that convinces the reader of the failure of the various players to understand each other, Schwab essentially chronicles the many events that took place between 1991 and the end of combat operations in 2003. The three main chapters that follow his discussion of *Desert Storm* regress into an encyclopedic chronology of events, with each chapter divided by 12 separate subheadings and having little serious analysis. This is unfortunate, since Schwab's message is fundamentally sound. American planners and politicians, in the years after 1991, simply ignored the complexity of the interaction between their narrative and the one developed by the Iraqi leadership, and other players, living in a demanding and difficult international neighborhood. The author needs to package his argument better.

Packaging is not solely the author's responsibility, however. A content editor should have challenged Schwab's errors of substance, such as calling Clausewitz "Eric" rather than Carl (p. 9). A knowledgeable editor also would have cautioned him about using unreliable books, such as Scales's *Certain Victory*, to define the conduct of the war and recommended more recent and balanced resources. That editor might have pointed out other areas where Schwab's content is fundamentally wrong, such as linking Army planners to the U.S. Military Academy at West Point (p. 92). A copyeditor should have helped the author present his argument in a more readable format. Book chapters do not deserve to be broken up by as many as 12 boldface subheadings disrupting the narrative's natural flow. Editors would also have caught the use of passive voice such as "the war has been viewed" and "has been attributed" that dominates much of the text and diminishes the power of the arguments (p. 77). Therefore, if readers of this journal are trying to understand the connections of the American long war with Iraq, this book will not provide the intellectual or substantial evidence they are seeking. **JFQ**

Dr. Stephen A. Bourque is a Professor of Military History in the School of Advanced Military Studies at the U.S. Army Command and General Staff College.



**Deciphering the Rising Sun:
Navy and Marine Corps
Codebreakers, Translators, and
Interpreters in the Pacific War**

By Roger Dingman
Naval Institute Press, 2009
340 pp. \$29.95
ISBN: 978-1-59114-211-9

Reviewed by
ROBERT J. HANYOK

When the United States entered World War II, it lacked nearly everything it immediately needed to fight that war effectively. Programs to build ships and planes and to train men had only recently begun to produce results; prevailing shortages would make the early Pacific battles near gambles. But one critical shortage in combat support was the lack of sufficient U.S. Navy and Marine personnel trained in the language of the Axis opponent in the Pacific—Japan.

It was not that the Services had been oblivious to the possibility of war between the United States and Japan. The Army and Navy had instituted small language training programs for future intelligence officers that included tours in Japan. While some of these naval officer-linguists would perform outstanding service during World War II—Joseph Rochefort, Edwin Layton, and Art McCollum come to mind—the

total number of those completing programs would be only a few score, hardly sufficient for the needs of any conflict.

Like much else in the American war effort in 1941, a major Japanese language training program had to be started from scratch, and it was difficult. As Dingman demonstrates in his readable *Deciphering the Rising Sun*, the Navy's program was fraught with internal issues and buffeted by external forces that hampered its productivity. That the program succeeded was due to the people who ran it, as well as those who graduated from it.

The program began in late 1941. The driving and sustaining force behind the training was a language instructor newly arrived at Berkeley, California, named Florence Walne. Mostly forgotten today, she organized the first program just before the war began in the Pacific. Her faculty was made up largely of *Nisei*, second-generation Japanese-Americans. Their presence became an issue when the relocation of Japanese-Americans started in early 1942. The military and political authorities would grant no exception for the instructors. To accommodate them, the program moved to Boulder, Colorado, at the University of Colorado.

In Colorado, Walne's problems continued: the never-ending distrust of the *Nisei* faculty, the gulf between the regular students and the military, and the interference of "regular" Navy officers who were intent on subjecting the language students to a strict military regimen. Then there was the intense course of study itself, which was enough to challenge any student.

Once in the field, the raw linguists had to confront new challenges. Those sent to intelligence assignments found themselves in the world of "spooks" and codebreakers, each with their own jargon and

conventions. Those assigned to codebreaking operations found themselves mired in translating "the blatherings [sic] of . . . Japanese diplomats" (p. 102) or confounded by the mysterious technical jargon of the Japanese navy. Those sent to the frontlines faced an ironic dilemma: the paucity of Japanese prisoners of war in the early island-hopping campaigns meant there were few human sources of intelligence. Additionally, these officers had to convince combat commanders to restrict the natural bent of Sailors and Marines to collect war "souvenirs," such as letters, notebooks, and equipment that might have intelligence value.

As the Americans advanced west and north toward Japan, these linguists were in the midst of some of the toughest campaigns—Iwo Jima, Okinawa, and the Mariana Islands. The ferocity of Japanese defenders often left American combat troops with little desire to take prisoners. The linguists sometimes found themselves trying to coax Japanese troops to surrender, but uncertain if accompanying American troops would hold their fire when the Japanese emerged from their bunkers. Once they had the prisoners, many linguists felt overwhelmed by the complexity of spoken Japanese. Unsure of their abilities, they worried about face-to-face sessions and whether they could use their conversational classroom Japanese on hardened enemy soldiers and sailors.

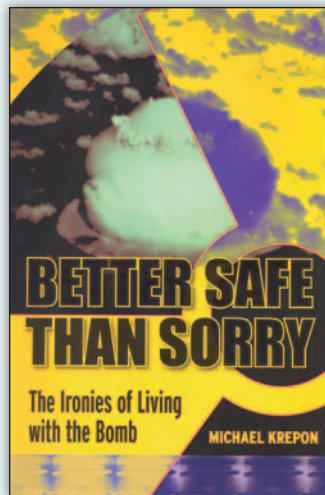
Dingman describes how a few Navy linguists got one of the hardest jobs imaginable: interrogating surviving Kamikaze pilots. The first task was simply to convince these survivors that they did not need to commit suicide to assuage their shame at failing to hit an American ship. In some cases, these linguists won the trust of the pilots and gained valuable intelligence about Kamikaze staging bases and formations.

Another area the linguists had to master was civilian relations. On Saipan and Okinawa, the Americans had to deal with substantial refugee civilian populations. Winning the trust of the civilians was critical, but organizing the camps where they had been resettled were tasks way beyond what the linguists were trained for. That they succeeded at all was due to individual initiative. Finally, after August 15, 1945, there were the numerous Japanese garrisons whose surrender these linguists had to negotiate, all the while knowing that a single slip in translation or cultural protocol could lead to bloodshed. Dingman successfully recreates these small dramas across the Pacific and China.

Dingman has woven a detailed and interesting tale from hundreds of individual stories of Navy and Marine linguists (mostly men, but a few women as well). The story he relates is rich with telling anecdotes of the numerous people who made up the program. His “bottom-up” approach makes concrete the many high-level issues they faced.

However, Dingman does leave some larger questions unanswered. For example, he refers to the presence of Army *Nisei* translators in the Pacific, often serving as noncommissioned officers. Why did the Navy not take this route as well? Also, there is little about the bureaucratic infighting among the Services and commands for the scarce number of translators. These few questions aside, Dingman has produced a valuable study about the Navy and Marine linguists and their contribution to the Pacific war. **JFQ**

Robert J. Hanyok is a retired Department of Defense historian. His latest work, co-authored with David P. Mowry, is *West Wind Clear: Cryptology and the Winds Message Controversy—A Documentary History* (National Security Agency, 2008).



Better Safe than Sorry: The Ironies of Living with the Bomb

By Michael Krepon
Stanford University Press, 2009
270 pp. \$29.95
ISBN: 978-0-8047-6063-8

Reviewed by
FRANCESCO N. MORO

Although nuclear strategy has arguably been one of the most widely treated themes in military theory and political science, Michael Krepon’s *Better Safe than Sorry: The Ironies of Living with the Bomb* is both an innovative and timely contribution to the academic and policy debate. The innovation lies not so much in the author’s espousing totally new ideas, but rather in his ability to elucidate the major issues and likely developments in a realm—nuclear weapons—that is often esoteric and perplexing for those in the policy world who are supposed to make key decisions and for the informed public who want to assess them.

Krepon begins by stressing the challenges to the system, created with much effort since the 1960s, to prevent nuclear proliferation. Besides proliferators themselves, we immediately discover the book’s culprit, the George W. Bush administration, responsible for dismantling the U.S. commitment to such a regime

and for enacting preventive policies that eventually made the world less safe. This is connected to the underlying thesis of the book: that regime—reformed to fit the needs of the new security environment—is still the best guarantee the world and its major stakeholder (the United States) have to avoid an unwanted nuclear disaster. To show that, Krepon goes back to the first nuclear age and describes its main features. His firm support for arms control does not prevent him from seeing the paradoxical aspects of nuclear strategy and the nonuse of nuclear weapons. Rather, the author argues, it was the hawks and doves combined who guaranteed the dynamic balance that made deterrence work; hardliners such as President Ronald Reagan happened to be the figures who signed the most important nuclear deals with the “evil empire.”

The second nuclear era, starting after the demise of the Soviet Union, required adaptation to new challenges. Threats to U.S. security arguably have become less vital (no arsenal comparable to the Soviet one is in sight), but they are more diverse and scattered. There is an ironic aspect that Krepon brilliantly highlights: the United States seems to consider the new threats apocalyptic because of the millenarianism and megalomania of the new potential nuclear actors (Iran’s Mahmoud Ahmadinejad, North Korea’s Kim Jong-il), whereas during the “peaceful” Cold War, much larger arsenals were in the hands of some of history’s largest mass murderers (such as Joseph Stalin). Rather, the risk that nuclear weapons will be used would be now higher because of the complex calculations in existing (such as among China, India, and Pakistan) and potential triangular relations should proliferation continue.

To prevent such an environment, there are two ideal

strategies. The first is the one followed by the Bush administration: adopting preventive action against unfriendly potential nuclear states. The second is the creation of a series of comprehensive initiatives (such as those proposed by Senators Sam Nunn and Richard Lugar in the early 1990s) aimed at securing existing arsenals, preventing the spread of fissile materials, and pursuing transparency and “best practices” in management of nuclear facilities. It is a shame, Krepon insists, that the interaction between dominators and conciliators (a post-Cold War version of hawks and doves) does not seem to have produced the good results of its predecessor, as its hijacking by dominators in the wake of 9/11 has led to catastrophic adventures such as the Iraq War, the result of which has been to strengthen the will of American adversaries.

From these premises, Krepon ranks what he believes are the nine most dangerous “negative drivers” and then builds five scenarios of likely nuclear futures. What should be feared the most is that nuclear weapons could be used in a conventional campaign: this would possibly lead to retaliation (if possible) and would break the now-strong “nuclear taboo,” a tradition of nonuse of nuclear weapons. As for nuclear futures, he looks with skepticism at a U.S. attempt to build a world in which its nuclear primacy (the scenario of “dominance”) allows the country to achieve “strategic objectives in the worst cases” (p. 172). This would have the result of maintaining high readiness in times of crisis and forcing Russia and China to keep their arsenals on alert by so doing. As Krepon states, Murphy’s law applies to nuclear weapons as well—even more so if they are ready to use in an environment in which there is more than one adversary to figure into the equation.

There are, for sure, specific issues with which one could disagree. One is Krepon's ranking of threats: Pakistan-related risks are ranked as third, nuclear terrorism against a state by extremist groups is sixth. But that is probably the good thing about rankings, too: they solicit immediate discussion based on clear premises. The second debatable issue is the scant mention the book makes about the increasing weight of a nuclear China in the Pacific region and the consequences for Japan's security. More space is given to North Korea, but it is probably time that a more systematic discussion of Japan's uneasy reconsideration of its security in a more heavily "nuclearized" area takes off. A third point is the absence of a more thorough discussion on how to frame nuclear deterrence among regional powers. Most scholars or practitioners—Krepon himself, arguably—would agree that once nuclear weapons are acquired, a careful look at the command and control and specific features of military organizations and postures of those countries is needed, together with including them in comprehensive treaties banning explosions and intensively controlling fissile materials.

As a whole, the reader should appreciate the witty prose, the ability to condense into 200 pages an intricate and eclectic bulk of notions and ideas, and the balanced support the author provides to his thesis on the importance of multilateral systems of control, rather than unilateral preventive actions, as the only "safe passage" through the second nuclear age. This book is a must read, and not just for "nuclear professionals." **JFQ**

Francesco N. Moro is a Visiting Lecturer in Strategy and International Politics at the Institute of Aeronautical Military Sciences, Italian Air Force.



War

by Sebastian Junger

Twelve, 2010

287 pp. \$26.99

ISBN: 978-0-446-55624-8

Reviewed by

JAMES P. TERRY

Sebastian Junger, author of *The Perfect Storm*, *A Death in Belmont*, and *Fire*, offers a remarkable look into the modern insurgent battlefield and the young U.S. Soldiers who are fighting there. In 2007 and 2008, Junger and photojournalist Tim Hetherington took five extended trips into Konar Province in eastern Afghanistan, where they were embedded with 2^d Platoon of Battle Company, an element of the 173^d Infantry. The setting is the Korengal Valley, a small but extraordinarily violent slit in the foothills of the Hindu Kush Mountains. Junger accurately reports the nature of the violent war, the lack of any accommodation for the law of war or common decency on the part of the insurgents, and the extreme physical rigors that troops encounter in this mountain environment.

In section one, "Fear," Junger sets the scene for his story. He describes the physical makeup of the firebases (often built from huge dumpster-like containers filled with rocks) and

outposts that the 173^d created on the mountainsides to manage the movement of insurgents through the valley and to provide protection from the constant shelling. As described by Junger, the 30 men of the 2^d Platoon could have been in any platoon in any war we have fought. Tough, confident, capable—each gains a sense of how to survive and to efficiently accomplish the daily missions of service in a stark environment in preparation for moments of chaos. This is not a war for the privileged. Young men gain equality when providing covering fire for each other and compressing one another's wounds until a medevac flight can get in. Natural leaders emerge in this setting, and Junger has an uncanny knack of making readers feel as if they know each of these men like a brother. Those killed or wounded are replaced by new and untested troops, who are designated as "cherries." Interesting and comical descriptions of older troops forcing "cherries" to fight each other to relieve firebase boredom will bring back vivid memories to many.

Section two, "Killing," is a tutorial on the operational science and tactical considerations one must carefully employ to win in this stark environment. This section examines intelligence gathering, the use of overhead assets, and the use of local informants as the Soldiers of Battle Company track a fluid and agile enemy, search for weapons caches, or interdict infiltration routes while carrying enormous loads on their backs. It was not unusual for the platoon to have contact with and engage the enemy several times each day. The issue of friendly Afghan casualties all too often seen in this war is a serious matter that requires diplomacy and compensation. The tactics used to hold the high ground, avoid exposure to enemy firing points,

deny key terrain to the enemy, close infiltration and exfiltration routes, and preclude resupply are as old as war itself, but they are done with precision by Battle Company. Through the discussion of each of the operations planned and executed, the character and strength of the American Soldier are clearly evident. Just as I found as a Marine in Vietnam, when young Americans are well trained and fight effectively to keep each other alive, the mission takes care of itself.

Section three, "Love," portrays the deep commitment that develops among Soldiers who must depend upon each other totally to survive their tour and return home. The emotional and irrational are explored as tours wind down and men realize their days could be numbered simply by the sheer number of times they have already been spared. The close relationships become bonding that will last their lifetimes. The emotional scarring takes its toll, however. The number of limbs lost, men killed, and lives forever altered makes all these men very different than when they came into the Korengal. Then there are the concerns of these men (and every person who has ever gone to war) of what going home will be like. In the Korengal, at least, every problem could be solved by getting violent faster than the other guy. And the violence does continue until the end of 2^d Platoon's deployment: on the last day, a major attack is foiled, and A-10s take out a key Taliban force.

War is the most realistic and absorbing account of combat I have ever read, even exceeding Jim Webb's *Fields of Fire* for mesmerizing readers. This is not a book for the faint of heart, and the language is just what I remember from Marines on the battlefield. The descriptions are raw, accurate, and insightful. This is the story not only of the

operations, the sweat, the slogging, the emotions, and the total heartbreak when good men are lost, but also of what a great commitment those who serve this country have made, and what a blessing it is to have men of this caliber willing to serve. **JFQ**

James P. Terry is Chairman of the Board of Veterans Appeals. He is a retired Marine colonel and holds a doctorate from The George Washington University.



Death by Moderation: The U.S. Military's Quest for Useable Weapons

by David A. Koplow
Cambridge University
Press, 2010
263 pp. \$29.99
ISBN: 978-0-521-11951-1

Reviewed by
DAVID M. OAKS

General Rupert Smith, in *The Utility of Force*, characterizes the current state of global confrontation as “conflict among the peoples.” In this environment, firepower and escalation of force—to date, the mainstays of modern Western militaries—have less relevance; today, we are engaged more in a contest to win over the will of the people.

U.S. forces have experienced this shift in the application of force in current operations. In Afghanistan, for example, airstrike tactics were modified to try to reduce the risk to civilians and secure popular support. Such a reorientation of military might denotes our efforts to regain the advantage in an environment where the enemy is setting both the terms and timing of engagements.

Koplow focuses on just this problem in *Death by Moderation*. He sets the stage by cataloging the long history of weapons designers increasing the destructive effects of their products, from ancient swords to nuclear weapons, and then pointing out how these increases conferred military advantage. The contemporary challenges of peacekeeping, counterinsurgency, and counterterrorism have driven a new interest in “useable” weapons that allow forces to “act without overreacting.” Koplow finds the source of this divergence in the historical trends of deterrence and international law.

Civilized societies, he notes, are constrained first by reasons of not employing wanton force. (Here, the author adds an interesting observation about al Qaeda terrorists “weaponizing” our moral restraint.) Second, societies are self-deterred by practicality: a desire to win wars at a lower cost to the enemy so as to avoid postwar recovery costs and to steer clear of the appearance of disproportionate use of force that might call into question the justness of one’s cause. The third reason is the self-imposed constraint to model good behavior; for example, other countries might construe the precedent of U.S. use of a low-yield nuclear weapon as a rationale for their employment of a nuclear weapon.

Koplow, a professor of law at Georgetown University, also discusses the constraints imposed on civilized societies by

the Law of Armed Conflict, the basic tenets of which hold that the use of force must be valid, undertaken as a last resort, and proportional to the threat. This last tenet of proportionality fits well with the development of useable weapons technology.

These concepts of self-deterrence and law are thoroughly explored in five case studies: precision-guided munitions (the harbingers of smaller, more useable weapons, but perhaps seductively so); low-yield nuclear weapons (even if capable, not to be used for a first strike); smart antipersonnel landmines (the ability to make them inert after a fixed period will make them more useable); antisatellite weapons (the United States has the most to gain from international restraint in their development); and nonlethal weapons (which can allow militaries to use force more quickly and effectively, but also perhaps with less restraint). Koplow devotes a chapter to each, and together they represent a thoughtful and thorough selection of supporting evidence. Of great value, too, are the detailed bibliographies that conclude each chapter.

An interesting case the author chose not to include is that of unmanned aerial systems (UAS). The use of UAS has increased considerably over the past 15 years, as has the pairing of UAS with on-board precision weapons. The quest for smaller effects (thus making weapons more useable) is playing out with UAS. For example, the Army has modified the Brilliant Anti-Tank weapon from its role as a Cold War tank killer into a precision, limited-effect munition mounted on the Hunter UAS.

Koplow notes that each of these programs has come about independent of an overarching security philosophy or Department of Defense-wide program. The 2011 National Military Strat-

egy states that “the disciplined application of force is consistent with our values and international law,” a point that is parallel to Koplow’s thesis, but similar parallels are harder to find in joint concepts and doctrine. *The Capstone Concept for Joint Operations* does describe challenges in “shaping the narrative” and warns that self-imposed restrictions on the use of lethal force by Western nations could degrade combat readiness and lead to failure in battle. Joint Publication 3.0, *Joint Operations*, discusses lethality and restraint in the chapter on “Crisis Response and Limited Contingency Operations” but relegates a discussion of restraint and legitimacy to an appendix.

As Koplow succinctly writes, “If our weapons are more deft in this way, and if they can be wielded with greater effectiveness and reduced collateral damage, we will less often be inhibited—self-deterred—in applying them. Our enemies would then believe that we can and will exercise ourselves with discretion and precision, not artificially constrained by worries about overdoing it.”

Koplow ends with two cautionary questions. If the development of more useable weapons leads to a real revolution in military affairs, will we lose too much self-deterrence; and, if others catch up to our capabilities, will that be to our advantage or detriment? These are important questions that concept and doctrine writers should continue to develop. A broader audience, one beyond the inquisitive military professional, is encouraged to add Koplow’s book to its reading list to understand better the potential gains and risks of this trend in contemporary weapons development. **JFQ**

Colonel David M. Oaks, USAR, serves part-time on the Joint Staff, J7, and is a senior consultant at the Logistics Management Institute in McLean, Virginia.

Joint Chiefs of Staff J7, Joint Education and Doctrine Division

By GEORGE E. KATSOS

In 1949, the Chairman of the Joint Chiefs of Staff (CJCS) established doctrine to inform the joint force commander and staff on how to plan and conduct joint military operations. Prior to congressionally mandated and directed actions to remove institutional barriers to jointness, there was no single individual or agency responsible for joint doctrine development. Joint doctrine lacked a single standardized process, clear differentiation from multi-Service doctrine, and consistency among joint, Service, and combined doctrine. Major shortcomings included logistics and command and control doctrinal gaps, as well as several joint doctrine issues requiring resolution (for example, impact on command and control).

By 1982, over 20 joint publications and approximately a dozen multi-Service publications focused on joint operations. That year, the Chairman initiated the Joint Doctrine Pilot Program, which directed the commanders in chief (now combatant commanders) to develop Chairman-identified joint doctrine projects. However, only one project became doctrine during the pilot project.

The Goldwater-Nichols Department of Defense (DOD) Reorganization Act of 1986 provided the statutory basis for changes in our military command structure. This law consolidated operational authority through the Chairman instead of the Service chiefs for review of major personnel, materiel, and logistics requirements of the Armed Forces. As a result, the Chairman reorganized the Joint Staff and created the Director for Operational Plans and Interoperability (J7). This new directorate developed and established doctrine for all aspects of the joint employment of the Services.

In 1987, the Chairman released Joint Chiefs of Staff Memorandum of Policy 190, which provided specific guidance on the new

joint doctrine development process. This policy established systematic procedures to develop the process through the Director for Operational Plans and Interoperability, Joint Staff/J7. The Joint Staff/J7 directorate's responsibilities included deciding content of joint publications and managing the new joint doctrine development process. Furthermore, the Joint Staff/J7 would manage the process and monitor all milestones through a standardized timeline for publication development.

One of the first actions of the Joint Staff/J7 was an initiative known as the Joint Doctrine Master Plan. These new procedures for a joint doctrine development system set in motion a 3-year development cycle. In February 1988, the master plan materialized through a series of DOD meetings and conferences addressing every aspect of the joint doctrine development process. In April of the same year, the approved plan's process became Joint Publication (JP) 1-01, *The Joint Publication System: Joint Doctrine and Joint Tactics, Techniques and Procedures Development Program*, and outlined a new publication hierarchy, terms of reference, and development process fundamentally still used today.

Under JP 1-01, existing joint publications were assigned new numbers, with J7 establishing review cycles. All new publications were placed into the test publication cycle and had a 35- to 43-month timeline. In 1989, Change 1 to JP 1-01 included a revision timetable from 3 to 5 years. By 1991, 22 publications had entered the test publication timeline. As a result of new publications flooding the doctrine development community, the Chairman removed the prerequisite that all new publications go through the existing process and instituted instead that publications undergo the evaluation as a test publication only when significant differences of opinion existed. This dropped the number of joint test publications (JTPs) to zero. Regardless of the decrease in test publications, the number of joint publications still reached 112 in 1993.

Over the next decade, the normal publication timeline continued to be streamlined. Concerns emerged, however, that the doctrine development process was too slow and not responsive enough to rapid changes. The JP cycle stood at 21 months, while JTPs were reduced to 27 to 33 months. The number of publications increased to well over 100. In 2000, JP 1-01 was renamed the Joint Doctrine Development System. In 2004, JP 1-01 became a Chairman's instruction (CJCSI 5120.02), which shortened the JTP process to 20 to 26 months. Three years later, the amended instruction shortened the JP process to the existing timeline of 17.5 months, and the amount of publications was eventually reduced from 115 to 78 in 2010.

As of February 2011, there are 82 joint doctrine publications (33 publications written by the combatant commands, 28 by the Services, and 21 by the Joint Staff). This number includes two JTPs: JTP 3-12, "Cyberspace Operations," currently under evaluation, and JTP 3-70, "Total Force Fitness."

Still open to changes, all ideas and amendments are provided periodically through the Joint Doctrine Development Community. As a result, we can acknowledge from the dust of processes past that the Joint Doctrine Master Plan survived first contact, continues to work, and will be further validated through existing authoritative documents. **JFQ**

For access to joint publications, go to the Joint Doctrine, Education, and Training Electronic Information System Web portal at <https://jdeis.js.mil> (.mil users only). For those without access to .mil accounts, go to the Joint Electronic Library Web portal at <http://www.dtic.mil/doctrine>.

George E. Katsos is a Joint Doctrine Planner in the Joint Chiefs of Staff J7, Joint Education and Doctrine Division.

JPs Under Revision

- JP 1, *Doctrine for the Armed Forces of the United States*
- JP 1-0, *Personnel Support to Joint Operations*
- JP 1-04, *Legal Support to Military Operations*
- JP 1-06, *Financial Management Support in Joint Operations*
- JP 2-01, *Joint and National Intelligence Support to Military Operations*
- JP 2-01.2, *Counterintelligence and Human Intelligence Support in Joint Operations*
- JP 2-03, *Geospatial Intelligence Support to Joint Operations*
- JP 3-0, *Joint Operations*
- JP 3-00.1, *Strategic Communication*
- JP 3-01, *Countering Air and Missile Threats*
- JP 3-03, *Joint Interdiction*
- JP 3-05, *Joint Special Operations*
- JP 3-07, *Stability Operations*
- JP 3-07.3, *Peace Operations*
- JP 3-07.4, *Joint Counterdrug Operations*
- JP 3-08, *Interorganizational Coordination during Joint Operations*
- JP 3-13, *Information Operations*
- JP 3-13.1, *Electronic Warfare*
- JP 3-13.3, *Operations Security*
- JP 3-13.4, *Military Deception*
- JP 3-15, *Barriers, Obstacles, and Mine Warfare for Joint Operations*
- JP 3-15.1, *Counter-Improvised Explosive Device Operations*
- JP 3-16, *Multinational Operations*
- JP 3-32, *Command and Control for Joint Maritime Operations*
- JP 3-33, *Joint Task Force Headquarters*
- JP 3-34, *Joint Engineer Operations*
- JP 3-35, *Deployment and Redeployment Operations*
- JP 3-41, *Chemical, Biological, Radiological, Nuclear, and High-Yield Explosives Consequence Management*
- JP 3-50, *Personnel Recovery*
- JP 3-60, *Joint Targeting*
- JP 4-01, *The Defense Transportation System*
- JP 4-01.2, *Sealift Support to Joint Operations*
- JP 4-01.5, *Joint Tactics, Techniques, and Procedures for Transportation Terminal Operations*
- JP 4-01.6, *Joint Logistics Over-the-Shore*
- JP 4-02, *Health Service Support*
- JP 4-06, *Mortuary Affairs in Joint Operations*
- JP 4-08, *Logistics in Support of Multinational Operations*
- JP 5-0, *Joint Operation Planning*
- JP 6-01, *Joint Electromagnetic Spectrum Operations*

JPs Revised (within last 6 months)

- JP 3-02.1, *Amphibious Embarkation and Debarkation*
- JP 3-07.2, *Antiterrorism*
- JP 3-09, *Joint Fire Support*
- JP 3-22, *Foreign Internal Defense*
- JP 3-61, *Public Affairs*
- JP 3-68, *Noncombatant Evacuation Operations*
- JP 4-03, *Joint Bulk Petroleum and Water Doctrine*

Defining Asymmetric Warfare

A Losing Proposition

By JESSE G. CHACE

If this work seems so threatening, this is because it isn't simply eccentric or strange, but competent, rigorously argued, and carrying conviction.

—Jacques Derrida

There is a new generation whose voices are only beginning to pierce the thick granite walls of the conventional, institutional, and academic military fortress—walls wherein the lingering residue of Cold War-era philosophy continues to tarnish even the freshest concepts and ideas. Author Jack Kerouac coined the term *Beat Generation* in 1948 to describe a group of American writers who prompted a cultural phenomenon through a rejection of mainstream values.¹ While controversial, this subculture's return to an appreciation of idiosyncrasy as opposed to state regimentation went on to effect immense change in the subjects of ecology, environmental preservation, social and cultural understanding, human rights, medicine, and the arts.

While achieving tactical success through imaginative and courageous acts of nonconformity and spontaneous creativity on the battlefield, characteristics reminiscent of the Beat Generation, this new Blink Generation, inspired by Malcolm Gladwell's *Blink: The Power of Thinking without Thinking*, has struggled to influence strategic decisions.² Why? Despite the best efforts of a handful of senior leaders, military culture, unlike popular culture, remains nonconducive to free thought and expression, forcing many talented, intelligent, and imaginative junior noncommissioned officers and officers out of military service before their voices and ideas can be effective on a strategic level. Those who remain often find a home in the special operations community, from which few ever return to change the culture of an operational force entrenched in a long, deep history of regimentation and inflexibility.

Forefathers of the Blink Generation existed in special operations long before Gladwell popularized the notion of combining rational analysis with instinctive judgment. Although the special operations communities have dealt aptly with asymmetric warfare since their inceptions, thriving in perpetual states of chaotic and ambiguous situations, they never aspired to define the term. Within the past 10 years, however, as adversaries and missions traditionally reserved for special operations have crept into the forefront of conventional military engagements, there have been countless efforts on the conventional, institutional, and academic side to provide a definition.³ While it is easy to understand a desire to

Major Jesse G. Chace, USA, is a Military Intelligence Officer in the Army's Asymmetric Warfare Group, a Field Operating Agency under the Army Deputy Chief of Staff for Operations, Plans, and Training.

define *asymmetric warfare*, there is a growing minority who disagree not only with elements of proposed definitions, but also the fundamental theory behind defining this/the term; to *define* the term *defies* its very meaning, purpose, and significance.

The Challenge

Subjective and ambiguous terms are part of any language (compare Plato's *Gorgias*). Some, such as French philosopher Jacques Derrida, argued that language itself is "built" upon ambiguity—the *lack of* true or foundational *meaning* is *what gives language its meaning*. A few such terms include *art, justice, beauty, brilliance, and asymmetric warfare*. Arthur Schopenhauer believed that great art is the product of an immediate insight in which a (wo)man of genius grasps the true nature of things without the long process of rational analysis upon which scientific knowledge depends.⁴ While referring to *creation*, it does not take a genius to recognize that certain ideas are better *understood* using immediate insight over well-calculated explication, particularly those concepts whose boundless scopes meet restriction only at the far reaches of imagination.

implying that technology plays a critical if not obligatory role in asymmetric warfare contradicts the outcomes of most conflicts in the last 40 years

Defined in its literal state as simply "an imbalance," the nature of *asymmetry* is infinite in infinite directions and planes, uncontainable in any way. Thus, with usage of the catchphrase *asymmetric warfare*—as exploited and clichéd as it has become—coupled with its lack of established definition, policy writers are faced with three options:

- risk dissonance with fundamental philosophies of individual insight and the true nature of asymmetry in order to define the term
- abandon all effort of creating inadequate definitions in favor of an artistic reliance on instinct and understanding to limit clichéd interpretation
- ignore the term completely and ban it from our lexicon.

While an inherent tension exists between doctrine and the *nature* of asym-

metric warfare, doctrine has the potential not only to acknowledge, but also to provide an operational philosophy and understanding of the term.⁵ But that may require an unconventional approach.

Why Existing Definitions Are Wrong

What Pentagon officials and researchers identify as "unrestrained use of an impressive sounding, melodic phrase to describe any number of concepts or ideas" has incited various campaigns to eliminate the confusion generated by the lack of a definition for asymmetric warfare.⁶ While the term first appeared in policy statements in 1997 and has shown up in various National Security Strategies and doctrinal definitions ever since, doctrine has yet to define it.⁷ Assertions proclaiming the term as so new to our lexicon that its ambiguity is not conducive to clear discussion, analysis, or operational use as a warfighting concept have prompted arguments as to whether the term should be banned from use in military doctrine and discussion.⁸ Often inappropriately interchanged with "irregular warfare," asymmetric warfare has a diluted meaning in joint doctrine, fueling a perceived need for a formal and unique definition.⁹

In an effort to propose an official definition for joint publication, one Pentagon office has recently framed the following:

*asymmetric warfare (n)—A war fighting methodology that exploits vulnerabilities of organization, function, culture, technology, behavior, situation, or location by employing innovative tactics and technologies to achieve surprise and neutralize or stymie an opponent's military capabilities and technological strengths. In contemporary practice, asymmetric warfare is often used to achieve an information campaign objective of strategic impact.*¹⁰

This definition combines several of the most sensible points of preceding definitions, making it a logical representation of past attempts and arguably the best definition of the term to date. The authors justify the notion that asymmetric warfare is not a new form or category of war in the manner of

irregular warfare and major combat operations—terms defined in joint doctrine—but a warfighting methodology employed throughout the full spectrum of conflict.¹¹ However, this effort reinforces several fallacies.

1. In attempting to make the phrasing all-encompassing, listing all potential vulnerability areas that asymmetric warfare can affect immediately gives the reader tunnel vision, stymieing any potential for imagination and open-mindedness. Similar attempts to stifle independent judgment and free thought have become commonplace in military doctrine and rules of engagement, causing hesitation and costing lives. Michel Foucault draws parallels to the Army's overdoctrinalization of concepts and the power of the Blink Generation to overcome this vulnerability. He asserts that "those in power assume the self-appointed task of upholding reason for and revealing truth to those who they think are unable to see for themselves and who are not allowed to speak for themselves. Argument and reason can and have been used to silence and control others, and an unyielding insistence on rational discourse can silence or diminish those who think differently."¹²

2. Use of the word *innovative* replaces ambiguity with ambiguity and fails to clarify the term. An innovation—whether material or nonmaterial—that is considered brilliant by one may be seen as outrageous and useless by others. Consider the recent introduction of the Mine Resistant Ambush Protected (MRAP) class of vehicles, which received widespread acclaim in the press as a primary tool for executing asymmetric warfare.¹³ While it is innovative, many question which side the MRAP has actually aided in combat, confirming that innovation does not always equate to adaptation on the battlefield and making its inclusion in an official definition questionable at best.¹⁴

3. Implying that technology plays a critical if not obligatory role in asymmetric warfare contradicts the outcomes of most conflicts in the last 40 years, where rudimentary methods coupled with tactical patience have proven to overcome many technologically advanced systems.¹⁵

4. Despite an admission that asymmetric warfare can also be an effective means for the military superpower to (re)capitalize on its technological advantages in an offensive mode, the definition suggests decisive victory through asymmetric warfare succumbs to its

defensive utilization. On the contrary, specific recent and historical events prove asymmetric warfare can produce decisive tactical and strategic victories through both lethal and nonlethal offensive means. The Mongol army, for instance, used such methodologies to defeat a host of larger opponent armies in the 13th century. The American Revolution was an exhibition of asymmetric warfare—not simply through the success of skirmish tactics and guerrilla warfare, but in the colonists' precise and creative use of propaganda, partisan civilians, sea warfare, and terrain to target specific vulnerabilities and defeat a superior British army.¹⁶ In 2008, Russia's nonlethal assault on the Georgian Internet proved paramount in a swift strategic victory, demonstrating that a superior force can offensively utilize asymmetric warfare to achieve victory.¹⁷

Because our enemies' use of asymmetric warfare seemingly increased after 1990 as the United States evolved into the only remaining superpower, it has become strictly associated with state and nonstate terrorist organizations that are no match for the U.S. military in a force-on-force engagement, spawning the misconception that the ultimate goal of any protagonist using asymmetric warfare is to convince his opponent—through confusion, loss of confidence, or a stymied ability to act—that victory is unattainable or too costly to pursue.¹⁸ While insurgents' reliance on improvised explosive devices in Iraq typified this theory, the ability to achieve a decisive battlefield victory through asymmetric warfare is certainly possible, even in conflicts between similar (symmetric) forces where creative use of intangible attributes such as will, patience, method, and morale plays a critical role in offsetting symmetry.¹⁹ Examples include military use of children, noncombatants as human shields, use of sexual slaves for spreading disease, information operations, and rapid development and employment of previously unfathomed technologies like nuclear weapons in World War II (for the United States and Japan).

The instantaneous global reach of modern communications technologies that enable a tactical event to produce a disproportionate strategic effect has led to the idea that asymmetry in war did not evolve into asymmetric warfare until the latter half of the 20th century.²⁰ Because strategy follows time and culture, the mere possibility of enterprise does not necessarily elevate asymmetry to a more holistic approach to warfare than history has

shown. The idea that modern communications is the first and only mechanism enabling tactical outcomes to reach a noncombatant audience is a desperate and ethnocentric attempt to classify asymmetric warfare as a modern, revolutionary event rather than one stage in a continuing evolution of such. In reality, the idea is no more modern than the printing press, telegraphy, or harnessing the electromagnetic spectrum were as each was first introduced into warfare.

for years, our military has been sitting at an empty chess table while our enemies play poker with our shadows

No doubt modern communications technologies such as satellite television and the Internet have enabled warfare in all corners of the Earth to instantaneously and strategically affect global diplomacy, politics, and economics, and are one of only several monumental stepping stones in the history of warfare, but revolutionary mechanisms throughout history have enabled intervillage, intertribe, intercity-state, and transcontinental communication to influence warfare in ways just as revolutionary as modern communications when compared to the technology and strategic scope of their eras. However, these once progressive catalysts are now as archaic as our current methods may one day seem to our descendants.

All asymmetric stratagems share a common thread that binds them throughout the ages while permitting the realities of the modern world to shape and weave them in progressive directions with increasingly widespread strategic results. Definitions such as that above identify *surprise* as that linchpin, a basis founded upon the idea that although the impact of surprise and subsequent denial of capabilities may only be temporary, it is enough to springboard a strategic information campaign.²¹

While surprise may be a critical principle of war and the linchpin of many conventional combat operations (ambush, air assault, raid), asymmetric warfare is far from conventional. Surprise in asymmetric warfare is merely a byproduct of innovative, adaptive, and predictive action rendered through creative intelligence. Such attributes are synonymous with traits more commonly identified in our enemies: cunning, creativity, and deceit.

For this reason, coupled with its ability to be shaped by lessons from the past and modern scientific and technological advances alike, it is *imagination*, not *surprise*, that is the linchpin of an asymmetric stratagem. Schopenhauer identified this notion in 1818 when he wrote, "Thus, imagination extends the mental horizon of the genius beyond the objects that actually present themselves to his person, as regards both quality and quantity."²² Asymmetric warfare embodies this unknown. Without rapidly and holistically fusing intelligence, history, and cultural understanding with imagination, we will never surpass the imaginative capacity of our enemies and achieve surprise. Failure to make this connection speaks volumes to the very reason U.S. forces have often failed to anticipate and rapidly adapt to a clever enemy.

For years, our military has been sitting at an empty chess table while our enemies play poker with our shadows. The difference? Their ability to bluff and, more importantly, to "cheat." Asymmetric warfare is not a chess match; it is a poker game.²³

Argument Against Future Definition

Staff officers and commanders who work under the umbrella of Headquarters Department of the Army quickly recognize and appreciate the importance of the phrase *words mean something*, for when it comes to mission statements and mission-essential tasks amid budgetary struggles, words truly do *mean something*. However, a rudimentary understanding of linguistic anthropology reveals that words actually do much more than "mean something"; the language we use to internalize and define sensory perceptions shapes the entire world we live in.²⁴ The word *asymmetric* itself produces a strong, unique response in our language that simply does not translate well—literally, notionally, and perhaps emotionally—into other languages and cultures.

The U.S. military's heavy reliance on definitions and acronyms harkens to the principles of early cognitive anthropology, which asserted that people classify by checking off a mental list of essential features. For example, apple = red + round + no stem. Today, cognitive experts argue that people conceptualize by reference to general mental prototypes called schema. Psychologist George Mandler describes schema in the following manner:

The schema that is developed as a result of prior experiences with a particular kind

*of event is not a carbon copy of that event; schemas are abstract representations of environmental regularities. We comprehend events in terms of the schemas they activate. Schemas are also processing mechanisms; they are active in selecting evidence, parsing the data provided by our environment, and providing appropriate general or specific hypothesis. Most, if not all, of the activation processes occur automatically and without awareness on the part of the perceiver-comprehender.*²⁵

This theory, commonly referred to as Connectionism, suggests knowledge is linked, networked, and distributed by “processing units” (schema) that work like neurons through which humans access and analyze information. Because schema are connected and work simultaneously rather than in sequence, humans can process information faster than any computer.²⁶

Because our judgment defines the word *asymmetric* at its very utterance, the phrase *asymmetric warfare* instantaneously arouses a particular meaning in our consciousness through various subconscious steps, a meaning that may not be accurately regenerated, let alone taught or explained, through an alternate list of traits. In fact, widely accepted theories such as Connectionism suggest that the habitual act of sequential trait analysis commonplace among many military definitions and processes runs counter to our instinctive nature. Thus, any stance against defining asymmetric warfare stems not from a naïve lack of understanding of doctrinal language, but a deeper appreciation for the power that a single word can generate within our consciousness. Efforts to break down such abstract terms and confine them to a definition by applying alternate language can cause devastatingly diminished effects.

Blink introduces readers to the notion of combining rational analysis with instinctive judgment, and how our subconscious can instantaneously fish through mountains of data, enabling us to make critical decisions in the blink of an eye. Recognizing asymmetric warfare is not something one has to ponder upon exposure. The most inexperienced Soldiers, Sailors, Marines, or Airmen instantly know it, regardless of their ability to think outside the box. In this way, as previously suggested, asymmetric warfare may be likened to art, music, and, oddly, pornography: hard to define, but certainly recognized when seen. Using an early cogni-

tive anthropological approach/explanation, a child, upon seeing an apple, will systematically go through a list of essential features (it is red, round, and has no stem—therefore, it is an apple) in order to identify the object as such. Instead, what Mandler points out in his description of schema is that a child will identify an object that is *green*, round, and has no stem as an apple because of its “apple-ness,” rather than because it matches an exact list of traits.²⁷ This is how we recognize pornography—not because what is seen matches an exact list of traits, but because of its “pornographic-ness” as dictated by abstract representations of prior experiences. There is no universal list of traits and therefore no clear-cut definition. In fact, the case *Miller vs. California* prompted the U.S. Supreme Court to establish a “basic legal standard” of pornography in 1973, taking careful precaution not to label it a definition.²⁸

asymmetric warfare may be likened to art, music, and, oddly, pornography: hard to define, but certainly recognized when seen

Although the process of recognizing asymmetry is instinctive, the ability to *apply* asymmetric warfare and *adapt* to an enemy’s application requires a level of intangible skills not inherent to most individuals.

The Army’s recent Outcomes-based Training and Education (OBTE) philosophy demonstrates the importance of combining rational analysis and understanding with instinctive judgment and other intangible attributes, and how that can be applied to a myriad of fundamental military tasks to achieve a mastery of expected skills.²⁹ The result is adaptive problem-solvers who are more lethal, agile, versatile, proactive, and confident in combat. Generated from the special operations community, OBTE contrasts the conventional military’s long history of promoting habitual memorization of information in a manner unconnected to related tasks.

In *Blink*, Gladwell describes the U.S. Joint Forces Command pre-9/11 wargaming scenario in which retired Lieutenant General Paul Van Riper played the part of the Enemy Forces (Red Team) commander. The scenario pitted a multinational force against a rogue

military commander (Van Riper) who had broken away from his government and was threatening to engulf an entire region in war. Friendly Forces (Blue Team) commanders were afforded various revolutionary planning tools, common operating systems, and information from every department of the U.S. Government. Although described as the most comprehensive and rigorous infrastructure ever designed to know and affect the adversary’s total environment, Red Team achieved a decisive victory before Blue Team ever fired a shot. Van Riper told Gladwell:

*They had all these acronyms. The elements of national power were diplomatic, informational, military and economic [DIME]. That gives you DIME. They would always talk about the Blue DIME. Then there was the political, military, economic, social, infrastructure, and information instruments, PMESI. So they’d have these terrible conversations where it would be our DIME versus their PMESI. I wanted to gag. What are you talking about? You get caught up in forms, matrixes, in computer programs, and it just draws you in. They were so focused on the mechanics and the process that they never looked at the problem holistically. In the act of tearing something apart, you lose its meaning.*³⁰

Van Riper’s comments echo elements of highly respected linguistic and philosophical theories while emphasizing the danger of dissecting and restricting the meaning of asymmetric warfare. Jacques Derrida is credited with conceiving the highly unconventional notion of deconstruction, which pursues the “meaning” of a text to the point of exposing the contradictions and internal oppositions upon which it is founded, revealing those foundations as complex, unstable, or impossible. He writes, “Deconstructive analysis deprives the present of its prestige and exposes it to something *tout autre* (wholly other), beyond what is foreseeable from the present, beyond the horizon of the ‘same.’”³¹ Deconstruction is not a dismantling of the structure of a text, but a demonstration that it has already dismantled itself—that its solid ground is no rock, but thin air.³² It aims to open and loosen interpretation, not to wax over at the thought of unchanging essences or ageless traditions, but rather to advocate an “inventionalistic” outlook; to constantly remain on the lookout for something unforeseeable and new.³³

Proponents of a definition maintain, “Previously voiced arguments against a definition . . . have led to unrestrained use of an impressive sounding, melodic phrase to describe any number of concepts or ideas. Clarity is needed to eliminate the confusion generated by lack of a standard term of reference.”³⁴ This process will take years of grooming as the intangible traits promoted through OBTE spread throughout the force, enabling the personalities who fail to see past a term to move beyond their discomfort with abstract regularities.

Authors of a recent Pentagon paper state, “With a clear definition the intellectual process can begin to logically and methodically incorporate asymmetric warfare into modern war fighting concepts, doctrine, and operational use.”³⁵ Consider the possibility that a “clear definition” not only impedes, but also terminates the intellectual process and that “logically and methodically” incorporating asymmetric warfare is a dangerous oxymoron. Analysts are encouraged to “think like the enemy” in order to predict the next enemy move. Although they study our manuals and periodicals, the enemy does not use definitions or acronyms; they use imagination driven by intelligence, understanding, instinct, and deceit. To “define” asymmetric warfare sends the wrong symbolism to an enemy that feeds off symbolism and an innate ability to exploit weakness in culture and character. Doing so would mean we have already lost.

Proposing a Common Understanding

While well intentioned, the reasons supporting a definition of asymmetric warfare apply a *symmetric* solution to, literally, an asymmetric problem. Without a pure definition, would use of the term run rampant, as many suggest? Maybe. But is there harm in that, or just discomfort?

In his foreword to Stephen Blank’s 2001 article, “Rethinking Asymmetric Threats,” Douglas Lovelace, director of the Strategic Studies Institute, writes, “A correct assessment of the nature of the threat environment is essential to any sound defense doctrine for the U.S. Army and the military as a whole.”³⁶ A basic militaristic understanding of asymmetric warfare would indeed lessen confusion and promote flexible doctrine—but not, as illustrated by *Miller vs. California*, a definition.

Recognizing that definitions and acronyms can sometimes only narrow scope, not open it, we must understand the laws of lin-

guistic relativity and cognitive anthropology. Therefore, any basic understanding of asymmetric warfare must find harmony between explaining what is already known through instinctive judgment, or “feeling,” and tearing down the phrase so much that its meaning is lost. Asymmetric warfare, therefore, can be understood through three basic tenets:

- a warfighting methodology that can be applied throughout the full spectrum of operations, aspects of national power, or actions by hostile actors
- no rules; it is constrained only by the imagination
- targets any real or perceived vulnerability in an adversary’s holistic environment in order to gain an advantage.

Asymmetric warfare is not a new form or category of war, but a methodology applicable throughout full-spectrum operations and one of many options available to a commander charged with planning and executing a campaign. Its philosophy is also mirrored in the political, economic, and scientific communities, which often directly and indirectly affect defense strategy and combat operations.

the enemy does not use definitions or acronyms; they use imagination driven by intelligence, understanding, instinct, and deceit

A 1998 National Defense University study defined asymmetric warfare as “a version of not ‘fighting fair,’” a notion that carries a large ethnocentric burden avoided by the second tenet.³⁷ Regardless of belief systems or behavior, asymmetric warfare is constrained only by the imagination and, consequently, falls outside the realm of any rules of war (for example, The Hague or Geneva Conventions) or society. This does not mean that the U.S. military’s use of asymmetric warfare falls outside the laws of war that we and many others throughout the world subscribe to, but merely that the tactics and strategies of others may *not*, as evidenced by countless vignettes from Iraq, Afghanistan, Somalia, the Philippines, and beyond. The absence of rules inherent in asymmetric warfare can also apply to cultural taboos. For instance, a pious Muslim male may be permitted to stray from

very strict religious and cultural practices in the name of jihad. Shaving his beard, failing to preach, and even undergoing plastic surgery are just a few examples.

Asymmetric warfare targets any real or perceived vulnerability in order to gain an advantage, often ideally done without an adversary’s awareness. Dr. Blank writes, “The idea of avoiding enemy strengths while probing for their weaknesses and maximizing our own advantages is hardly revolutionary,” an idea that Stephen Metz acknowledges as a “core logic” of all competitive endeavors, downplaying the need for a specified asymmetric branding of threat-based warfare.³⁸ Asymmetric warfare is surgical in its focus on enemy vulnerabilities; it exists where the sole purpose of any action is to create and exploit a real or perceived weakness. While it goes without saying that any adversary prefers to avoid enemy strengths while probing for weaknesses and maximizing advantages, no other brand of warfare targets vulnerabilities with such precision, focus, and purpose.

Rather than oppose doctrine, this argument reveals that previous efforts to provide a doctrinal definition of asymmetric warfare have failed not only to respect the nature of asymmetry and independent rational cognizance, but also to adhere to several principles doctrine must provide. Doctrine must facilitate flexibility, not promote intransigence. Doctrine must embrace a philosophy of initiative and creative thinking to deal with an adaptive, cunning, and typically asymmetric enemy, not create tunnel vision. Doctrine must recognize the elements of uncertainty and the unexpected, not fight them. Doctrine cannot predict the nature and form of asymmetric conflicts and enemies, but it can forecast the necessary traits and body of conceptual knowledge necessary to cope with and understand a chaotic asymmetric warfare environment.³⁹ *Doctrine* has become synonymous with *definition* and often serves as a glossary for *what to think* rather than a philosophy for *how to think*, resulting in closed-minded approaches to abstract and complex situations. The education process that addresses the true problem and will eventually alter this mentality begins with OBTE and the grooming of the intangible attributes that will propagate among the Blink Generation and ultimately change the culture of the military.

To those who believe that a definition impedes not only our intellectual process but also our ability to adapt at the same level of

our enemies, any attempt to force the concept of asymmetric warfare into a cookie-cutter template regimentally inserted into a catalogue of associated situations only reinforces a weak and unsound approach to combating the overarching methodology of rogue state and non-state terrorists, providing our enemies with the symbolism and reaffirmation that the U.S. military is as inflexible, nonadaptive, and incapable of independent thought as ever before. The three tenets identified in this article illustrate the schema that enable instantaneous recognition of asymmetry, or “asymmetric-ness” in warfare—something we do intrinsically and without the need of a definition.

Asymmetric warfare can be violent or nonviolent, material or psychological, technological or primitive, criminal or judicial. It is “black” warfare—unknown and limitless—and will continue to transform. To ensure relevance, we must do likewise. The Armed Forces need fewer chess players and more poker players. **JFQ**

NOTES

¹ John Clellon Holmes, “This is the Beat Generation,” *New York Times Magazine*, November 16, 1952.

² Malcolm Gladwell, *Blink: The Power of Thinking without Thinking* (New York: Little, Brown, 2005).

³ See “Defining Asymmetric Warfare: A White Paper,” annex A, “Definitions of Asymmetric Warfare,” Army Asymmetric Warfare Office (AAWO) Plans Division, February 20, 2009, 37.

⁴ Arthur Schopenhauer, *The World as Will and Representation*, vol. 2, trans. E.F.J. Payne (New York: Dover, 1966).

⁵ Clinton J. Ancker III and Michael D. Burke, “Doctrine for Asymmetric Warfare,” *Military Review* (July–August 2003), 18.

⁶ “Defining Asymmetric Warfare,” 28.

⁷ There is no entry for *asymmetric warfare* in Joint Publication (JP) 1–02, *Department of Defense Dictionary of Military and Associated Terms* (Washington, DC: The Joint Staff, November 8, 2010).

⁸ Steven Lambakis, James Kiras, and Kristin Kolet, “Understanding ‘Asymmetric’ Threats to the United States,” *Comparative Strategy* 21, no. 4 (October 2002), 241–277.

⁹ DOD Joint Operating Concept (JOC), *Irregular Warfare* (IW), Version 1.0, September 11, 2007, 5–6.

¹⁰ “Defining Asymmetric Warfare,” 3–4.

¹¹ *Ibid.*

¹² Terry Barrett, *Criticizing Art: Understanding the Contemporary* (New York: McGraw Hill, 2000), 59.

¹³ Jason Verdugo, “MRAP’s Growth, Maturation and Transformation into the M-ATV,” Institute for Defense and Government Advancement, September 8, 2009.

¹⁴ The MRAP was first used by the South African military and designed to survive underbelly attacks from mines, improvised explosive devices (IEDs), and other explosive hazards. While statistics favor its improvement in soldier survivability in the event of an IED attack, many believe that the MRAP has actually aided the enemy, particularly in urban environments where soldier mobility, situational/navigational awareness, combat readiness (that is, ability to quickly react with lethal or nonlethal means), and stealth are drastically reduced by the vehicle. Anonymous sources argue that these factors may have contributed to as many, if not more, casualties than the effects of increased armor against an already depleting IED threat. Due to the ability of the enemy to rapidly change tactics, techniques, and procedures and to adapt to expensive and time-consuming technological developments, many believe that the MRAP was much less “innovative” or “progressive” in its current operating environment than advertised, and that resources would have been much better spent toward alternate solutions to the IED problem in Iraq.

¹⁵ Examples include the downing of two UH–60 helicopters in Mogadishu in 1993, bombing of USS *Cole* in 2000, use of command wire and victim-actuated IEDs to overcome electronic countermeasures in Iraq and Afghanistan, and employment of improvised rocket-assisted mortars in Iraq.

¹⁶ Timothy May, *The Mongol Art of War* (Yardley, PA: Westholme Publishing, 2007); Jeremy Black, *War for America: The Fight for Independence, 1775–1783* (London: Sutton Publishing, 2001); Arthur Bernon Tourtellot, “Harold Murdock’s ‘The Nineteenth of April 1775,’” *American Heritage Magazine* 10, no. 5 (August 1959).

¹⁷ Brian Krebs, “Georgian Web Sites under Attack,” August 10, 2008, available at <http://voices.washingtonpost.com/securityfix/2008/08/georgian_web_sites_under_attac.html>.

¹⁸ “Defining Asymmetric Warfare,” 6.

¹⁹ Steven Metz and Douglas V. Johnson II, *Asymmetry and U.S. Military Strategy: Definition, Background, and Strategic Concepts* (Carlisle Barracks, PA: Strategic Studies Institute, U.S. Army War College, 2001), 6–12.

²⁰ “Defining Asymmetric Warfare,” 3–4.

²¹ *Ibid.*

²² Schopenhauer, 166.

²³ Russell Howard, “Winning the Campaign against Terrorism—Howard’s Alternatives,” briefing to the Asymmetric Warfare Group, October, 19, 2009.

²⁴ R. Jon McGee and Richard L. Warms, *Anthropological Theory: An Introductory History* (New York: McGraw Hill, 2000), 369–372.

²⁵ *Ibid.*

²⁶ *Ibid.*

²⁷ *Ibid.*

²⁸ *Marvin Miller v. State of California*, 413 U.S. 15, 93 S. Ct. 2607, 37 L. Ed. 2d 419 (1973).

²⁹ Asymmetric Warfare Group, “Outcome-Based Training and Education (OBTE) Integration Workshop—Final Report,” The Johns Hopkins University Applied Physics Laboratory, May 2009, 1–6.

³⁰ Gladwell, 102–111, 124–125.

³¹ John D. Caputo, *Deconstruction in a Nutshell: A Conversation with Jacques Derrida* (New York: Fordham University Press, 1997), 42.

³² Briankle G. Chang, *Deconstructing Communication* (Minneapolis: University of Minnesota Press, 1996), 119.

³³ Caputo, 42.

³⁴ “Defining Asymmetric Warfare,” 28.

³⁵ *Ibid.*

³⁶ See Douglas Lovelace, Jr., foreword to *Rethinking Asymmetric Threats*, by Stephen Blank (Carlisle Barracks, PA: Strategic Studies Institute, Army War College, September 2003), iii.

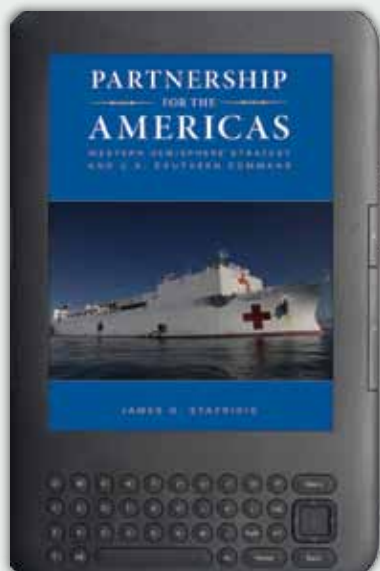
³⁷ Stephen Blank, *Rethinking Asymmetric Threats* (Carlisle Barracks, PA: Strategic Studies Institute, Army War College, September 2003), 16.

³⁸ *Ibid.*, 4.

³⁹ Ancker and Burke, 19–24.

NEW from *NDU Press*

Now available in e-book format!



Partnership for the Americas: Western Hemisphere Strategy and U.S. Southern Command

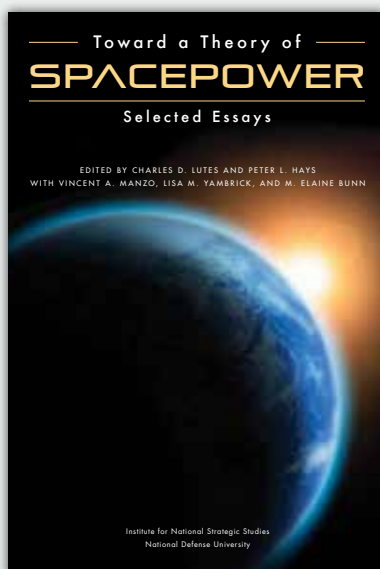
by James G. Stavridis

Admiral James G. Stavridis, USN, reflects on his tenure as Commander of United States Southern Command. Upon taking command, Admiral Stavridis discarded the customary military model and created an innovative organization designed not solely to subdue adversaries, but to build durable partnerships with friends. From his unique perspective as commander, Stavridis uses his engagingly personal style to describe his vision for the Americas.

Partnership for the Americas is available in an e-book format. This new format makes the book readable not only on desktop and laptop computers, but also on Apple's iPad, Sony's Reader, the Barnes & Noble Nook, and Android-based phones.

Find it online at:

<http://www.ndu.edu/press/stavridis.html>



Toward a Theory of Spacepower: Selected Essays

edited by Charles D. Lutes and Peter L. Hays, with Vincent A. Manzo, Lisa M. Yambrick, and M. Elaine Bunn

This volume is a product of the Institute for National Strategic Studies Spacepower Theory Project Team, which was tasked by the Department of Defense to create a theoretical framework for examining spacepower and its relationship to the achievement of national objectives. The team considered the space domain in a broad and holistic way, incorporating a wide range of perspectives from U.S. and international space actors engaged in scientific, commercial, intelligence, and military enterprises. This collection of essays serves as a starting point for continued discourse on ways to extend, modify, refine, and integrate a broad range of viewpoints about human-initiated space activity, its relationship to our globalized society, and its economic, political, and security interactions. The volume should help to equip practitioners, scholars, students, and citizens with the historical background and a conceptual framework to navigate through and assess the challenges and opportunities of an increasingly complex space environment.



Visit the NDU Press Web site for more information on publications at ndupress.ndu.edu



From NDU Press

PRISM

A Journal of the Center for Complex Operations

PRISM 2, no. 2 (March 2011) offers the most content ever, including the following Feature articles: Professor Mary Kaldor on “human security” in complex operations; Ambassador Nancy Soderberg on enhancing U.S. support for UN peacekeeping; Colonel Eric Jorgensen on the “Interagency”; Dr. James Orton and Dr. Christopher Lamb on interagency national security teams; Admiral James Stavridis on the Comprehensive Approach in Afghanistan; Rear Admiral Brian Losey on conflict prevention in East Africa; Dr. Roger Myerson on state-building; Major General (Ret.) Michael Smith and Rebecca Shrimpton on an Australian perspective of nation-building; Major Rebecca Patterson and Jonathan Robinson on changing CERP practices; and General Norton Schwartz on airpower in

counterinsurgency and stability operations. From the Field articles include Dr. James Schear, Lieutenant General William Caldwell IV, and Frank DiGiovanni on ministerial advisors; and David Becker and Robert Grossman-Vermaas on measuring Haiti stabilization. Lessons Learned articles include Jessica Lee and Maureen Farrell on civil-military operations in Kenya and Lieutenant General Ranier Glatz on a German perspective of ISAF. Finally, there is an interview with General William Ward on U.S. Africa Command.



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.

Last Call for Entries for the 2011

Secretary of Defense National Security Strategy Essay Competition and Chairman of the Joint Chiefs of Staff National Defense and Military Strategy Essay Competition



Are you a Joint Professional Military Education (JPME) student? Imagine your winning essay in the pages of a future issue of *Joint Force Quarterly*. In addition, imagine a chance to catch the ear of the Secretary of Defense or the Chairman of the Joint Chiefs of Staff on an important national security issue. Recognition by peers and monetary prizes await the winners.

Who's Eligible: Students at JPME colleges, schools, and other educational programs. Students must submit essay entries *through their respective colleges*.

What: Research and write an original, unclassified essay in one (or more) categories.

When: Colleges are responsible for running their own internal competitions to select nominees and must meet these deadlines:

April 27, 2011: Colleges submit nominated essays to NDU Press for first-round judging

May 17–18, 2011: Final-round judging and selection of winners

For complete information on the competitions, see your college's essay coordinator or go to:

<http://www.ndu.edu/press/essayCompetitions.html>



JOINT FORCE QUARTERLY

Published for the Chairman of the Joint Chiefs of Staff by National Defense University Press
National Defense University, Washington, DC

