JFQ

JOINT FORCE QUARTERLY

Issue 46, 3d Quarter 2007

Published for the Chairman of the Joint Chiefs of Staff by National Defense University

U.S. STRATEGIC COMMAND

Intelligence and Technology

Officer Attitudes Toward UAV Adoption

Combating Terrorism with Socioeconomics

JFQ

JOINT FORCE QUARTERLY

ISSUE FORTY-SIX, 3D QUARTER 2007

A PROFESSIONAL MILITARY AND SECURITY JOURNAL

Inside

Issue 46, 3d Quarter 2007

Editor **Col David H. Gurney, USMC (Ret.)**
gurneyd@ndu.edu

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**

Associate Editors **Jennifer C. Veilleux**
Chaim E. Mandelbaum

Design **Rebecca J. White, Chris Dunham, Gwynn Fuchs, and Jamie Harvey**
U.S. Government Printing Office

Staff Photographer **SSgt D. Myles Cullen, USAF**

Printed in St. Louis, Missouri
by UNIVERSAL Printing Company

NDU Press is the National Defense University's cross-component, professional, military, and academic publishing house. It publishes books, policy briefs, occasional papers, monographs, and special reports on national security strategy, defense policy, national military strategy, regional security affairs, and global strategic problems. NDU Press is part of the Institute for National Strategic Studies, a policy research and strategic gaming organization.

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
300 Fifth Avenue
Fort Lesley J. McNair
Washington, DC 20319-5066

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

3d Quarter, July 2007

ISSN 1070-0692

A PROFESSIONAL MILITARY AND SECURITY JOURNAL

JFQ Dialogue

Forum

Special Feature

ABOUT THE COVERS

The front cover shows a collage of images from the U.S. Strategic Command Special Feature. The back cover shows (clockwise) Army Special Forces and Philippine Scout Rangers lifting wounded into helicopter after firefight with rebels in Upper Mangar, Philippines (U.S. Army/Andrew Meyers); USS *Fitzgerald* and USS *John Paul Jones* preparing to fire during Exercise Talisman Sabre (U.S. Navy/Bo J. Flannigan); Royal British Army soldiers driving Pinzgauer reconnaissance vehicles through logistics support area at Camp Viper, Iraq (U.S. Air Force/Edward D. Kniery); and Navy officer speaking with Chinese sailors during a joint search and rescue exercise (U.S. Navy/Ashley Hickman).

JFQ

Commentary

Features

Interagency Dialogue

Recall

Book Reviews

SHOWN ABOVE

The table of contents shows Sailors from Riverine Squadron 1 and Marines from 2d Marine Expeditionary Force aboard riverine craft in Taqaddum, Al Anbar Province, Iraq (2d Marine Aircraft Wing/Michael Kropiewnicki); Marines discussing coalition operations with French sailor onboard USS *John C. Stennis* under way in Arabian Sea (U.S. Navy/Paul J. Jenkins); launch of Peacekeeper missile, the newest intercontinental ballistic nuclear missile (U.S. Air Force); and B–2 Spirit bomber followed by F–117 Nighthawks (U.S. Air Force).

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 smothermanj@ndu.edu "Attention A&R Editor" in the subject line. For further information see the guidelines on the NDU Press Web site at ndupress.ndu.edu.

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

ndupress.ndu.edu

DEADLINE Approaching for *JFQ* Issue 48

FEATURING:

U.S. Northern Command

AND

The Long War and Homeland Defense

Submissions Due by

September 1 2007

Visit **ndupress.ndu.edu** to view our Guide for Contributors. Share your professional insights and improve national security.

JFQ Dialogue

Open Letter to *JFQ* Readers

Joint Force Quarterly is distributed to senior interagency leaders as well as to all flag officers, military Services, and combatant commands, and it is translated into several languages. The journal has increased in size 150 percent over the past year, and the number of private subscriptions is at a record level. *JFQ* owes its success to the high-quality manuscripts that National Defense University Press receives from national security professionals in and out of uniform. Thanks to the generous support of the National Defense University Foundation, three *JFQ* authors each year receive special recognition for articles of exceptional quality. Twenty professors from all senior military educational institutions convened on May 22–23 to judge articles from the July 2006 through April 2007 issues, and they awarded three $1,000 cash prizes to the authors of the articles they deemed to be most influential. The winning authors will be acknowledged in the October issue of Joint Force Quarterly.

The *JFQ* staff would like to solicit manuscripts on specific subject areas in concert with future thematic focuses. The following topics are tied to submission deadlines for specific upcoming issues:

September 1, 2007 (Issue 48, 1st quarter 2008):
The Long War
Homeland Defense
U.S. Northern Command

December 1, 2007 (Issue 49, 2d quarter 2008):
Focus on Air and Space Power
U.S. Special Operations Command

March 1, 2008 (Issue 50, 3d quarter 2008):
Weapons of Mass Destruction
Stability and Security Operations
U.S. Central Command

June 1, 2008 (Issue 51, 4th quarter 2008):
Focus on Naval Power
National Security Council

JFQ readers are typically subject matter experts who can take an issue or debate to the next level of application or utility. Quality manuscripts harbor the potential to save money and lives. When framing your argument, please focus on the *So what*? question. That is, how does your research, experience, or critical analysis improve the reader's professional understanding or performance? Speak to the implications from the operational to the strategic level of influence, and tailor the message for an interagency readership without using acronyms or jargon. Also, write prose, not terse bullets. Even the most prosaic doctrinal debate can be interesting if presented with care! Visit ndupress.ndu.edu to view our NDU Press Submission Guidelines. Share your professional insights, and improve national security.

Colonel David H. Gurney, USMC (Ret.)
Editor, *Joint Force Quarterly*
Gurneyd@ndu.edu

Joint Doctrine Update

Joint Chief of Staff J7 Joint Education and Doctrine Division

The joint doctrine development community continues its aggressive pace of publication revision. Among more than a dozen titles already signed this year, of most significance is the approval of the Capstone joint publication in the joint doctrine hierarchy. Joint Publication (JP) 1, *Doctrine for the Armed Forces of the United States*, recently signed by the Chairman of the Joint Chiefs of Staff, provides the overarching, authoritative guidance for the employment of the Armed Forces. The importance of the Capstone publication cannot be overstated, particularly with its treatment of warfare and unity of effort.

"Foundations," the first chapter of JP 1, captures for the first time in joint doctrine the intellectual framework surrounding traditional and irregular warfare. At the crux of this discussion with regard to the two types of warfare is the fundamental difference between them—*the strategic purpose*. Whereas traditional warfare aims to force a change in an adversary's government or policies, irregular warfare seeks to gain legitimacy and influence over a relevant population.

JP 1, the consolidated product of its previous version and JP 0–2, *Unified Action Armed Forces*, also provides clarity with respect to the relationships between national strategic direction, unified action, and unity of effort. According to JP 1, *National Strategic Direction*—governed by the Constitution, Federal law, and U.S. Government policy regarding internationally recognized law—leads to unified action. JP 1 redefines *unified action* as the "synchronization, coordination and/or integration of the activities of governmental and nongovernmental entities with military operations to achieve unity of effort." *Coordination*, a word absent from the previous definition, acknowledges the lack of a hierarchical relationship between myriad organizations that may work together. Defense Department terminology no longer recognizes the phrase *Unified Action Armed Forces*. Finally, JP 1 introduces the joint definition of *unity of effort*: "Coordination and cooperation toward common objectives, even if the participants are not necessarily part of the same command or organization—the product of successful unified action." The exact wording of these definitions provides accuracy and precision to often confusing relationships (that is, does unity of effort lead to unified action, or vice versa?). Simply stated, national strategic direction leads to unified action; successful unified action produces unity of effort.

The revision of JP 1 followed shortly after the approval of the Keystone publications for personnel, operations, and planning (JPs 1–0, 3–0, and 5–0, respectively). With the projected approval of the revisions of the intelligence and logistics Keystone publications (JPs 2–0 and 4–0, respectively) anticipated for later this year, joint doctrine will remain relevant, consistent, and beneficial to the joint warfighter. These documents will guide the doctrine for their subordinate publications.

Publication revision must not be viewed as an endstate, but rather a starting point for common reference. The joint force—the combatant commands, Services, and Joint Staff—has an inherent responsibility to determine what fundamentally works best throughout the planning, preparation, execution, and assessment activities of operations. Capturing these best practices based on extant capabilities—the essence of joint doctrine—serves to increase the overall effectiveness of the U.S. military.

For access to joint publications, go to the Joint Doctrine, Education, and Training Electronic Information System Web site at https://jdeis.js.mil (.mil users only). For those without access to .mil accounts, please go the Joint Electronic Library Web site at http://www.dtic.mil/doctrine.

Joint Publications (JP) Revised, Calendar Year 2007

JP 1, *Doctrine for the Armed Forces of the United States*

JP 1–04, *Legal Support to Military Operations*

JP 2–03, *Geospatial Intelligence Support to Joint Operations*

JP 3–01, *Countering Air and Missile Threats*

JP 3–03, *Doctrine for Joint Interdiction Operations*

JP 3–05.1, *Joint Tactics, Techniques, and Procedures for Joint Special Operations Task Force Operations*

JP 3–07.3, *Joint Tactics, Techniques, and Procedures for Peace Operations*

JP 3–07.5, *Joint Tactics, Techniques, and Procedures for Noncombatant Evacuation Operations (renumbered as JP 3–68)*

JP 3–13.1, *Electronic Warfare*

JP 3–15, *Joint Doctrine for Barriers, Obstacles, and Mine Warfare*

JP 3–16, *Multinational Operations*

JP 3–33, *Joint Task Force Headquarters*

JP 3–34, *Joint Engineer Operations*

JP 3–35, *Joint Deployment and Redeployment Operations*

JP 3–50, *Personnel Recovery*

JP 3–60, *Joint Doctrine for Targeting*

JP 3–07.3, *Joint Tactics, Techniques, and Procedures for Peace Operations*

Joint Publications Near Revision (3d quarter, Fiscal Year 2007)

JP 2–0, *Doctrine for Intelligence Support to Joint Operations*

JP 3–04, *Joint Tactics, Techniques, and Procedures for Shipboard Helicopter Operations*

JP 3–07.4, *Joint Counterdrug Operations*

JP 3–26, *Homeland Defense*

JP 3–28, *Civil Support*

JP 3–63, *Joint Doctrine for Detainee Operations*

Strategic Communication and National Security

By **JAMES G. STAVRIDIS**

I don't know what the hell this* [strategic communication] *is that Marshall is always talking about, but I want some of it.

—Attributed to Admiral Ernest King during World War II

Winston Churchill is said to have observed that the principal difference between management and leadership is communication. Effective communication requires the leaders of an organization to take an early and persistent role in deciding how ideas and decisions are shaped and delivered. Certainly in the national security context, a leader can improve the effects of operational and policy planning by ensuring that the communications implications of that planning are considered as early as possible in the process. If planning is done in this fashion, then it is likely that the communications associated with it will indeed be strategic in their effects.

Simply stated, the objective of strategic communication is to provide audiences with truthful and timely information that will influence them to support the objectives of the communicator. In addition to truthfulness and timeliness, the information must be delivered to the right audience in a precise way. This generalized approach can be applied to essentially any organization, to the Department of Defense (DOD) broadly, and specifically to the individual nine combatant commands of the United States.

Admiral James G. Stavridis, USN, is Commander, U.S. Southern Command.

Our approach at U.S. Southern Command is to consider strategic communication as an enabling capability for our policy and planning decisions and actions; provide truthful information about those decisions or actions; communicate it in a timely and culturally sensible fashion; use messengers who are likely to be well received; measure the results of our efforts diligently (clearly our hardest challenge and greatest shortcoming); and adjust both message and method of delivery accordingly. In the Southern Command's region—32 countries and 13 territories including some 450 million people speaking 4 principal languages and dozens of dialects—our view is that nothing we do is more important than strategic communication. This is a part of the world, thankfully, where it appears highly unlikely that we will launch Tomahawk missiles. It is, however, an area where it is necessary to launch ideas, concepts, information, conferences, viewpoints, interviews, and the many other streams of data that constitute effective strategic communication. It is, in every sense, our "main battery" at U.S. Southern Command.

As Newt Gingrich, an astute student of strategic communication, has written, "Strategic Communication in a real-time worldwide information system is a branch of the art of war comparable to logistics or intelligence. It will require staffing, educating and practicing at about the same level of resources as intelligence or logistics to be successful." It also will require the early and persistent involvement of commanders at all levels. That is precisely our approach from our headquarters in Miami looking south, and we are working to add resources to this important—indeed, vital—aspect of our mission in Central and South America and the Caribbean.

In attempting to discover the right approach for strategic communication in the Southern Command's diverse region, we have examined a series of historical examples of strategic communication. Some of the more famous include the announcements surrounding the assassination of Julius Caesar in the first century CE, Abraham Lincoln's campaign to publicize the Emancipation Proclamation, and the Japanese Empire's "Economic Co-Prosperity Sphere" in the mid- to late 1930s. More recent examples of strategic communication that we have examined include the announcement of involuntary feeding of detainees at Guantanamo Bay; publicity for a humanitarian exercise in the Dominican Republic; and the cruise of the Navy's hospital ship, USNS *Mercy*, through the Pacific. Each of the recent case studies is worth thinking about in somewhat more depth as we consider an appropriate approach for the Southern Hemisphere.

Case Studies

The first case study was largely a public relations challenge and required a response at the tactical level. A group of detainees in Guantanamo Bay's detention and interrogation facility began a large coordinated hunger strike on August 8, 2005. DOD policy is to always preserve the lives of the detainees, and, as a result, 43 hunger strikers were enterally fed, using U.S. Federal Bureau of Prisons guidelines, which include use of a restraint chair and a very small diameter flexible rubber tube inserted through the nostril, down the throat, and into the stomach. A motion was filed in February 2006 alleging torture through the use of the restraint chair to assist in involuntary feedings.

Given the DOD policy of preserving life, the leadership view at Guantanamo Bay was that a detainee on a hunger strike requiring feeding clearly qualified as a lifesaving emergency. However, there was significant public outcry concerning the procedure, which we failed to anticipate. In particular, the use of a restraint chair—necessary to accommodate the procedure—was

categorized as "torture," despite the fact that it is an entirely humane and common procedure in U.S. and other prison systems worldwide to preserve life.

The surprise negative press and false characterizations, which reinforced challenges to DOD detention operations, compelled the Department to conduct a reassessment of policies and procedures in order to counter the impression that the United States had something to hide. This campaign included a wide variety of tactical responses, which were orchestrated loosely out of the Pentagon. They included bringing a team of distinguished physicians to Guantanamo to observe the procedure; publishing articles on the process; emphasizing the lifesaving character of the operation and the common procedures used in accredited prisons; and sending representatives to conduct interviews with the media to describe the procedure in detail. The commander of the Joint Task Force, Rear Admiral Harry Harris, USN, had the procedure performed on himself so that he could correctly describe it and personally refute allegations of torture. While an initial challenge was apparent, particularly in not correctly predicting the response to the feeding techniques, DOD eventually turned the corner, and when publicity died down, the vast majority of hunger-striking detainees began eating again.

A second case study involved a humanitarian exercise (New Horizons) in the Dominican Republic in the spring of 2006. Troops from U.S. Southern Command were sent to participate in a series of joint endeavors with the Dominican armed forces to build clinics and dig wells. Unfortunately, our strategic communication plan was not well executed, and as the Los Angeles Times reported, "As the equipment and troops amassed over weeks with little explanation in the local media, suspicions deepened that the Americans were engaged in something more than a humanitarian mission." As a result of not thinking through and executing a well-constructed strategic communication plan, our erstwhile effort actually created a negative backlash in the local media. We also need to link such events into 3-year plans for strategic communication, not treat each as an isolated event.

The third case study was an unqualified success and involved the strategic communication associated with the voyage of the hospital ship USNS *Mercy* through Southeast Asian waters in 2006. The cruise was conceived as a follow-up to American assistance rendered during the tsunami crisis of late 2004 and early 2005, and the ship's sailing a month later was designed to show continuing U.S. involvement, commitment, and presence in the region. During the course of the 60,000-ton ship's cruise from May to September, the crew of nearly 700 (including many volunteers from international relief organizations) performed over $30 million in services and goods transfers and saw over 200,000 patients. All of this was aggressively communicated using a detailed strategic communication plan. The onboard public affairs team, supplemented by people in each of the various ports of call, was able to have a measurable impact on the impressions Southeast Asians have about the United States.

Communication Guidelines

Drawing on these three case studies, as well as many others, we have developed a series of principles that serve to guide strategic communication, with a focus on our own efforts in the Southern region.

Tell the Truth. The first principle is the simplest: always provide the truth to the audiences with whom you are communicating. Nothing will more quickly doom strategic communication to failure than even a single instance of falsehood. A strategic communication team can have superb messages, excellent messengers, a carefully crafted plan—yet all of it can fail if they are proven to be lying about anything. This has been demonstrated most often in the history of "damage control" types of strategic communication. Many political scandals, for example, tend to explode when revelations of lying to investigators after the fact emerge, as opposed to during or immediately after the initial malfeasance. The truth, throughout a program of strategic communication, constitutes absolute bedrock. Tell the truth, and emphasize that you do tell the truth. Over the long run, it is unquestionably the best approach.

Have a Good Message. All the brilliant strategic communication in the world will not sell a bad message, as the Japanese Empire discovered with the East Asian Co-Prosperity Sphere. A brutal, extractive regime that brought little or no benefit to the "partner" nations could not be dressed up as anything other than imperialism. Again, this seems quite simple, but in practice, there are many in the world of strategic communication who believe that a bad message can be sold effectively. It cannot. The strategic message must resonate with the audience because it shares appropriate human values, such as liberty, justice, honesty, economic improvement, security, fair treatment, and so forth.

Naturally, there are times when the message is, in fact, bad news. The world will always be full of mistakes, disasters, failures, and acts of incompetence. But when that happens, the effort must be made not to spin the truth, but rather to tell what happened honestly, let people know truthfully how bad it was, apologize when warranted, pledge improvement, and outline measures taken to prevent reoccurrence. Torie Clark, in her excellent book on strategic communication, describes this as "not trying to put lipstick on a pig."

Understand the Audience. This is the constantly rediscovered golden rule of strategic communication. Too many communicators develop plans in a vacuum without spending the necessary time and resources to understand the nuances of the audiences to whom they are pitching the product. A classic example of this is in Central and South America and the Caribbean, where one message definitely does not fit all audiences. Can there be two more different countries in the world than enormous Portuguese-speaking Brazil and tiny English-speaking St. Kitts? Or more different than Spanish-speaking, economically strong Chile and poverty-stricken French-/Creole-speaking Haiti? In each country or territory, to each group of people, during each particular season, the audience is different, and therefore the messages must be evaluated and tailored with the diverse qualities of the receiver in mind.

Pull the Trigger Promptly. This seems self-evident, but all too frequently an excellent plan comes to naught because we are unable to execute in a timely manner. Do not let "perfect" become the enemy of "very good." In other words, develop a reasonably good plan fast and execute it. Otherwise, it is far too easy to end up "back on your heels" in the world of the perpetual news cycle.

Think at the Strategic Level. Public affairs and strategic communication are two very different things. A strategic communi-

cator must stay at the strategic level and not dip down to the tactical level represented by public affairs. Strategic communication consists of a wide variety of tools and processes within a command such as U.S. Southern Command, to include public affairs, protocol, legal, political-military analysis, medical outreach, engineer and construction support, logistics, personnel, and many more. Each has a role to play in effective strategic communication at the tactical or operational level, but none of them is a substitute for a strategic plan operating at the level of the entire theater, across time, space, language, and culture. At the strategic level, the intellectual firepower of the command must be brought most distinctly to bear.

Organize at the Operational Level to Enable at the Tactical. For a combatant commander, the place to "organize" strategic communication is at the operational level. This means that strategic communication plans must be developed that can operate across subregional sections of the command area. In U.S. Southern Command, we divide the region into four subregions: Andean Ridge (Bolivia, Colombia, Ecuador, Peru, and Venezuela); the Southern Cone (Argentina, Brazil, Chile, Paraguay, and Uruguay); Central America; and the Caribbean. By organizing in this fashion, we can better tailor messages, maximize resources, find

synergies, and move out on the strategic plan that we have developed for the region as a whole.

After organizing at the operational level, we try to execute smoothly. Tactically, in the sense of strategic communication for U.S. Southern Command, we are operating at the individual national level. This is where all the components of the strategic communication plan must fit together, and most particularly our plan must be fully coordinated and synched up with the Embassy's efforts. The tactical level is where public affairs and all the associated efforts are linked together and execution of the plan occurs—all of it fast, furious, and energetic. This is not the cerebral part of the operation, but rather the place where instant response, dynamic creativity, and good language skills matter most.

Measure Results. So many strategic communication plans flounder because the implementers, thrilled with having developed and "sold" the plan, are completely consumed with execution—but then end up not doing what is the most important single step: measuring results. The absolute key to effective communication is rolling out a plan, organizing it widely, executing energetically, and then measuring results. There are obviously many means of doing so, but a few crucial ones include polling by reputable local firms and backing up the polls with an international polling firm; contacting individual trusted and sensible interlocutors for candid assessments; monitoring articles in journals, newspapers, and other publications; sampling Web content, including blogs; observing television and radio coverage; and working with a local public relations firm. We are in the infant state of this at U.S. Southern Command but are working hard to improve because it is the critical path for achieving results.

Adjust Fire. No strategic communication plan is perfect from conception. All must be put into practice and adjusted as time goes by. A way to approach measurement is to adopt a short-, medium-, and long-term view. Short term is immediate reactions, say 24 to 48 hours. Medium-term measurement is after 30 to 45 days. And finally, long-term measurement must occur at the 1-year point. After each of these measurement windows, the plan should be evaluated and recast, after reacting to what is working and what is not.

Add Spice. Strategic communication should not be boring. A look at the "strategic communication" of the Cold War by both sides shows a pattern of rote, predictable, and almost entirely ineffective patterns of communication. It was not until late in the Cold War with the arrival of the Reagan administration that spice was added to the diet with strategic communication tactics (for example, describing the Soviet Union as the "evil empire" and President Reagan ordering, "Mr. Gorbachev, tear down this wall"). When looking at successful strategic communication plans, industry is often a good guide. The performance of Chrysler Corporation under Lee Iacocca provides a wonderful example of a plan perfectly executed. To communicate his vision, Iacocca began with a simple message that inspired customers and employees alike: "Quality, hard work, and commitment—The stuff America is made of. Our goal is to be the best. What else is there? If you can find a better car, buy it!"

For a combatant commander, the place to "organize" strategic communication is at the operational level

Chrysler's remarkable turnaround resulting from Iacocca's leadership shows that following each of the principles above—from having a truthful plan to constantly measuring and adding spice—is the best approach. In the case of U.S. Southern Command, we are constantly seeking new ways to describe the benefits of partnering with the United States in our areas of expertise (for example, military-to-military relations, counternarcotics, antismuggling). These can range from new techniques (use of unmanned vehicles and subsurface surveillance) to better packaged training for officers and soldiers of individual countries back in the United States. Mix it up!

Steady Pressure. Very seldom do strategic communication plans succeed overnight. Just as careers of individuals take time to build to fruition, a good strategic communication plan needs steady pressure over a significant period to bear fruit. In U.S. Southern Command, we have been working hard over the long term to make improvements across the board in reducing human rights violations by military forces in a region with a long tradition of such problems. This is a strategic communication plan that takes a long time, sometimes generations, to fulfill. It includes sending key officers and enlisted leaders to schools in the United States; our leadership giving speeches and writing articles on the subject; hosting regional conferences, often including international

human rights groups; and a myriad of other initiatives. It is gradually bearing fruit, but there will be setbacks. The key is applying steady pressure.

Bursts of Energy. The analog to steady pressure, of course, is bursts of energy. In any strategic communication plan, there will be moments when it is opportune to hit with bursts of energy. Such a moment might be immediately before or after an international conference or a national election; it might occur following a natural disaster; it could be on the anniversary of a particular event. A creative strategic planner is constantly looking for the right moment to come in high and hard with a burst technique. Such moments become efficient ways to increase "bang for the buck" of a particular event, speech, or other strategic communication resource.

Accepting Defeat and Moving On. Some strategic communication battles are unwinnable. There will be moments when no matter how effective the plan, the message is not going to have any effect. This can occur for a wide variety of reasons, generally when the audience is simply unwilling to listen to anything at all. For example, when the Persian empire sought to invade Greece in 300 BCE, the Persian emperor Darius crafted a clever strategic communication plan that sought to divide the Greek city-states and offered reasonably benign terms to any state willing to sign on with the Persians. But the Greeks were utterly devoted to their nascent form of democracy and were unreceptive, leading to war. Despite having a rational message, a fairly good series of messengers, and a coherent strategy, Darius was unable to find an outcome other than war. And when he was eventually defeated by a coalition of the Greek city-states, he was wise enough to turn his attentions to the east and move on. So it must be, occasionally, in the world of strategic planning.

Knowing When You Win. Sometimes the hardest thing for any strategic planner is not accepting defeat but rather recognizing victory. As a general rule, "winning" in the world of strategic communication is never clean and seldom obvious. If your charter is to convince the populace of a given region that democracy and liberty are important values, it will not suddenly be obvious that you have succeeded. Tipping points are often hard to spot. But gradually, the benchmark measurements should turn in the right direction, media outlets should repeat messages, and trends should begin to turn. At such times, a determination must be made as to whether it is time to back out and let the audience find its own way forward, apply a final burst of energy, or continue steady pressure. It is an art, not a science.

Recommendations

In addition to the principles above, there are four final recommendations worth considering as we approach strategic communication in the 21st century.

First, strategic communication is the ultimate team sport. It must be done as part of a joint, interagency, and commercial system. It does no good whatsoever to have a perfect strategic communication plan that is ultimately contradicted by other U.S. Government agencies, as—unfortunately—is often the case. Each plan must be vetted properly and hopefully become a combined effort. It should take into account what U.S. private industry is doing in a given country or region so that inherent contractions between public and private institutions do not undermine the entire effort. It must be crafted in a sensible, collaborative, collegial way and done in an appropriate voice.

Second, at least for strategic communication that goes beyond the shores of the United States (a safe assumption for virtually everything we do in this arena), the international community must be considered and often consulted. In other words, the impact on individual countries and international organizations should be considered, and—if possible—they should be part of the plan. In particular, international organizations have resources that can be used in execution and even in planning, as they were, for example, in the voyage of the *Mercy* and the Pakistani earthquake relief effort. Likewise, little can be done effectively in a foreign country without the cooperation of the host nation and regional organizations. Often, they can contribute to strategic messaging and should be consulted in many instances. While there are clearly exceptions, such consultations and cooperation can frequently pay enormous dividends.

Third, as we develop and execute our strategic communication plans, we should ask the simple question: Who are the thinkers? It is not inherently obvious who is "good" at strategic communication. Many commands, including U.S. Southern Command, have hired individuals and sometimes commercial consulting firms to participate. We can find thousands of such entities by Googling "strategic communication." But each strategic plan and each organization—and indeed each time a plan needs to be developed—may need a different set of thinkers. So look around the organization and even outside it, especially to non-U.S. sources of input and criticism, for advice, execution, measurement, and judgment. Also, recognize that the "strategic communication director" is more like the conductor of a band than an expert on a given instrument. Moreover, give the director of strategic communication unfettered access to the commander. At U.S. Southern Command, our director of strategic communication attends the daily morning standup with the commander, interacts constantly with the senior leadership of the command, and is a prime mover in every sense in our organization.

Fourth, and finally, we in the business of national security must work together to arrive at a shared understanding of what constitutes strategic communication in an international context. This is an effort that must involve practitioners at the Department of Defense, Department of State, and indeed at all Cabinet organizations and national agencies engaged in international strategic communication on behalf of the United States. It is also an effort that can be informed by those in private industry who work in this milieu.

In the end, working in strategic communication for national security is a bit like working in a laboratory trying to find a cure for cancer. There are many false starts, mistakes, and incorrect leads. Resources are often difficult to obtain, especially because it is often hard to show prime results. Steady pressure is generally the right solution, and occasionally a true burst of energy can make great strides. There is unlikely to be a perfect single-point solution, but one should expect incremental progress, measured in years, and only a series of partial palliatives obtained along the way. But it is all in a worthy cause, the work is fascinating, and in the end, the efforts of the strategic communicator can be of enormous benefit to the national security of the United States, especially in the emerging complex world of this unsettled 21st century. **JFQ**

"Deconfusing" Lethal and Kinetic Terms

By KARL E. WINGENBACH *and* DONALD G. LISENBEE, JR.

It is time to "deconfuse" ourselves concerning the words *lethal* and *kinetic*. The joint force—in both its doctrine and concepts communities—must not only adopt standard definitions and usages of these terms but also achieve a common understanding of the ideas *behind* the terms. As the joint force continues to advance its doctrinal and conceptual language beyond today's environment, we find ourselves searching for words to describe the ideas, actions, and consequences necessary for complex operations where both lethal and nonlethal methods must be skillfully intertwined.

The use of the words *kinetic* and *nonkinetic* has proliferated beyond the merely colloquial into formal concepts and doctrinal literature. Unfortunately, use of these terms has been inconsistent and ill defined without a proper foundation built on Defense Department usage.

A standard dictionary defines *kinetic* as "of, relating to, or produced by motion." Our military will often redefine words to provide clarity or specificity to our usage; we make certain words part of our jargon. Common examples include "operation" or "maneuver." These definitions, however, rarely contradict accepted usage. First used as shorthand for any bomb or bullet, the use of "kinetic" evolved, somewhat logically, to mean any lethal action. However, the converse, "nonkinetic," does not follow the same logic. *Nonkinetic* denotes inaction or lack of motion. Clearly, this is not the intent of those who would classify, for example, psychological operations as nonkinetic. There is a great deal of action, motion, and effort to the deliberate, successful use of psychological operations against an adversary. Our use of the term nonkinetic is more likely an attempt to describe actions that do not intentionally or normally have lethal consequences. The imprecision that has evolved is confusing and not helpful to military art.

Kinetic and nonkinetic are not good replacements for words describing and differentiating lethal and nonlethal actions. We should discontinue the indiscriminate use of the word *nonkinetic* when we really mean *nonlethal*. Lethal and nonlethal are clearly defined, objectively understood terms.[1] It is generally understood what is meant by application or use of lethal force; it is a phrase that has specific legal implications in the military and in law enforcement. Lethal weapons can have both kinetic and nonkinetic properties. Moreover, kinetic energy weapons are not necessarily lethal (for example, a rubber bullet). Correct usage can be determined by a simple two-part test:

1. If it is desirable to differentiate between kinetic energy or explosive weapons and those that can disrupt, degrade, or disable without a physically destructive effect, then kinetic and nonkinetic can be used as shorthand for kinetic energy and nonkinetic energy weapons. Weapons are classified based on the source of energy that the weapon delivers to a target or the method of lethality. This point deserves elaboration; there are families of weapons:[2]

- kinetic energy (bullets, sabots)
- potential energy (grenades, bombs, nuclear weapons)
- directed energy (lasers, particle beams, high-power microwave)
- chemical (not to be confused with chemical explosives, which are part of the potential energy family)
- biological.

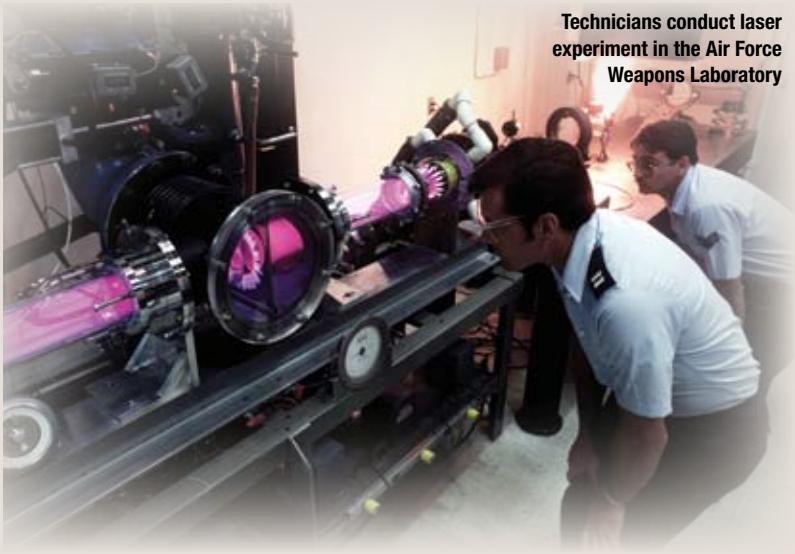
So nonkinetic would include everything *except* kinetic energy weapons. There is little doubt, though, that the users of nonkinetic understand that meaning. The use of the word *kinetic* when referring to weapons could apply to potential energy weapons because they have kinetic terminal properties (that is, the blast creates fragments with kinetic energy). Also, some directed energy weapons, such as lasers and particle beams, deliver kinetic energy to a target and have physically destructive effects, so they could be considered kinetic.[3] Therefore, it is reasonable to band kinetic energy, potential energy, and some directed energy weapons together and call everything else nonkinetic.[4]

2. If it is desirable to differentiate between lethal, physically destructive actions and nonlethal actions, then lethal and nonlethal should be used. *Lethal actions* include the entire range of offensive military operations (including kinetic weapons and some nonkinetic weapons, as discussed above) designed to result in the destruction of the target.[5] *Nonlethal actions* include psychological operations, some elements of information operations, civil affairs operations, and some unconventional warfare or foreign internal defense activities, among others. Lethal and non-

DOD (Andrew McGalliard)

Soldier displays rubber bullets, used for riot control

Lieutenant Colonel Karl E. Wingenbach, USA, is Senior Joint Doctrine Developer in the Joint and Allied Doctrine Division at the Army Capabilities Integration Center. Colonel Donald G. Lisenbee, Jr., USA, is Chief of the Joint and Army Concepts Division.



Technicians conduct laser experiment in the Air Force Weapons Laboratory

U.S. Air Force

lethal can apply to actions, capabilities, or effects. It is commonly understood that one can use lethal force in a nonlethal manner. The fact that a lethal weapon can be used in a nonlethal way does not change its lethality. Conversely, it is possible to apply lethal force with an instrument (such as an entrenching tool) that is designed for nonlethal purposes. Since the definition of *nonlethal weapons* includes the statement that they are designed to "minimize fatalities," the potential to use nonlethal weapons in a lethal manner is understood.

As we attempt to describe our capabilities in the most clear, correct, and concise manner possible, we should ask, "What is the intent or purpose of the action?" If the intent is to influence an adversary through a combination of lethal and nonlethal means, it is not essential to describe whether the action or capability is kinetic or nonkinetic. In today's, and even in tomorrow's, operational environment, commanders will continue to determine objectives and decide how they want to achieve those objectives using lethal or nonlethal means. Will the commander tell his staff, "Don't kill them, but use some kinetics"? Or, conversely, "Kill the scoundrels, but don't use kinetics"? Doubtful—it makes little sense. How, then, does it help to have a list of capabilities categorized into kinetic and nonkinetic bins?

Clearly, our military language has room for colloquialisms. However, in formal writing or military orders, it is important to be clear, concise, and accurate. Therefore, when speaking of actions or effects, use the terms *lethal* and *nonlethal*. When describing weapons and ammunition classifications, continue to use the terms *kinetic* and *nonkinetic*. The proper use of terminology, including the preferred lethal and nonlethal over the less precise kinetic and nonkinetic, reduces the ambiguity in professional writing and, more importantly, helps "deconfuse" us as we attempt to describe the range of military actions and capabilities. **JFQ**

NOTES

[1] See Joint Publication 1–02, *Department of Defense Dictionary of Military and Associated Terms* (Washington, DC: Department of Defense, November 30, 2004) for the definition of nonlethal weapons.

[2] U.S. Naval Academy, *Fundamentals of Navy Weapon Systems*, chapter 12, "Military Explosives."

[3] Without movement and mass, there is no kinetic energy ($E_k = \frac{1}{2} mv^2$). Projectiles, fragments, and particles have mass and can generate kinetic energy. Waves (for example, radar, microwave, sound) do not have mass and cannot generate kinetic energy. Photons (lasers) are in the middle; they are packets of electromagnetic radiation without mass, but they clearly deliver energy to the target and are technically kinetic.

[4] Nonkinetic does not imply nonlethal; obviously, directed energy, chemical, and biological weapons can be quite lethal. Also, kinetic would not equate to lethal; rubber bullets, for example, are nonlethal kinetic munitions.

[5] It is not necessary to kill a person for something to be considered lethal.

Letters to the Editor

To the Editor: After reading the Special Feature on U.S. European Command (USEUCOM) in the last issue of *Joint Force Quarterly* (issue 45, 2d quarter), I wanted to share my own experiences and insight as the foreign policy advisor (POLAD) to the USEUCOM commander.

All five geographic combatant commands have senior foreign policy advisors who assist in facilitating continuous and effective interface for their senior military commanders with the Washington, DC, interagency community. As a career diplomat in the Foreign Service, I have spent my professional lifetime serving the United States through diplomacy. My fundamental objective is to offer the interagency point of view and to assist the command with its expanding responsibilities.

Despite troubling and persistent setbacks in the international arena of public opinion, Americans must continue to try to influence events with soft power aspects of U.S. strength, particularly in the USEUCOM area of responsibility. In many situations, this kind of approach promises to be more effective than the traditional "hard power" aspects of our lethal force projection capabilities. Whatever the appropriate course of action, maintaining a mix of capabilities is absolutely essential across the spectrum of conflict and will mandate that all U.S. Government agency actions be synchronized. The expression "one team, one fight" is more than just a slogan.

Emphasizing our focus on hearts and minds does not redefine warfare, but rather enhances and optimizes the options for response. Among the most critical questions asked at USEUCOM are those that relate to long-term engagement—where and how we apply limited resources to shape a battle and favorably determine its outcome. There is clear recognition at this headquarters that certain regions of our area of responsibility demand increasing attention. In these locations (many of which are in Africa), responding to the multifaceted challenges of fragile states, poverty, disease, corruption, helplessness, and alienation may help prevent the rise of extremism and ultimately avoid the necessity of future traditional combat actions.

Challenges such as those faced in Africa mandate a U.S. command structure that directly and explicitly oversees engagement there. Moreover, as a result of Africa's

unique environment, this new structure most likely will deviate from traditional military staff models and more effectively capitalize on interagency expertise and resources. USEUCOM already recognizes the need for this interagency approach and is at the threshold of substantial changes. In the near future, a new command will be created to deal more directly and effectively with the problems facing Africa.

With almost 12 million square miles of territory and 800 million inhabitants, Africa is a continent of extraordinary human and natural resource wealth. A number of its 53 countries are considered developing democracies, but these nations are also challenged by economic, social, and health problems that defy purely military solutions and call for a new and more integrated U.S. Government approach. All Americans are filled with a sense of democratic freedom and dignity for human rights. Acting in the spirit of brotherhood and partnering to share our common values to live in a free society is the essential message that can be delivered by U.S. military personnel working alongside the Department of State Foreign Service. The notion is to make available the correct set of tools to address the multiple, complex, and varied problems across so huge a continent.

all Americans are filled with a sense of democratic freedom and dignity for human rights

However, as if Africa did not offer enough challenges, Eastern and Western Europe along with Russia also face problems and uncertainties. Significant terrorist attacks have taken place in major European capitals. Demographic trends, immigration, and the resulting backlash have brought concerns for cultural clashes and intolerance to the forefront. Resurgent nationalism and religious extremism have been unforeseen outgrowths of globalization. Finally, USEUCOM must be sensitive to the competing and often divergent requirements of emerging democracies in the Caucasus. Considered collectively, the scale and complexities of these disparate international challenges appear daunting and certainly defy simplistic solutions. Fortunately, a fully integrated U.S. Government interagency response offers a new approach and a promise of long-term success.

One of the potential keys to this interagency response will be the POLADs at combatant commands. With a heritage of service that stretches back to World War II, these Foreign Service officers have long brought multiple capabilities to the senior military officers they advise. Schooled in the nuanced art of diplomacy, and often equipped with specialized regional expertise and foreign language skills, they have succeeded precisely because of their ability to examine strategic issues from political dimensions and to bring the Department of State point of view to bear on regional problems.

Also key have been the advisors' abilities to build relationships, mitigate interdepartmental confusion, and harmonize the commanders' intentions. Almost one-third of current POLADs have served as U.S. Ambassadors and have developed skills in orchestrating interagency constituencies and resources. Moreover, as civilian contractors assume a larger and larger role in U.S. national security policy implementation, POLADs are positioned to facilitate interaction. Changes in the nature of the threat mandate the need for more interagency dialogue.

As effective as the POLAD can be in advising the commander regarding the employment of the instruments of power, it is important to understand the limitations and boundaries. Foreign policy advisors do not, in the strictest sense, act as Ambassadors to a specific country and cannot proceed as if they were. Accordingly, their facilitation, communication, and synchronization of State Department policy across numerous countries in the combatant command often present considerable challenges. Similarly, foreign policy advisors are not military staff officers, although they and their support staff are frequently and appropriately tasked to illuminate and evaluate political and foreign policy dimensions of various operations, programs, or initiatives. The POLAD's office does not generally provide action officers or planners. Organized to handle and deconflict more routine staff coordination activities at the headquarters, this function should be considered separate and distinct. To be most beneficial, the foreign policy advisor and associated office staff should remain an independent advisor team reporting directly to the command leadership. Traveling with the commander and sitting beside him at meetings with foreign heads of state and military officials present an integrated U.S. Government team. An experienced POLAD can provide valuable input during diplomatic meetings. For a diplomat, the key decisive engagement occurs most often at that critical meeting with foreign decisionmakers.

The major question addressed by this office is how to bring added value and enhanced mission effectiveness to USEUCOM. Senior American defense officials have long engaged with the changing conditions of the strategic environment, under terms that might best be described as operational uncertainty. The latest Quadrennial Defense Review underscores the notion that within the next 10 years, American forces are likely to be needed in areas of the world where they are not engaged currently. This being the case—and considering that the mission is so broad—the Department of Defense cannot accomplish the task alone. In Europe, Africa, and elsewhere, success ultimately depends on partnerships and unity of effort.

Ultimately, eliminating transnational terrorism, restoring stability to troubled regions of the world, and ensuring the future security of the United States and its allies will require well managed and thorough integration of our primary elements of national influence with those of our allies and friends. Considering the challenges facing us today, foreign policy advisors at the geographic combatant commands should be an increasingly vital asset. By building and strengthening relationships between the military commander and other governmental agencies, particularly the Department of State, a broad range of interagency tools may be effectively brought to bear to address the complex and significant challenges we face in every combatant command area of responsibility.

—Ambassador Mary C. Yates,
Political Advisor to the Commander,
U.S. European Command

To the Editor: Working my way through *JFQ* 45 (2d quarter, 2007), I came upon a jarring sentence on page 30. Concerning the internal political situation in Nigeria, Lieutenant Commander Patrick Paterson, USN, in "Maritime Security in the Gulf of Guinea," writes:

According to some U.S. officials, the worst-case scenario for America would be the emergence of a northern Muslim general or politician into the presidency, either democratically or through unconstitutional means. The United States could then find itself facing a Muslim population—nearly three times that of Iraq—in control of vast energy resources. Such a situation could result in U.S. military intervention on a much larger scale than in Iraq.

There's no indication in the sentence, or the surrounding context, that the author's concern is with the emergence of an Islamist, jihadist, or otherwise extreme Muslim faction controlling Nigeria's oil—as written, he seems concerned that control of these resources by Muslims of any description would be a threat potentially justifying U.S. military intervention.

Given our relations with Saudi Arabia and the Gulf emirates, professing the Muslim religion does not disqualify a government from playing a longstanding and relatively stable role as an American energy supplier. I have a difficult time believing our government would choose to intervene by force to overturn the results of a democratic Nigerian election that returned a Muslim as president. Naturally, our Islamist enemies would like the world to believe that the United States will support our "coreligionists" in places such as Nigeria at the expense of Muslims, and they would be happy to seize on any evidence that we do in fact harbor anti-Muslim intentions, such as the portion of the article cited above.

There are a number of scenarios that might argue for U.S. intervention in the Gulf of Guinea, but a Muslim's assuming the presidency of Nigeria, in itself, is probably not one of them.

—LtCol Matthew L. Jones, USMC
Quantico, Virginia

Executive Summary

The geographic combatant commander has a certain amount of capability, but when things start to heat up, he's going to want to reach back for scale. He is still the best person positioned for the agility of day-to-day transactions and activities, whether that be in trying to defuse a crisis or in trying to defeat an adversary. What we're trying to do is provide in a service construct the ability to move scale to him for whatever objective he's trying to do, whether it's to defuse or to defeat. If we do it that way, that tends to keep unity of command and unity of effort intact.

— General James E. Cartwright, USMC
Commander, U.S. Strategic Command

In this issue, *JFQ* again draws thematic parallels between focus areas in the Forum and the subject of our Special Feature: U.S. Strategic Command. In the Forum, we have essays addressing developments in intelligence and technology, which lead quite naturally to the combatant command charged to enable effects through the application and advocacy of integrated intelligence and cutting edge technologies across a remarkably wide spectrum of responsibility. Those who haven't kept up with the changes and challenges that USSTRATCOM has shouldered in recent years will be impressed—as we were—with the diversity and gravity of this command's functional expertise. In the lead interview, General Cartwright speaks with candor and clarity about the command's progress in cyber security, combating weapons of mass destruction (WMD), and space policy.

Before introducing these articles, a few words should be said about the *JFQ* Dialogue section that preceded this overview. On a recent trip to U.S. Southern Command, *JFQ* learned that its commander, Admiral James Stavridis, was working on a book addressing the thorny challenge of strategic communication. At our request, he generously submitted an essay exploring the issues that will be examined in greater detail in his larger work. Readers should compare the Admiral's perspective with that of Dr. Carnes Lord, whose complementary article in the Commentary section speaks to the *nature* of strategic communication.

Also up front is an argument against elements of contemporary military jargon that may hearten the Russian linguists who translated *JFQ* 45 in its entirety. Proof that English is a living language, military euphemisms are frequently more troublesome than enlightening (the parallel case against an endless supply of unnecessary acronyms such as BLUF, *bottom line up front*, is already widely lamented). This trend is particularly egregious when suitable words already exist to communicate the intended thought. Long before Colonels Donald Lisenbee and Karl Wingenbach submitted "'Deconfusing' Lethal and Kinetic Terms," *JFQ* replaced these otherwise useful words when they described physical and nonphysical or dynamic and static effects. As the authors point out, however, some also interpret these words to underline a distinction between lethal and nonlethal actions. Ironically, the authors' case against sloppy jargon arrived coincidently with a research paper detailing kinetic and nonkinetic information. It is worth noting that part of U.S. Strategic Command's mission statement includes "decisive global kinetic and nonkinetic combat effects."

As a final note about *JFQ* Dialog, we gratefully acknowledge the Political Advisor from U.S. European Command, whose manuscript arrived shortly after the last issue (which featured that command) had gone to press. Coordinated interagency action is clearly essential for most security challenges, and the Department of Defense plays an important *supporting* role in many bilateral security efforts. Understanding the institutional orientations and individual perspectives of our interagency colleagues is essential in our patient face-off against agile, unconventional enemies. *JFQ*, as always, seeks insightful viewpoints from Federal, allied, and private sector partners.

Our first installment in the Forum makes the case that globalism has fundamentally changed the nature of warfare as Clausewitz described it. Dr. Marion Bowman suggests that classic political objectives are now passé and that a new reality inspires mission sets that promote "stability and responsible participation in international affairs." He further asserts that global complexity has increased the importance of intelligence and that associated requirements are increasing far more rapidly than capability. The solution, offered in an essay that ranges from biometrics through improvised explosive devices to economics and WMD, begins with efficient coordination between interagency partners.

Colonel James Howcroft, the author of our second Forum entry, would deny that the fundamentals of war have changed at all but agrees that traditional notions of the intelligence cycle seriously limit the emerging potential of intelligence efficacy on contemporary and future battlefields. In the course of his argument, he restates the widely acknowledged complaint that that those at the tactical level—who are in greatest need of current intelligence—are precisely those least able to access it absent direct exposure. In response to calls for "actionable intelligence," CIA Director General Michael V. Hayden is noted for his counter to operators: "You give me action and I'll give you intelligence." The author complains that this is simply not happening for the forces in contact. Where Colonel Howcroft *does* fully agree with Dr. Bowman is in his assertion that the tools wielded by the interagency are critical to strategic success. Moreover, leaders and their organizations at the tactical level must be trained to paint the battlefield picture with fidelity in return for a commitment by higher headquarters to provide mission guidance and resources, and then step aside. The incessant demand for nonessential data by senior

command echelons must be disciplined. "Need to know" is a two-way street and this problem can only be resolved through trust.

Our third Forum article is an intelligence window on a topic that *JFQ* returns to frequently due to both writer supply and reader demand. The effects-based operations (EBO) concept has evolved from Millennium Challenge 2002 to General Lance Smith's effects-based *approach* to operations (EBAO) informed by his experience at U.S. Central Command. Among the several issues that critics bring to bear on this method is the problem of metrics. *JFQ* asked a tenacious proponent of EBO, Dr. Jim Ellsworth, to address the ability of intelligence to inform and measure operational effects. He acknowledges that the current intelligence cycle must evolve to widen the focus of the commander's priority intelligence requirements and focus on the systemic or psychological effects following stimulus. He then proposes refocusing the intelligence preparation of the battlespace and improving interagency collaboration. The author's case for EBO efficacy rests upon intelligence fusion beyond current practices. It is instructive that interagency synergy is emphasized by each Forum author and numerous academic studies, but recognition of this cry for cooperative discipline has not led to progress at the National Security Council. That is the focus of a future *JFQ*.

The fourth Forum offering is an excellent complement to the Special Feature interview, as the commander of U.S. Strategic Command speaks at length on China's antisatellite test and subsequently noted that "we don't need an arms race in space." Dr. Phil Saunders and Colonel Chuck Lutes present the findings of a roundtable convened at National Defense University to debate the motivations and implications of China's success against a target in low Earth orbit. China may have seriously underestimated the political damage the test would do to its claims of "peaceful development." The authors survey the implications of this event for the liberty of Taiwan and U.S. relations. Readers will be interested in the range of technical and operational means proposed to mitigate potential Chinese ASAT capabilities as well as the broader military and policy options.

The final Forum entry springs from the premise that tactical counterinsurgency operations closely resemble police work and demand civilian "beat cop" skills and sensitivities. The authors begin by identifying four

FOTODYNAMICS (Fred Carlson)

contextual elements that interfere with the skills that are essential for effective counterinsurgents. As in the second Forum piece, the authors emphasize that high technology solutions are not available to the lower echelons where they are needed most. The authors seek to equip insurgency warfighters with the law enforcement technology employed successfully in cities with similar challenges. A reader short on time should skim directly to the concluding six recommendations.

In our Special Feature, we survey U.S. Strategic Command (USSTRATCOM), beginning with a lengthy interview with its commander, General James E. "Hoss" Cartwright. In 2002, the Secretary of Defense directed the merger of USSTRATCOM and U.S. Space Command, and in the following year it was assigned four new responsibilities: global strike, missile defense integration, Department of Defense information operations, and intelligence, surveillance, and reconnaissance. In a 2005 reorganization to focus USSTRATCOM on strategic-level integration and advocacy of its chartered missions, General Cartwright delegated authority for operational and tactical level planning, force execution, and day-to-day management of forces to a handful of Joint Functional Component Commands (JFCCs). Since 2006, there have been five such JFCCs with the establishment of a separate functional command for space. Rounding out the organization are three organizations focusing on information operations, WMD and network operations. These functional subordinate commands are individually explored in a series of short articles following General Cartwright's very interesting introduction.

This is the longest issue of *JFQ* that has been printed in 10 years, thanks to an unprecedented number of submissions from civilian and military security personnel in the field. As mentioned earlier, *JFQ* is especially interested in non-military professional insights and interagency collaboration lessons as joint forces move to the next level of skill orchestration through partnership with nontraditional partners and colleagues in the war on terror. This said, military personnel are the writers, developers, and keepers of conventional warfare doctrine for the low frequency, high severity wars for which there can be no lapse in vigilance. General Burwell Bell, commander of U.S. Forces, Korea, recently warned *JFQ* that "conventional war is not extinct—it will happen again." As this is undoubtedly true, manuscripts proposing innovation and analyzing the implications of technology and change are solicited across the entire spectrum of conflict, stabilization, and security. The National Defense University Foundation has generously awarded $5,000 to *JFQ* authors in 2007 in recognition of the value and influence of this kind of scholarship. In the next issue, three articles from the Chairman of the Joint Chiefs of Staff and Secretary of Defense Essay Competitions will be featured.

—D.H. Gurney

Vehicle is destroyed as part of post-blast crime scene demonstration

U.S. Air Force

Law Enforcement Technology, Intelligence, and the War on Terror

By **M. E. BOWMAN**

The warfare that most of us trained for now seems likely to become more an artifact of historical interest than the reality we feared. Today, the objective of conflict is less to obtain a political outcome than to create the conditions necessary for stability and responsible participation in international affairs. Perhaps the most striking difference from the war that Carl von Clausewitz spoke of is that today's conflicts have no time horizon. Still, there are constants; one is the requirement for intelligence concerning the enemy.

History illustrates that intelligence is a critical element of success in conflict. Even so, when military conflict encompasses transnational threats that include terrorism, insurgency, organized crime, weapons proliferation, and weapons of mass destruction—all of which inevitably invite the complications of public corruption—intelligence takes on a new meaning and generates requirements unknown a few years ago. The reasons are many, with technology at the top of the list.

Even though intelligence remains a critical element of warfare, it is startlingly apparent that the Department of Defense (DOD), even with a vast array of intelligence capabilities, is not able to produce and analyze all the vital information necessary. In an era when the enemy is supported globally and transnational capabilities for communications, financial transactions, and transportation confound the utility for direct application of force, civilian agencies are key to obtaining vital elements of information for the success of the mission.

Indeed, modern technology has greatly improved the combat capabilities of the American fighting forces. Network-centric warfare is a significant technological advancement and a proven way of fighting both more efficiently and more safely. However, the object is no longer merely to win the fight. Today, the object is to win the peace, which means creating conditions that will lead to stable societies. For that, partnering the technologies and capabilities of law enforcement, particularly those found within the Federal Bureau of Investigation (FBI), with the military mission is necessary. Coupling the innovations and skills discussed in this article with true cooperation between civilian law enforcement and the U.S. military will undoubtedly lead to a more effective prosecution of the war on terror.

Communications

Advances in communications technology have made our lives more convenient, but they have also provided the means for terrorists and criminals to communicate more easily. Twenty years ago, cellular telephones were relatively rare, clunky, and inefficient. Today, they are marketed to grade-school children. Cell phones and satellite phones are used by terrorists just as commonly as they are by organized crime members. What does

M.E. "Spike" Bowman is a Senior Research Fellow in the Center for Technology and National Security Policy at the National Defense University. Previously, he served in the Senior Executive Service at the Federal Bureau of Investigation.

this mean? Take a clue from organized crime: The FBI has stated many times that the defeat of organized crime on the U.S. east coast could never have been accomplished without electronic surveillance. The same is true of terrorism, but the task is now infinitely more difficult because of not only cell phones but also the Internet.

Members of al Qaeda may live in caves, but many of them are sophisticated and learned. Using skills unimagined only a few years ago, al Qaeda has set a standard for terrorists by embracing the Internet as a tool for organizing, training, and propagandizing. Although the Internet is not new, improvements in computer, communications, and storage technology have made it a medium of choice for networking, information-gathering, and anonymous activities. Moreover, it is so cheap—often free—that anyone can use it.

Using the skills of modern technocrats, al Qaeda has adopted online tactics that mirror its offline techniques for evading discovery. These tactics include instant messaging, chat, bulletin boards, and a constantly shifting collection of Web sites where propaganda can be posted. For example, in 2005, a Web server operated by the Arkansas highway office was hijacked and used to distribute 70 files, including videos featuring Osama bin Laden. Recently, a group believed to be al Qaeda's Web-based propaganda arm debuted a weekly state-of-affairs Web cast and is reportedly searching online for recruits to aid with the coverage. This means that the group and their recruits will be searching for more and more computers to hijack in order to distribute additional content.

Officials of all nations are faced with the prospect of choosing between sabotaging terrorist uses of the Web (commonly referred to as "whack-a-mole") or attempting to monitor them. Neither option yields a satisfactory response. On the one hand, nearly anyone can put up Web sites. On the other, monitoring the Web is like counting grains of sand on a beach, so vast are the opportunities and methods of communication over the Internet. Moreover, if the choice is to monitor, it begs the questions of who can do it and who has authority to do it.

The largest Internet providers are located in the United States. Hotmail and Yahoo! offer unlimited free accounts. Terrorists can, and do, use the Internet extensively, undoubtedly changing their free accounts as often as practicable. A terrorist in Pakistan can log into a Yahoo! account in the United States and communicate with a networked terrorist in Jordan. Chat rooms, instant messaging, anonymizers, and other attributes of modern communications make the life of a terrorist much more flexible. However, monitoring email requires a judicially approved warrant. This means that the military must depend on law enforcement, perhaps even that of many nations, to bring in that part of the intelligence puzzle.

using the skills of modern technocrats, al Qaeda has adopted online tactics that mirror its offline techniques for evading discovery

Iraqi man in custody fingerprinted at Camp Fallujah, Iraq

U.S. Marine Corps (Louis Corwise)

DNA Testing

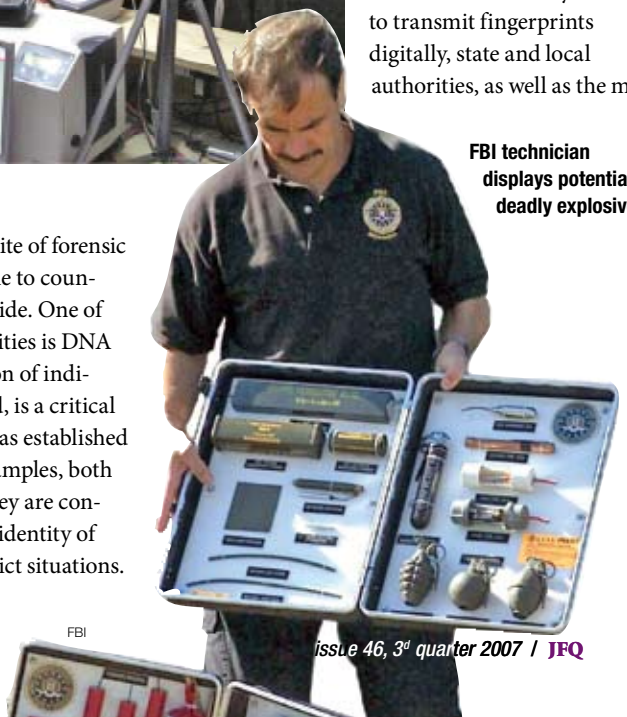
The FBI has a large suite of forensic capabilities that are germane to counterterrorism efforts worldwide. One of the most important capabilities is DNA testing. Precise identification of individuals, both alive and dead, is a critical need. To this end, the FBI has established a large inventory of DNA samples, both to identify persons when they are confronted and to confirm the identity of bodies resulting from conflict situations. For example, DNA testing confirmed a claim by the Pakistani government that Muhsin Musa Matwalli Atwah, an al Qaeda operative wanted by the United States in connection with the 1998 U.S. Embassy bombings, had been killed in an airstrike by Pakistani forces near the border with Afghanistan.[1] On the other side of the world, FBI DNA testing confirmed the death of the Philippines' "most wanted" terrorist.

However, as valuable as this identification capability is, there are more subtle uses for DNA. For example, even though the body of Abu Musab al-Zarqawi was identified by fingerprints, tattoos, and scars after he was killed in an airstrike, DNA samples were sent to the FBI crime laboratory in Quantico, Virginia. The DNA collected was then compared to other samples in an effort to help establish locales where al-Zarqawi had been and who had been with him.

Fingerprints

One of the most common forensic capabilities is fingerprinting.[2] The FBI maintains an Integrated Automated Fingerprint Identification System (IAFIS), which comprises the largest biometric database in the world. It contains the fingerprints and corresponding criminal history information for more than 47 million subjects in the criminal master file. This information is submitted voluntarily by state, local, and Federal law enforcement agencies.

With the ability to transmit fingerprints digitally, state and local authorities, as well as the mil-



FBI technician displays potentially deadly explosives

FBI

itary abroad, can send prints for comparison and receive electronic responses to criminal 10-print fingerprint submissions within 2 hours and civilian fingerprint submissions within 24 hours. The ability to identify suspected terrorists and insurgents in Iraq and Afghanistan is a highly desirable capability. As early as April 2002, the Attorney General directed that terrorist fingerprints and biographical data be gathered internationally from military detainees, from cooperative international exchange programs, through legal attaches in Embassies abroad, and from domestic law enforcement sources. As of September 1, 2006, more than 19,000 such prints had been added.[3]

Today, when the U.S. military rounds up suspected terrorists, they are "booked" and fingerprinted, using the same tools that police in the United States use to check criminal backgrounds. Consequently, if those fingerprinted subsequently attempt to enter the United States, they will be flagged. When a large group was rounded up in 2004 in Iraq, 44 were determined to have criminal records in the United States and 2 were sought on Federal warrants.[4] In 2005, the Department of Defense created its own biometric database, the Automated Biometric Identification System (ABIS), modeled on IAFIS. To ensure quality and interoperability of all fingerprint data collected, DOD has directed that all acquisitions related to fingerprinting must conform to the same standards and be interoperable with the IAFIS system.[5]

today, suspected terrorists are "booked" using the same tools that police in the United States use to check criminal backgrounds

Now, prints sent to ABIS are sifted through IAFIS, where they are screened and compared to the FBI's most-wanted terrorists lists.[6] The value of that screening has been demonstrated several times when suspects were detained after their fingerprints showed they had been arrested before. In one case, suspected al Qaeda terrorist Mohamad al Kahtani was positively identified based on prints taken when he was denied entry to the United States in August 2001.

Improvised Explosive Devices

More deaths in Iraq are caused by improvised explosive devices (IEDs) than anything else. Additionally, IEDs have become the weapon of choice for terrorists worldwide. To address this threat, in December 2003, the FBI created the Terrorist Explosive Device Analytical Center (TEDAC). This center established a single Federal program responsible for the worldwide collection, complete forensic and technical analysis, and timely dissemination of intelligence regarding terrorist bombs. All information gleaned from TEDAC's analysis is shared throughout the law enforcement, intelligence, and military communities.

Additionally, using breakthrough technology, FBI technicians are beginning to identify the locales where the devices are made and even who is making them.[7] According to a 5-year accounting of FBI progress in transformation, 56 bomb-makers were identified through TEDAC analysis.[8] These analyses suggest that there is a relatively small number of master bomb-makers, and those identifications have resulted in the capture of some, while others who were identified are being sought.

The FBI also runs a Large Vehicle Bomb Post-Blast Crime Scene School that replicates a 2002 bomb blast overseas that killed more than 200 people. Students do not watch the explosion; they pick up the actual pieces from the scattered wreckage that set the forensic groundwork for a criminal or terrorist investigation. They then learn how to identify the vehicle that blew up.

The post-blast school started as a basic lesson on working a car-bomb scene—from forensics and equipment to crime scene mapping and processing—but it evolved to a graduate level curriculum in 1998, so law enforcement and military investigators with plenty of bomb-scene experience can get practical training in the devastation created by large-vehicle explosions.

The FBI has sponsored more than 70 classes around the Nation—and 2

U.S. Navy (Jim Watson)

Agents examine Pentagon after terrorist attack

overseas—since the school was launched in 1998. The size of the explosions limits where the course can convene; a 6,000-pound bomb, for example, might spread a field of evidence across 225 acres. Fortunately, the U.S. military has provided bases with huge barren acreage for the classes and even vehicles to blow up. Bomb technicians deploying to Iraq and Afghanistan get first crack at the maximum 50 slots in each class.

Financing

The technology that allows us to pay our bills online or send money to a child at college also permits the transfer of funds to or between terrorists. If those funds can be stopped short of their ultimate goal, the means to finance the terrorist fight against military forces can be curtailed. To do so, however, requires investigations at a great distance from the battlefield and often involves the authorities of several nations. It also requires information developed in the conflict zone—information that may be best recognized and evaluated by law enforcement personnel. However, the situation is complicated for two reasons. First, money laundering is not illegal in most nations. Second, and of immense importance, transactional data are not required to "follow the money." That means anonymous transfers of money are both possible and likely.

Where do authorities have to look to find the sources of terrorism financing? Donors, nongovernmental organizations, and criminal enterprises all fund terrorist causes. The Detroit U.S. Attorney's Office recently indicted a Hezbollah smuggling ring operating in Michigan that helped fund that terrorist organization with profits from bootlegged cigarettes, counterfeit tax stamps, phony Viagra tablets, and stolen toilet paper, according to a Federal indictment unsealed in Detroit in July 2006. A similar Hezbollah ring was prosecuted in North Carolina in 2003.

Other terrorist supporters in the United States have been indicted for credit card fraud, smuggling blue jeans, and currency violations. Moreover, just as with terrorism itself, terrorism financing is global. According to the Canadian agency responsible for tracking money laundering, Canada's suspected financing for terrorism almost tripled to C$180 million (US$153 million) in 2005.[9] In the United States, a Federal judge found two U.S.-based Islamic charitable organizations and an individual fundraiser liable for the 1996 killing of an American in Israel by Hamas terrorists. The Islamic Association for Palestine and the Texas-based Holy Land Foundation were both found liable for funneling money to Hamas.[10]

Battling such sources of terrorist support is a universal task—and one that yields information at every turn. The need is to exploit that information. In November 2005, more than 180 experts from 55 countries met in Vienna to consider the problem. Attendees included specialists from the North Atlantic Treaty Organization, United Nations Office on Drugs and Crime, U.S. State Department, and the Organization for Security and Cooperation in Europe.[11]

Closer to home, U.S. intelligence agencies, including those of the Department of Treasury and FBI, have been adopting innovative forms of investigation to deal with the issue. For example, the Terrorist Financing Operations Section (TFOS) of the FBI Counterterrorism Division was formed in response to this critical need. TFOS combines traditional FBI expertise in conducting complex criminal financial investigations with advanced technologies and has built on these established mechanisms by obtaining cooperation and coordination among law enforcement, regulatory, and intelligence agencies, both domestic and foreign, to become an internationally effective terrorist financing investigative operation. The mission of TFOS has evolved into a broad strategy to identify, investigate, disrupt, and dismantle all terrorist-related financing and fundraising activities. Following the money can lead to an individual relevant to the military mission abroad.

following the money can lead to an individual relevant to the military mission abroad

Weapons of Mass Destruction

If it is true that we are in for a long, drawn-out struggle against terrorism, the chance of avoiding another event involving weapons of mass destruction (WMD) grows slimmer. The difficulty of obtaining or developing chemical, biological, or nuclear weapons has made their use rare, but these weapons have been used for terror purposes. Sarin, a chemical nerve agent, was used in the Tokyo subway system in 1995 by the Aum Shinrikyo cult. Anthrax bacteria were used in 2001, infecting individuals in Connecticut, New York, Florida, and the District of Columbia. Also, salmonella bacteria were used by the Rajneeshee cult in 1984 in an attempt to influence local election turnout in Oregon. Ricin, a toxin, was mailed to the White House in 2003 and Congress in 2004.[12]

Domestically, there is a significant opportunity to control access to materials that contribute to WMD. Federal law enforcement agencies now have greater power to gather intelligence on terror groups and their members. Increased information about groups, combined with apprehension of any who have chemical or biological weapons, may create further barriers to terrorist acquisition and use of these weapons. A registration system for researchers and facilities possessing select agents has been developed by the Department of Health and Human Services, and additional restrictions regarding access to these agents have been made law.

Internationally, the picture is far murkier. Where terrorists find haven, they can seek the means of destruction they desire. It is known that terrorists have experimented with chemical and biological materials, most likely without significant success. Furthermore, most chemical and biological agents are difficult to apply with the precision that would be desirable to induce terror. However, chemical, biological, radiological, and nuclear weapons are themselves harbingers of fear, so it is almost beyond cavil that terrorists will seek and use them if possible.

Although there is repeated evidence of terrorist interest in chemical weapons or chemically enhanced explosive devices, available information suggests that this is more a reflection of jihadist aspiration than an indication of genuine capability. Nevertheless, jihadist Web forums contain manuals describing the construction of gas dispersal devices. Also, in late 2001, videos discovered in Afghanistan purported to show the testing of hydrogen cyanide gas on dogs.

This category also has to take into account the possibility of a "dirty bomb." There are no truly accurate historical events that give us an idea of what the effect of a dirty bomb might be. However, there is a relevant event in which a tragic radiological accident occurred in Brazil between September 1987 and March 1988. An abandoned radiotherapy clinic was burglarized, and a capsule

containing Cesium-137 chloride was opened and handled by several individuals. From this incident of common burglary, over 112,000 people were potentially exposed. After careful monitoring, it was determined that a total of 249 people had been contaminated. Of these, 151 exhibited both internal and external contamination and 49 were admitted to hospitals, with the most seriously irradiated having doses from 100 to 800 rads (radiation absorbed dose). The contaminated patients were themselves radioactive, seriously complicating their treatment. In the end, 28 suffered radiation burns, and 3 men, 1 woman, and 1 child died.[13]

Far more problematic is the potential use of conventional explosives or other easily obtained materials to create a WMD event. Not unlike the idea of turning fuel-laden aircraft into WMDs, a conventional explosive at a chemical plant or a dam could wreak massive destruction. When household items, fertilizer, or castor beans can be turned into WMD devices, it is not governments, with all their capabilities, that are likely to detect the threat. Rather, it is local policemen, storekeepers, tourists, and ticket agents who are the eyes and ears of prevention. If terrorism is to be prevented, then any theory of transformation has to take into account all those who have a role in prevention.

U.S. Air Force (Roy Santana)

Decontamination facility set up after simulated chemical attack during Exercise Seahawk

Terrorist Screening Center

The Terrorist Screening Center (TSC) is a unified watch list of known or appropriately suspected terrorists that can be used by every official sworn to protect the United States—from border patrol and transportation officials to Federal agents and local police officers working their beats. "There is one watch list," TSC Director Donna Bucella told reporters during a briefing at FBI headquarters. "Our list is not a stagnant list. We add, modify, and delete every day."[14] The information that flows into the TSC comes from the FBI (domestic terrorist information) and the National Counter Terrorism Center (international terrorist information), which gets information from more than a dozen intelligence agencies, such as the Central Intelligence Agency and the Department of Homeland Security, under the umbrella of the Director of National Intelligence.

By serving as the day-to-day, 24-hour conduit that links frontline law enforcement, and even foreign officials, to critical field intelligence on terrorists, the TSC staff can do more than maintain the database and link phone calls. Their access to a constant flow of intelligence helps them assemble a big picture view of potential threats and connect the dots for the agencies they support.

Preserving Information

Precisely because contemporary threats have no time horizon, carefully preserving information becomes an important intelligence capability. For example, what does it mean to find a telephone number in a country without telephone books? Phone numbers in other countries can be traced through law enforcement channels. Additionally, law enforcement agents have provided training to U.S. military personnel on how to exploit "pocket litter."[15] Moreover, it is a normal function of the FBI to build up dossiers, often with fingerprints and increasingly with DNA, on every potential criminal or terrorist.[16]

In the battlespace, law enforcement officers have aided military enterprises by applying law enforcement skills to data, tangible objects, and interrogations of individuals. They have photographed, catalogued, and organized items as they would for evidentiary purposes, thereby preserving the integrity of the items for future reference. Moreover, they have applied their skills operationally, providing interpretation of information that often has been instrumental in helping the military know how and where to next apply force.

Of significant importance, the FBI has developed and maintains the Investigative Data Warehouse (IDW), a centralized, Web-enabled closed system repository for intelligence and investigative data. This system allows appropriately trained and authorized personnel throughout the country to submit queries relevant to investigative and intelligence matters. Information contained in IDW comes from all agencies of government and, more importantly, from information picked up on the battlefields of Iraq and Afghanistan. This is a constantly growing database.

IDW now provides special agents, intelligence analysts, and members of Joint Terrorism Task Forces with a single access point to more than 47 sources of counterterrorism data, including information from FBI files, other government agency data, and open source news feeds, that were previously available only through separate, stovepiped

law enforcement officers have aided military enterprises by applying law enforcement skills to data, tangible objects, and interrogations

systems. New analytical tools are used across multiple data sources providing a more complete view of the information possessed by the Bureau. Users can presently search up to 560 million pages of international terrorism-related documents and billions of structured records, such as addresses and phone numbers, in seconds. They can also rapidly search for pictures of known terrorists and match or compare the pictures with other individuals in minutes rather than days. Coupled with sophisticated state-of-the-art search tools, the IDW enhances governmental ability to identify relationships across cases quickly and easily.

It is a simple fact of contemporary life that the current security environment presents unique and difficult issues that few of us have trained for. Even leaving aside the complexities of stabilization and reconstruction, addressing the direct threat requires the expertise and technological capabilities of law enforcement agencies, both in the conflict arena and at great distances, in order to terminate or restrict support to terrorism. Moreover, the effective utilization of law enforcement capabilities requires the cooperation of networks of not only law enforcement organizations but also military organizations across the globe. **JFQ**

NOTES

[1] Henry Schuster, "One of FBI's 'Most Wanted Terrorists' confirmed dead," October 24, 2006, available at <www.cnn.com/2006/WORLD/asiapcf/10/24/alqaeda.operative/index.html>.

[2] A more complete explanation of the utility of fingerprinting in the war on terror can be found in Paul J. Shannon, "Fingerprints and the War on Terror: An FBI Perspective," *Joint Force Quarterly* 43 (4th Quarter, October 2006), 76–82.

[3] Federal Bureau of Investigation (FBI) Web site, International Operations, available at <www.fbi.gov/aboutus/transformation/international.htm>.

[4] FBI Web site, Headline Archives, "Protecting America from Terrorist Attack: War Zones link to FBI's Fingerprint Database," available at <www.fbi.gov/page2/june05/iafis062705.htm>.

[5] Robert S. Mueller III, FBI Director, before the House of Representatives Committee on Appropriations, Subcommittee on Science, State, Justice, and Commerce, September 14, 2005.

[6] Ibid.

[7] CBS News, "Forensics ID Bomb Makers in Iraq: FBI Uses Breakthrough Forensics to Track Homemade Bombs," January 17, 2006, available at <www.cbsnews.com/stories/2006/01/17/evening-news/printable1216945.shtml>.

[8] FBI Web site, Headline Archive, "What's New in the FBI? A Five-Year Accounting," September 15, 2006, available at <www.fbi.gov/page2/september06/testimony091406.htm>.

[9] Alexandre Deslongchamps, "Canadian Financing for Terrorism Triples to C$180 Million," Bloomberg, November 4, 2005.

[10] The ruling is the first to hold American organizations responsible for damages for terrorist acts committed overseas and opens a new window for the use of civil suits to stop the flow of funds to terrorist organizations. Whether the ruling is a watershed or an aberration that opens the door to frivolous law suits is yet to be seen. See Hilary Leila Krieger, "U.S. charity found liable for Hamas attack," *Chicago Tribune*, November 14, 2004. Additionally, the Holy Land Foundation has since been dismantled and officers of the organization are under indictment for material support to terrorism.

[11] Henry Crumpton, the U.S. State Department's counterterrorism coordinator, stated that at least US$150 million in terrorism funding has been intercepted worldwide, and millions more—in cash or other resources—has been stopped in transit or at borders. See Susanna Loof, "Battling terrorist financing helps map terrorist networks, experts say," Associated Press, November 9, 2005.

[12] Dana A. Shea, "Terrorism: Background on Chemical, Biological, and Toxin Weapons and Options for Lessening Their Impact," Congressional Research Service, Order Code RL31669, December 1, 2004, available at <www.fas.org/irp/crs/RL31669.pdf>.

[13] Peter D. Zimmerman and Cheryl Loeb, *Dirty Bombs: The Threat Revisited*, Defense Horizons 52 (Washington, DC: National Defense University Press, January 2004), available at <www.ndu.edu/ctnsp/defense_horizons/DH38.pdf>.

[14] Statement by Donna Bucella, Director of the Terrorist Screening Center, March 15, 2006, available at <www.fbi.gov/page2/march06/tsc031506.htm>.

[15] Law enforcement officers are well aware that the items a person carries on him have significance to the person. It may be a phone number, a matchbook from his favorite bar, or the address of a girlfriend. All of this "pocket litter" tells a story about the person and his habits and will often lead to useful intelligence.

[16] When the United States invaded Afghanistan, it was agents of the FBI's New York field office who were the most knowledgeable about al Qaeda and who were able to provide information to military forces who were picking up people on the battlefield.

Troops receive intelligence briefing before Mosul raid

U.S. Air Force (Vanessa Valentine)

Technology, Intelligence, and TRUST

By **JAMES R. HOWCROFT**

The outcome of the conflicts that the American military is likely to fight in the decades ahead will increasingly depend on tactical success and the empowerment of small unit leaders. Recent advances in technology have the potential to improve the intelligence collection and dissemination capabilities of tactical military units. Unfortunately, perceptions about who "does" intelligence and the role and responsibilities of intelligence collection, analysis, and dissemination threaten to limit the warfighting potential of intelligence technology on the battlefields of the 21st century. A mindset change is required to maximize the evolving capabilities of modern technology.

Cold War Intelligence Paradigm

During the Cold War, much of our intelligence collection was centralized at the national level and focused on strategic targets, which were seen as the key to victory against conventional armed forces. Cold War targets were generally static sites, such as headquarters, missile silos, airfields, or railroad marshalling yards. Intelligence collection was prioritized to provide accurate targeting data and follow-on bomb damage assessment on these targets for manned and unmanned airborne weapons platforms. The requirements of ground-based tactical and operational level intelligence consumers were only of secondary importance; units at this level were not critical to success. Victory was won or lost at the strategic level.

Strategic level headquarters naturally determined the target sets for this Cold War intelligence collection. Units at the operational or tactical commands could input collection requests, but these requests required validation by every headquarters in the command hierarchy prior to arrival at the national tasking level. The requirements of a unit lower in the hierarchy could be trumped by anyone higher in the chain. In this process, tactical units had little or no visibility. Transparency did not exist to allow a tactical consumer to determine easily when or if his requirement would be collected.

Ironically, the tactical commander who had the most pressing need for the greatest resolution of the battlefield had the least ability to access or influence the centralized intelligence collections architecture. In 2003, following the invasion of Iraq and the capture of Baghdad and Tikrit, the 1st Marine Division in its official after-action report noted, "The Byzantine collections process inhibited our ability to get timely responses to combat requirements. . . . The existing hierarchical collections architecture is wildly impractical and does not lend itself to providing timely support to combat operations."[1]

Sadly, much of this Byzantine bureaucracy is with us still today. In addition to the burden of competing with every unit above him in the collections chain, the tactical consumer must depend on a collections hierarchy to push critical intelligence down to him rapidly in an accessible, relevant format. The tactical consumer is dependent on those above him in the distant headquarters who carried out the collection and analysis of the raw data to understand and appreciate his

Colonel James R. Howcroft, USMC, serves as the U.S. Marine Corps Chair and Military Professor of International Security Studies at the George C. Marshall Center for European Security Studies in Garmisch-Partenkirchen, Germany. He is a career Intelligence Officer.

specific information needs. If the tactical consumer were successful at precisely describing his requirements days ahead of time and in a manner and method that were understandable to the analyst conducting the "readout" of the collection data, he might just be fortunate enough to receive a useful product.

While Service-centric intelligence is a step in the right direction, the military consumer is still U.S. Central Command or U.S. European Command headquarters in Tampa or Stuttgart, respectively (at least in the eyes of the distant national level intelligence agencies), not an infantry battalion on the Syrian border. The distant analyst often has little visibility or understanding of exactly why the tactical consumer is asking for the information, the impact of the data, or how to package the information so it is actionable for the ground commander.

For example, if the tactical consumer in his formalized collections request asks for information regarding the presence of armored vehicles at a given set of coordinates, the analyst looks for and reports on that particular informational request at that specific place—not on the implied request for trafficability, presence of an artillery battery 10 kilometers away, or the presence or absence of a bridge or tactical fortifications. The communications connectivity and permissions rarely exist for a direct and timely dialogue between the tactical consumer and the distant analyst to define and refine the evolving needs of the consumer.

Once in combat, the needs of tactical intelligence consumers are time-sensitive and can rarely be supported by a hierarchy dependent on the flow and validation of information and permission up the chain of command and then back down this same chain once the intelligence has been collected and analyzed. This is not to say that national level collection is never responsive to tactical consumers, but information passed down to the consumer in a timely manner is still a rarity that requires an almost serendipitous convergence of adequate time, an analyst at the collections level who precisely understands the stated and implied requirements of the tactical user, no interference by higher headquarters to trump the tactical request, and adequate communications means.[2]

the tactical commander who had the most pressing need for the greatest resolution of the battlefield had the least ability to access or influence the centralized intelligence collections architecture

In the past, tactical units were perceived—and perceived themselves—primarily as consumers of intelligence, not producers. Intelligence in this hierarchical model was seen as a commodity produced at higher headquarters (HHQ), which controlled the assets, validated and prioritized the intelligence requirements, and was then responsible for disseminating down the hierarchical chain the intelligence that it determined tactical units needed. During my career as an intelligence officer, I was told on numerous occasions, "Trust us, when the balloon goes up, you'll get all the intelligence you need." Intelligence was something that one went to HHQ to receive. Since HHQ owned and controlled intelligence, the (natural) perception within the hierarchy was that HHQ had the most accurate picture of the chaotic battlefield. This has led to a mistaken and misdirected concept that a relevant and accurate intelligence "common operating picture" can be produced at a senior headquarters and pushed down to a tactical unit.

Soldiers gather intelligence during Baghdad raid

U.S. Army (Tierney Nowland)

Evolving 21st Century Requirements

The dynamics of the current battlefield have changed the intelligence paradigm. This is true regardless of whether the foe is a conventional or an asymmetrical threat. While few conventional foes exist to challenge the American military now, those that do exist are defeated not by attrition but by our attacking their cohesion as a military entity. While part of this effort to destroy enemy cohesion entails attacking "traditional" fixed targets, such as headquarters buildings, airfields, or logistics nodes, speed at the tactical and operational levels is increasingly a weapon to be wielded against conventional or asymmetric foes. Success depends on the tactical commander quickly recognizing and immediately exploiting fleeting opportunities as they present themselves on the battlefield. These opportunities are most often visible only to engaged commanders, not to distant HHQs far removed from the battlefield.

This high operational tempo requires, indeed demands, informed decisionmaking on the spot by lower level units. The present hierarchical collection and dissemination chain is too slow and cumbersome to provide intelligence that is relevant and actionable to the tactical commander. While it is possible to reach back for information (intelligence pull) or for this information to be pushed down the hierarchical chain of command (intelligence push), intelligence must be "personalized" to be relevant for the battlespace

of each commander. Even military units in the early stages of defense transformation engaged in battle against symmetrical foes have outgrown the archaic system's capability to provide them with relevant, actionable intelligence on the battlefield. In March 2003, for example, once the 1st Marine Division crossed the Iraq-Kuwait border, "the Division received very little actionable intelligence from external intelligence agencies."[3] National level collection and dissemination systems were unable to keep pace with the dynamic environment—even against a symmetrical conventional foe. The national level system was hard at work but lacked an appreciation for the tactical situation on the ground and could not convert collected information into actionable intelligence.

success depends on the tactical commander recognizing and immediately exploiting fleeting opportunities

While the conventional military forces of foes such as China and North Korea still pose an ominous threat, the more likely scenarios for military employment are in counterinsurgency and stabilization operations. The 2006 Quadrennial Defense Review Report notes that "irregular warfare has emerged as the dominant form of warfare confronting the United States" and directs that future warriors "be as proficient in irregular operations, including counterinsurgency and stabilization operations, as they are in high intensity combat."[4] More so than the conventional wars of the past, counterinsurgencies and stabilization operations are fought at the tactical level. Tactical success may not equate to strategic victory; indeed, tools wielded by other agencies and departments are now often of greater importance in achieving strategic success, however defined.

What is clear is that strategic success is not the result of the destruction or capture of a single objective or individual. Capturing and killing Saddam, killing his sons, or killing Abu Musab al-Zarqawi have not led to victory in Iraq. Capturing or killing Osama bin Laden will not end the war on terror or result in victory in Afghanistan. Shock and awe do not apply. The target set is not there. As seen in Afghanistan in 2001, the ability to destroy headquarters or bridges or crater airfields is irrelevant in fighting the asymmetrical foe. Destroying fixed nodes is not only irrelevant; it also is counterproductive during counterinsurgency or stabilization operations.


Marine configures Trojan Lite satellite communications system

An important factor to consider when weighing current intelligence requirements is the fact that Soldiers will increasingly be deployed within growing urban sprawl. The current ability to collect intelligence using strategic assets in this environment is limited. While it may be possible to image individual buildings with great resolution, we still cannot see who is inside, whether he is armed, or if he is hostile. It requires a man on the ground to go into the building or to communicate face-to-face with the inhabitants of the neighborhood to collect and evaluate the intelligence. Even if it were possible with technology to determine that certain individuals within an individual building were hostile,

U.S. Marine Corps

striking urban targets with strategically controlled weapons carries with it the likelihood of civilian destruction and death.

If the point of the main effort is increasingly likely to be at the tactical level, then the intelligence focus also needs to shift to reflect this evolved paradigm. A shift in intelligence focus entails not only a reorientation in collection tools, intelligence manning, and analysis that is responsive to and supportive of the tactical commander, but also a deeper shift regarding intelligence responsibility and trust within the command hierarchy and the Intelligence Community.

Talking about intelligence in this new environment is impossible without first addressing communications. Intelligence and communications are inextricably linked. Technology is moving to fill the capability gap regarding high-bandwidth communications to dispersed tactical users. Advances in the ability of tactical units to be part of a wider information network hold great promise. Larger amounts of data can be moved faster, and tactical units have an enhanced capability to receive and send information via the communications network. Fortunately, the headquarters of tactical units are generally static during counterinsurgency and stability operations, which allows them access to the common communications network that they would lack if on the move in a conventional fight. Networked systems have the potential to allow widely scattered units within the hierarchy to have simultaneous access to intelligence. With the proper permissions, tactical, operational, and strategic consumers can pull required information from throughout the network and tailor the product to meet their own specific intelligence needs.

Decentralized Focus and Tools

Tactical commanders require decentralized collection tools that respond immediately to their needs. The belief that a few capable centralized national systems alone are able to meet the needs of the tactical consumer is flawed. Regardless of the technological capability of the collection platform, a tactical commander must still battle the collection validation bureaucracy and can still be trumped by anyone in his chain of command. The tactical commander needs his own intelligence collection toolkit to complement the national systems. This toolkit could include small-scale unmanned aircraft systems and unmanned ground vehicles that are simple and rugged enough to be operated by Soldiers and Marines, not contractors.

networked systems have the potential to allow widely scattered units within the hierarchy to have simultaneous access to intelligence

The Dragon Eye system, for instance, launched by a bungee cord and controlled via a laptop computer by a single Marine with an afternoon of training, is an example of a tactical collection tool with limited range, but one that is still responsive and can see over the next hill to provide "eyes-on" intelligence. Small seismic intrusion detectors, backpack ground surveillance radars, miniature motion sensors, and remote video cameras are

examples of the technology that exists today that must be placed in the hands of tactical commanders to help prevent tactical surprise. While technology of this type is valuable, it is important not to lose sight of the fact that the ultimate collection tool is a culturally attuned, language-capable Soldier or Marine who appreciates the context of the tactical environment in which he employs these tools. The investment should be in tactical systems to support this collector—not on national systems, more data infrastructure, or more buildings manned by analysts located far from the fight.

Similarly, intelligence collection teams attached to tactical units need to understand the requirement to provide immediate support to the tactical commander. Fortunately, human intelligence and signals intelligence collections teams operating in a tactical commander's battlespace now accept that their primary and immediate focus of collection and dissemination should be the local unit. It is unacceptable for reporting and the collection "take" to be passed up the chain of command and only be pushed back down to the tactical consumer after it has been analyzed and "massaged." By this time, the information has lost relevance or is so sanitized to protect its source that it has become worthless. The teams need to focus on time-sensitive, actionable intelligence to the tactical commander rather than on collecting information to be entered into a national level database. Fortunately, with contemporary networked communications, it is possible to have multiple addressees on a single email or message. The collections team does not have to make an either/or decision about whom to send its intercept or interrogation report to (either the battalion in whose battlespace the team is located or its higher headquarters). Now it can do both simultaneously.

additional tools, databases, and increased connectivity do not replace intelligence professionals at the tactical level

Similarly, an analyst at a facility removed from the tactical battlespace must have an appreciation of which time-sensitive information is relevant and actionable for the local commander. He must then be aware of which units are responsible for particular battlespaces so he knows specifically whom to include on his dissemination list when he transmits perishable intelligence. With the communications tools available today, pushing an intelligence product up the chain of command without immediate dissemination to the affected tactical unit is irresponsible. Unit boundaries and the hierarchical chain of command must not become barriers and impediments to time-sensitive support to those on the ground. Informal networks and peer cross-talk can serve to work around these artificial unit-based barriers, but peer cross-talk should supplement and refine regular reporting, not substitute for it.

This type of responsive, responsible collection and dissemination, which maximizes the capabilities of networked communications, depends on collectors being trusted by higher headquarters and granted the authority to disseminate their products directly to the tactical user as well as the wider community, without validation or "scrubbing" by a hier-

U.S. Marine Corps (Patrick Johnson-Campbell)

Marine collects short-range reconnaissance data

U.S. Marine Corps (Kenneth Madden)

Marines operate ground-control station for Dragon Eye unmanned aircraft system

archy seeking to ensure completeness or conformity with the assessments of a senior headquarters. When provided with a larger share of raw intelligence, the tactical consumer must be trusted not only to safeguard the specific capabilities of intelligence platforms (that is, sources and methods) but also to understand that raw intelligence data is often contradictory or wrong and may require corroboration before action. But it is, in fact, often the tactical commander, with an intimate knowledge of his battlespace and therefore the best understanding of the environment, who is best suited to corroborate and provide the proper context for the raw data.

Intelligence Manning Implications

If indeed the intelligence focus of effort is at the tactical level, then intelligence manning should reflect this fact. Tactical units currently lack adequate manning in their intelligence section to conduct a counterinsurgency campaign or to conduct stability operations for months at a time—24 hours a day, 7 days a week. A tactical commander equipped with his own organic collections tools will find his intelligence section quickly overwhelmed. Additional tools, databases, and increased connectivity do not replace intelligence professionals at the tactical level; on the contrary, they actually demand a personnel increase. Indications are that many tactical commanders in Iraq have dealt with this issue by shifting Soldiers and Marines from other table of organization billets into their intelligence sections.

The intelligence support teams provided to the tactical commander must be, as much as possible, attached early enough before deployment to give the supported unit and the intelligence attachments the time to develop a habitual relationship and build trust and confidence within the team. Commanders and staffs process information and intelligence in different ways and at different speeds. Prior to deploying, a commander must be able to see the capabilities of his organic and attached intelligence assets to understand their applicability and utility. He needs to know in advance just what their footprint is and what support requirements they entail. Prior to the invasion of Iraq in 2003, Trojan SPIRIT LITE communications systems and remote receive stations for unmanned aircraft systems were attached to several regiments in the 1st Marine Division. While planning and coordination were done ahead of time, transportation and logistics issues delayed their attachment with the regiments until the last minute. Predictably, the results were disappointing. In some cases, the regiments, faced with competing time and attention requirements, never had the chance to work through the difficulties involved in assimilating unfamiliar new systems and people. It is important to build cohesion, trust, and communication prior to the stress and rigor and fatigue of combat. Once attached, every attempt should be made to keep the tactical intelligence team together, rather than "robbing Peter to pay Paul" in response to emerging requirements or a perceived crisis elsewhere.

Responsibility and Trust

This shift to an increased tactical focus entails a transformation in the concept of intelligence responsibility and trust on the battlefield. No longer do senior headquarters have the most accurate view of the critical battlefield. The tactical commander, immersed 24/7 in the cultural nuances of his local environment, is now, more than ever, in possession of the most accurate picture of the battlefield. It may be only a small piece, but just as operational success is an accumulation of tactical successes, so is an accurate intelligence picture at the operational level an accumulation of smaller, accurate intelligence pictures from below. Having this information entails a responsibility for tactical commanders, armed with additional collections tools and analytical capability, to paint a relevant, precise picture for everyone else, including the other players and actors present on the contemporary battlefield. This reporting from the tactical level can then be used by analysts throughout the hierarchy to develop a tailored intelligence product for their respective commanders and staffs. The tactical commander now can, and must, send his reporting throughout the wider communications network.

senior commanders and their staffs need to step back from the tactical battle and focus on the war at their particular level

This paradigm entails a change in the trust relationship within the hierarchy. Previously, tactical commanders and intelligence officers relied on their higher headquarters to provide them needed intelligence. Now, HHQ must trust their subordinates to portray the battlefield. The immediate higher headquarters in the hierarchical chain has to trust its subordinate to input intelligence into the network that will be accessible and visible to all. If the raw intelligence reporting from

the tactical commander has to be routed or cleared by HHQ prior to dissemination, the advantage is nullified. Higher headquarters, in turn, has to be trusted not to second guess and micromanage tactical commanders and must accept that lower level commanders know what is best within their zones. They must understand that their role is to assign the mission, provide commander's guidance, prioritize the required resources—and then step aside.

Empowerment is a term loosely thrown around. True empowerment is HHQ entrusting tactical commanders with authority and assets to assess the situation locally and do what needs to be done to accomplish the assigned mission. Once they have entrusted their subordinates, higher headquarters must resist the temptation to intervene. Communications and collection advances have made it possible for distant senior commanders and their staffs to monitor, in real time, the tactical or operational situation in their subordinate units. This ability to view is not necessarily the same as the ability to understand; the context is missing. Due to the hierarchical nature of the military, most commanders previously have held the job of their subordinates. This tendency, combined with the increased ability to monitor and communicate directly to subordinates throughout the chain of command, compounds micromanagement. Just because a senior headquarters has increased connectivity, it does not mean that exercising that capability is the right thing to do.

Senior commanders and their staffs need to step back from the tactical battle and focus on the war at their particular level, rather than interfering in their subordinates' domain. Subordinates have to be trusted to do what needs to be done within their battlespace to achieve the mission assigned by their HHQ. Despite talk of empowerment, interference and micromanagement are, unfortunately, increasingly the norm. An example of this micromanagement was the order in March 2003 to I Marine Expeditionary Force (I MEF), while it was attacking toward Baghdad, to divert a brigade from the point of main effort to deal with Iraqi divisions along the Iranian border on the MEF eastern flank. The Iraqi divisions had long been a focus of the I MEF, who had conducted an in-depth risk assessment, continually refined and updated this assessment, and concluded that the Iraqi divisions were adequately addressed by information operations, airstrikes, and persistent surveillance sufficient to provide early warning should the divisions decide to leave garrison. Distant commanders, viewing the battlefield without the context, directed the diversion of precious ground combat power to attack Iraqi divisions that were already out of the fight.[5]

As the ability to gather information has grown, staffs at military headquarters have grown to keep pace with the perceived need to manage the information. Subordinate headquarters are overwhelmed with the need to "feed the beast"—to satisfy the voracious need for information to fill in a box on a briefing slide for a staff officer's portion of his commander's daily update. Just as the subordinate must be empowered and trusted to portray the situation relevant to his battlespace, the subordinate must trust his senior headquarters to exercise discipline not to micromanage the ongoing fight or overwhelm the subordinate with requests for nonessential data. It is difficult to exercise this discipline. The concept of "need to know," as currently employed, is most often used by a senior headquarters to limit information or intelligence to a subordinate. Is it unreasonable for this concept to work both ways? Is it unreasonable for a subordinate to ask his higher headquarters what it would do differently if the subordinate provided HHQ the requested information?

It is difficult for well-intentioned senior officers merely to observe and not interfere. It is extremely difficult in our hierarchical military for a staff officer to tell his boss, "General, I decided our headquarters won't access the video feed from the unmanned aircraft system for today's raid; our need to monitor isn't as important as the requirement of the battalion conducting the operation. If everyone logs into the site to monitor the mission, it slows down video feed to the battalion conducting the raid."

In this first decade of the 21st century, we have seen advances in technology that have the potential to provide the military commander with an unparalleled ability to monitor and collect intelligence on the battlefield. The questions become how to use this technology and which technology to buy. Based on the wars we will probably fight and our contemporary doctrine, it seems clear that there is a need to develop a number of smaller, decentralized collection systems rather than depend on a few, more capable systems managed and directed by a distant centralized hierarchy. To be effective, this decentralized intelligence collection demands continued development of the communications network to tie together tactical, operational, and strategic reporters and consumers.

This decentralized technology must be combined with a mentality shift that stresses that intelligence is something that everyone does. Everyone is a collector, and intelligence is not something delivered from above. Hand in hand with technological advances, there needs to be a realization of the vital human factor involved in order to maximize the technological potential. This human factor is trust: it is the trust to empower a subordinate and depend on him to complete his mission and fulfill his intelligence collection and reporting requirements. It is the trust of a subordinate in his higher headquarters that he will be given the tools and latitude to accomplish his mission without interference, second-guessing, and endless data requests from his higher headquarters. Without the effort to develop and maintain this trust, modern militaries will fall short in maximizing their potential. **JFQ**

NOTES

[1] 1st Marine Division, "Operation Iraqi Freedom (OIF): Lessons Learned," May 29, 2003, available at <www.globalsecurity.org/military/library/report/2003/1mardiv_oif_lessons_learned.doc>.

[2] One such success was the ability of lead regiments within the 1st Marine Division, via attached Trojan SPIRIT LITE communications systems, to reach back to the National Geospatial-Intelligence Agency (then the National Imagery and Mapping Agency) Web site to access accurate and timely intelligence on Iraqi ground forces hours prior to attacking across the Iraq-Kuwait border to capture the Rumaliya oilfields and associated national oil infrastructure in March 2003.

[3] 1st Marine Division.

[4] *Quadrennial Defense Review Report* (Washington, DC: Department of Defense, February 6, 2006), 36.

[5] Personal experience and observation by the author. For additional detail of this episode, consult Michael R. Gordon and Bernard E. Trainor, *Cobra II: The Inside Story of the Invasion and Occupation of Iraq* (New York: Pantheon Books, 2006).

Soldiers search home for weapons and contraband, acting on intelligence gathered from local Iraqis

1st Combat Camera (Suzanne Day)

Eyes on Target

Intelligence Support to an Effects-based Approach

By **JAMES B. ELLSWORTH**

The value of an effects-based approach has been recognized since the days of Sun Tzu, but the war on terror has reinforced the central role of effects in achieving victory. Whether fighting a country such as Saddam Hussein's Iraq or a nonstate adversary such as al Qaeda, traditional attrition warfare is unlikely to be strategically effective simply because opponents are likely to shun courses of action built around the kind of center of gravity that can be readily located and exposed to U.S. military might. Effects-based operations (EBO) attempt to transform America's warfighting doctrine to fit this world, where military supremacy over likely opponents is not realistically in doubt, yet where victory depends on the ability to wield (or restrain) that supremacy in synchronization with the other instruments of power toward common policy objectives.

The road to EBO, however, has been far from straight. Early skeptics skewered EBO as requiring the ability to see inside the enemy commander's mind, a concern that supporters largely answered by focusing on the concrete end of the effects spectrum. In turn (somewhat paradoxically), this has prompted other critics to dismiss EBO as either overly mechanistic or little different from traditional practices. Recently, the trend is for proponents to go to great lengths to paint EBO as revolutionary, downplaying its relationship to operational art and restricting any connections made to the enduring principles of war to perhaps the occasional soundbite attributed to Clausewitz or Sun Tzu,[1] while opponents charge that it ignores—and may even be incompatible with—such traditional wisdom.[2]

This odd dance around the issue of what actually persuades an enemy to give up has drawn scant clarity from recent operations, as evidenced by the lackluster response to a concept of operations billed for Iraq as "shock and awe." Yet the Iraq operation produced the stated objective of "regime change" without requiring attrition of a large proportion of the enemy force or the collateral damage typically associated with attrition warfare—a distinction frequently listed as an advantage of EBO.

Such conflicting impressions highlight another critical shortfall—metrics—both at the practical level, for assessing the extent to which a desired effect has been achieved, and at the doctrinal level, for testing the hypothesis that the investments an effects-based approach requires will enhance military effectiveness. At their respective levels, these represent gaps in critical information required by commanders if an effects-based approach is to work. As such, they require evolution of the intelligence system.

What follows suggests, first, that commanders must widen the focus of priority intelligence requirements (PIR) supporting an effects-based approach beyond traditional issues of military capabilities and intent (especially on "personalities" and "cultural" intelligence) and increase the focus of battle damage assessment (BDA) on detecting the systemic or psychological effects noted above. Second, it asserts that a key part of the value added by an effects-based approach is its application of the proven methodology of joint intelligence preparation of the battlespace (JIPB) to aid in these efforts beyond the purely military dimension of operations. Third, it explores the reconceptualization of the intelligence team that these developments require—to include issues surrounding enhanced interagency collaboration.

This article explores the evolving effects-based approach and identifies

Dr. James B. Ellsworth is Professor of Online Education at the U.S. Naval War College.

challenges and requirements for effective implementation. It then examines existing or emerging tool sets that may help answer these requirements. Finally, it derives general recommendations for an intelligence system that keeps "eyes on target." If the utility of shock and awe has been limited by the issues that EBO critics note—and if those issues, rather than being insoluble, can be addressed by a refocused intelligence system—then an effects-based approach can become a critical enabler for victory.

EBO and Intelligence: An Analysis

Notwithstanding the controversy over the feasibility of an effects-based approach, some themes are notable for their prevalence among proponents and skeptics alike. Its dependence upon a robust intelligence capability in general—and a greatly expanded ability to "get inside the heads" of enemy leadership in particular—is one such theme.

This theme in itself is not especially unusual; just as the roots of effects-based thinking can be traced back (at least) as far as Sun Tzu, so too can its relationship to detailed knowledge of the adversary—the latter, in fact, provides the best known Sun Tzu soundbite: "Know the enemy and know yourself; in a hundred battles you will never be in peril."[3] This wisdom also informs current U.S. doctrine. In particular, Joint Publications 3–13, *Joint Doctrine for Information Operations*, and 3–53, *Doctrine for Joint Psychological Operations*, address such knowledge, if largely as a matter of targeting those specific types of operations. When drawing on these publications, however, one should remember that such understanding—when one is thinking in effects-based terms—can be equally useful in planning a kinetic attack to stimulate desired effects.[4]

Curiously, though, another theme on both sides of the debate is lack of confidence in the ability of America's intelligence systems to deliver on this requirement—or at least lack of a clear understanding of how to get there from here. Together, these two themes hold key ramifications for the effects-based debate. Most particularly, if a plausible road map can be laid out, perhaps the debate itself can move from whether an effects-based approach is a solid operational concept to how the obstacles standing in the way of its implementation can most effectively be addressed.

This does not suggest that an automated analysis tool or even bona fide cultural experts will ever offer the commander a predictive certainty. Rich psychological and sociological data can seldom be reduced to terms from which a mathematical formula can derive a "right answer." Yet "qualitative" does not imply a lack of validity—or prevent the analyst from legitimately representing subjective data in "quantified" terms to facilitate systematic assessment. Staff officers exercise complex qualitative judgments during course of action comparison—using numerical ratings to represent their professional (subjective) assessments of the weight and value of the decision criteria—and the military is no stranger to "red-amber-green" characterization of everything from unit readiness to PIR status (essentially a quantification of subjective judgment on a three-point scale). In both cases, the culture readily accepts both the validity of the judgments themselves (based on faith in the professional competence of those making them) and the use of quantified representations to convey the bottom line. The inability to achieve a reductionist precision should no more deter the commander and his staff from leveraging competent cultural and psychological intelligence in effects-based planning than from employing these more familiar tools.

the trend is for proponents to go to great lengths to paint effects-based operations as revolutionary

In fact, the safeguards that will allow the joint force commander and his staff to reap the benefits of an effects-based approach without falling victim to a false sense of certainty are the familiar tenets of the military decisionmaking process and its supporting processes. The staff should not construct a linear plan based on the assumption that friendly actions will produce the desired effects (and only the desired effects), but rather should try to incorporate branches to minimize disruption and regain the initiative if events unfold in other ways.

A similar approach should be applied to the problem of assessment. Just as the prudent commander will want coverage of indicators that could suggest that a key kinetic BDA was incomplete or erroneous, so too should the plan incorporate indicators and sequels to address gaps or errors in nonkinetic effects assessment. Likewise, just as the chance of error and oversight does not prevent the commander from basing decision points on kinetic BDA, neither should it dissuade him from leveraging assessment of nonkinetic effects in his decisions.

For the intelligence function in particular, these safeguards are inherent in an effects-based approach. On close examination, it is clear that its system of systems analysis (SoSA) is built on the proven (and generalizable) methodology of JIPB. Just as JIPB expanded on the accepted intelligence preparation of the battlespace process to examine the military dimension from the perspective of all Services, SoSA expands on JIPB to connect and analyze all political, military, economic, social, informational, and infrastructure (PMESII) dimensions and to apply this analysis to "unaligned" as well as friendly and adversary systems.

This "systems perspective" is made explicit in the new *Commander's Handbook for an Effects-Based Approach to Joint Operations*,[5] which both depicts it in a figure[6] and describes the "SoSA-enhanced JIPB" process in an outline that will be familiar to all military intelligence professionals.[7] The *Commander's Handbook* has taken an important step toward emphasizing the criticality of these issues and suggesting approaches for addressing them. Yet it raises as many questions as it answers, with many details remaining vague and little explanation of how the manpower bills accompanying its recommendations are to be resourced within the combatant commands.

While the increased emphasis the effects-based literature places on "nodes" and "links" may remain less comfortable, this merely attaches concrete terms that facilitate a systems view of the battlespace to considerations already inherent in JIPB. For example, a force engaged in counterinsurgency, when conducting JIPB, would likely have taken notice of a fuel storage facility that was believed to be supplying the insurgents and assessed its effects on friendly and adversary courses of action. By systematically identifying battlespace elements in terms of nodes and links, though, it decreases its chances of overlooking that same facility's role in supplying fuel to local farmers, schools, and hospitals for whom traditional responses of destroying the facility or even imposing stronger access controls might pose significant hardship, alienating the populace.

In a more permissive environment such as disaster relief, the same principles apply. For example, if food distribution for a particular region was predominantly handled by a given facility—and that facility was decimated by the disaster—systematic node/link analysis would highlight that relationship, enabling the assisting U.S. or multinational force to identify a critical vulnerability to essential services in that region. Once again, a key part of the value added by an effects-based approach lies in broadening application of validated intelligence and planning methods to consider PMESII dimensions (and effects) beyond the military.

Further confidence can also be drawn from the historical experiences of other disciplines that have had to cope with the complexity of human thought and emotion. Education scholars were once baffled by the problem of assessing the causal relationship between a teaching "event" and actual learning in the student's mind. The pioneering work of B.F. Skinner overcame this obstacle by embracing the notion of the "black box." At the practical level, one does not need to see what is happening inside the mind of the student (the ability to peer inside the black box) if students exposed to the teaching event consistently retain observable behaviors not previously present.[8] On this foundation, later researchers constructed a sophisticated understanding of human learning, which is now being validated at the level of cognitive neuroscience. Starting with a similar premise (one need not be able to see into the mind of the enemy if he consistently shows a link between observable behaviors and certain effects), it may be possible to identify next steps toward more rigorous effects-based models by reviewing the historical path taken by educators as they moved from Skinnerian pragmatism to today's more robust models of learning.

That being said, several key challenges remain to implementing an effects-based approach as it is currently envisioned. Perhaps foremost among these is the absence of disciplinary expertise associated with these new intelligence demands on Joint Task Force and geographic combatant command staffs. Shortfalls in some of these fields—such as human intelligence, cultural expertise, and language skills—are commonly recognized. Yet other factors—despite their oft-cited roles in various missteps in Iraq—have received much less attention. Five years later, John Shanahan's call for inclusion of "the psychologist, psychiatrist, sociologist, or religious expert"[9] remains largely unheeded.

A second, related challenge is manning the myriad boards, centers, and cells supporting an effects-based approach. Such intensive manpower requirements are especially problematic for a developing concept that—by definition—offers scant evidence on which to judge whether the gains from that investment justify it. U.S. Joint Forces Command, in the *Commander's Handbook*, states confidently that "gaining a sufficient systems perspective may take more time and consume more resources up front, but ensuing planning, execution, and assessment should yield greater effectiveness and efficiency throughout the remainder of the operation,"[10] yet at this stage this is little more than an untested hypothesis.

Recommendations

Several actions should be taken to improve the ability of the intelligence system to support an effects-based approach. The most critical of these fall into three categories: "foundational"; associated with either SoSA-enhanced JIPB or BDA; and "guiding." Taking these actions now will enhance the commander's ability to target the adversary's will to resist, sway unaligned groups toward the friendly desired endstate, and safeguard friendly mission effectiveness. Of equal importance, it will facilitate the intelligence staff's assessment of the degree to which such desired effects have been achieved (and undesired effects avoided)—together with identification of unanticipated second- or third-order effects, thereby supporting timely selection of subsequent friendly actions to exploit or mitigate the results.[11]

Foundational actions will help acquire and institutionalize the expertise necessary to analyze and interpret data from the nonmilitary PMESII dimensions, especially cultural and psychological data, for either planning (JIPB) or assessment (BDA). In the near term, the commander and his intelligence staff should reach out to the interagency community. Counterparts within organizations likely to have been engaged in a country well

982d Combat Camera (Olarrewaju Akinwumi)

2d Communications Squadron (Stephen Otero)

Above: Iraqi colonel and intelligence officer plan raid on a weapons cache with help from U.S. Army Military Transition Team trainers. Right: Air Force tactical air control team reviews intelligence collection from previous day's missions

before the military instrument is called upon to operate there may have "a long history and understanding of the culture in which a military operation will take place,"[12] including the psychology and personalities of that culture's leaders. Integrated into the planning and intelligence staffs (perhaps as part of a National Intelligence Support Team[13] or within the Joint Interagency Coordination Group[14]), these experts may supply the very ability "to know any other nation, leader, or people in the requisite detail to anticipate behavior"[15] that much criticism of an effects-based approach has simply assumed to be out of reach.

Institutionalization of this solution requires reconceptualizing the intelligence team at the operational level, to incorporate such expertise organically to the joint force—now increasingly an interagency force—as it goes to war. This must go beyond merely absorbing interagency personnel to contribute to the accomplishment of military effects; ideally, it should translate into equal enhancements to the efforts of other agencies to leverage a systems view as they identify their own nodes and links, pursue desired nonmilitary effects, and assess their success at achieving them. Perhaps most important, it should facilitate country team efforts to ensure that all U.S. Government organizations pursuing the same national policy objectives coordinate their efforts from a shared understanding of the PMESII environment.

Longer-term action on this recommendation might include targeted recruiting, into a more broadly conceived foreign area officer corps, of a limited number of (for example) second-generation immigrants representing each nation of the world, educated in the profession of arms (and perhaps in intelligence), who would maintain in-depth language/cultural understanding, be trained and practiced in thinking like their nation's leaders/people, and specialize in advising commanders on the cultural and psychological issues of effects-based planning and assessment.

In the JIPB area, intelligence staff training must routinely incorporate—even if only via reachback—collaboration with interagency partners whose responsibilities lie in the same region, and should prepare J2 (Intelligence) personnel and their counterparts to:

- know the value of cultural and psychological understanding and other nontraditional expertise to a SoSA-enhanced JIPB process—that is, JIPB applied to all PMESII dimensions
- know sources for such expertise organic to the joint force, across the interagency community, and even outside government
- facilitate integration of that expertise into effects-based planning and assessment functions.

Over and above its facilitation of an effects-based approach, incorporation of this expertise would enhance the practice of traditional operational art by discouraging mirror-imaging and increasing the likelihood of identifying the enemy's center of gravity as he sees it—and not as the friendly commander would see it were the situation reversed.[16]

experts may supply the very ability "to know any other nation, leader, or people in the requisite detail to anticipate behavior" that much criticism of an effects-based approach has assumed to be out of reach

Commanders and staffs should also look outward to other disciplines to identify developments that might assist in JIPB for an effects-based approach. For example, Gary Klein has studied critical decisionmaking among firefighters and emergency medical services personnel, as well as "pilots, nurses, military leaders, nuclear power plant operators, chess masters, and experts in a range of other domains."[17] While his research aims to identify and develop competencies and conditions that help experts make good decisions, understanding of his findings by warfighters employing an effects-based approach might be of equal use in planning kinetic or information operations to undermine or degrade those competencies or conditions in an adversary system to increase the likelihood of its leaders making bad decisions.

This provides an apt segue into the next set of recommendations, those pertaining to "psychological BDA." Here, the task is monumental but critical: a wholesale retooling of intelligence support to BDA.[18] Analysts in existing disciplines must understand the indicators that suggest progress toward the critical types of psychological effects collectible by their intelligence and must become proficient at their detection. For example, signals intelligence analysts might be able to diagnose dissolving command and control when an adversary who consistently favors high levels of personal control over his military during crisis suddenly stops communicating with the field (or when spurious traffic from units seeking direction abruptly spikes).

Integration of new skill sets within the intelligence staff may also be in order. Among the most promising possibilities here is the pioneering adaptation of the discipline of movement analysis described by Brenda Connors.[19] In contrast to traditional profiling, which is specific to each individual and can take years, this technique—based on "hard-wired" behaviors common to all humans—can discern a subject's general psychological state in real time, and much more if the analyst can study historical footage. With the omnipresence of television—and with the increasing reliance on the information instrument of power by America's adversaries—it would be a rare enemy leader who does not appear regularly in some video format to his followers or the world and who has not been doing so for long enough for the media to have an extensive collection of recorded appearances to serve as a baseline. Related work includes Paul Ekman's research on "facial micro-expressions,"[20] and theoretical support for such techniques is available from the field of neurolinguistic programming,[21] which involves analysis of word choice, eye movements, and similar indicators.

A final recommendation in this area involves development of intelligence doctrine supporting an effects-based approach. One cannot read the *Commander's Handbook* without sensing the ease with which a SoSA-enhanced JIPB process could overwhelm the intelligence staff. A closer read will suggest some techniques for modulating the required level of effort. Its JIPB section specifies steps to "determine the relevant OE [operational environment] systems" and to "identify the amount of OE detail *required and feasible within the time available*" [emphasis added], yet little guidance for making these critical

judgments exists at this stage. Until this gap is addressed, commanders may wish to apply traditional criteria, beginning at their own level of responsibility and working up and down as time and resources permit (trusting other echelons to do likewise, contributing their respective insights to the shared situational understanding).[22]

Finally, in the "guiding" category, commanders and their J2s should collaborate to identify new types of PIRs that capture what is most critical for the commander to know about the other PMESII dimensions, and about the personalities and psychological states of key enemy leaders and what mechanisms might be available for manipulating or assessing them. What friendly actions—kinetic or otherwise—would be most likely to interfere with those leaders' abilities to make good decisions, to induce psychological paralysis, or to achieve other nonkinetic effects? What cultural attitudes, values, or beliefs are central to the adversary's will to resist—at the national leadership level, among the military, or among the people—and what in these categories might offer a critical vulnerability for attacking that will? Effects-based planning thrusts these "social science questions" concerning coercion and capitulation (and the paucity of validated theory surrounding them) squarely into the arena of the military professional.[23]

Note that this guidance must be tied to the other recommendations detailed above. Good PIR will be of no use if the intelligence staff—or outside resources they can tap—lack the capabilities and tools with which to answer them. At the same time, those capabilities and tools will sit idle if the commander establishes only the traditional military "capabilities or intentions" PIRs with which he has grown comfortable throughout his career.

Those seeking to implement these recommendations must remember that there are other cultures to be considered: those of the Joint Task Force or geographic combatant command staffs, the warfighter, and the Intelligence Community,[24] as well as the myriad cultures of the interagency community. Each is built upon a long history of doing things well—albeit often in different ways—and can be expected to offer some resistance to change. It is thus especially critical that those analyzing lessons learned from exercises and operations establish metrics and collect and analyze data to test the hypothesis that making the investments that an effects-based approach requires will enhance operational and strategic effectiveness.

While doing so will clearly impose an additional burden on already taxed organizations, its results will either validate the hypothesis, providing hard data justifying the force structure enhancements necessary to execute an effects-based approach; or, refute the hypothesis altogether, allowing senior leaders to adjust course without waste of additional resources; or, partially refute the hypothesis, providing hard data supporting development of doctrine to help leaders scale down the effects effort to fit within the time and resources available. Failure to do so leaves proponents and skeptics of an effects-based approach equally unarmed in the intellectual debates needed to shape the concept.

Those leading the effort must devote careful attention to well-informed persuasion and to helping these cultures grow together to meet the challenge that lies ahead. The new intelligence focus needed to keep an effects-based approach's eyes on target does not ask the warfighter to rely on blind faith—only to absorb new types of analysis into the intelligence process—and to trust the familiar tools that continue to serve him well. **JFQ**

NOTES

[1] Harlan K. Ullman, "Slogan or Strategy? Shock and Awe Reassessed," *The National Interest* 84 (Summer 2006), 43–49.

[2] Milan S. Vego, "Effects-Based Operations: A Critique," *Joint Force Quarterly* 41 (2d quarter, April 2006), 51–57. See also Ralph Peters, "Bloodless Theories, Bloody Wars," *Armed Forces Journal* (April 2006), 34–36. Ironically, Vego argues that an effects-based approach is too mathematical and concrete, paying inadequate attention to the "unquantifiable" or "intangible" factors that he identifies as critical to operational and strategic success, while Peters argues that effects-based thinking is too fuzzy and abstract, paying inadequate attention to what he claims to be a fundamental reality, that "only killing wins wars."

[3] Sun Tzu, *The Art of War*, trans. Samuel B. Griffith (Oxford: Oxford University Press, 1963), 84.

[4] Kevin D. Admiral, "Effects-Based Operations: Enhancing Operational Art and Design in the 21st Century" (master's thesis, Joint Forces Staff College, 2005), 46–47.

[5] U.S. Joint Forces Command, *Commander's Handbook for an Effects-Based Approach to Joint Operations* (Norfolk, VA: U.S. Joint Forces Command, February 24, 2006), available at <www.dtic.mil/doctrine/jel/other_pubs/eb_handbook.pdf>.

[6] Ibid., figure II–1.

[7] Ibid., II–7, II–8.

[8] David R. Krathwohl, *Methods of Educational and Social Science Research* (New York: Longman Press, 1993), 634.

[9] John N.T. Shanahan, "Shock-Based Operations: New Wine in an Old Jar," *Chronicles Online Journal* (October 2001), n. 33, available at <www.airpower.maxwell.af.mil/airchronicles/cc/shanahan.html>.

[10] *Commander's Handbook*, II–12.

[11] Stephen P. Perkins and John D. Jackson II, "Effects-Based Operations and Its Enabling Capabilities in Expeditionary Warfare," *Military Intelligence Professional Bulletin* 30, no. 3 (July-September 2004), 18.

[12] Cynthia G. Efird and Carl T. Sahlin, "Using the Information Instrument to Leverage Military Force: A Need for Deliberate Interagency Coordination" (research paper, National War College, 1994), 39.

[13] Bruce O. Lankford, "Know the Enemy: Expanded Use of Leadership and Cultural Profile Data in Operational Planning" (research paper, U.S. Naval War College, 2001), 17.

[14] Perkins and Jackson, 16.

[15] James L. Boling, "Rapid Decisive Operations: The Emperor's New Clothes of Modern Warfare," in *Essays 2002: Chairman of the Joint Chiefs of Staff Strategy Essay Competition* (Washington, DC: National Defense University Press, 2002), 50.

[16] Lankford, 4.

[17] Gary Klein, *Sources of Power: How People Make Decisions* (Cambridge: Massachusetts Institute of Technology Press, 1998), 1.

[18] Edward C. Mann, Gary Endersby, and Thomas R. Searle, *Thinking Effects: Effects-Based Methodology for Joint Operations*, CADRE Paper No. 15 (Maxwell AFB, AL: Air University Press, 2002), 67–78.

[19] Brenda L. Connors, "No Leader Is Ever Off Stage: Behavioral Analysis of Leadership," *Joint Force Quarterly* 43 (3d quarter, October 2006), 83–87.

[20] Sharon Jayson, "Facial Expert's Ability to See Deception Has Him in Demand," *USA Today*, July 23, 2005.

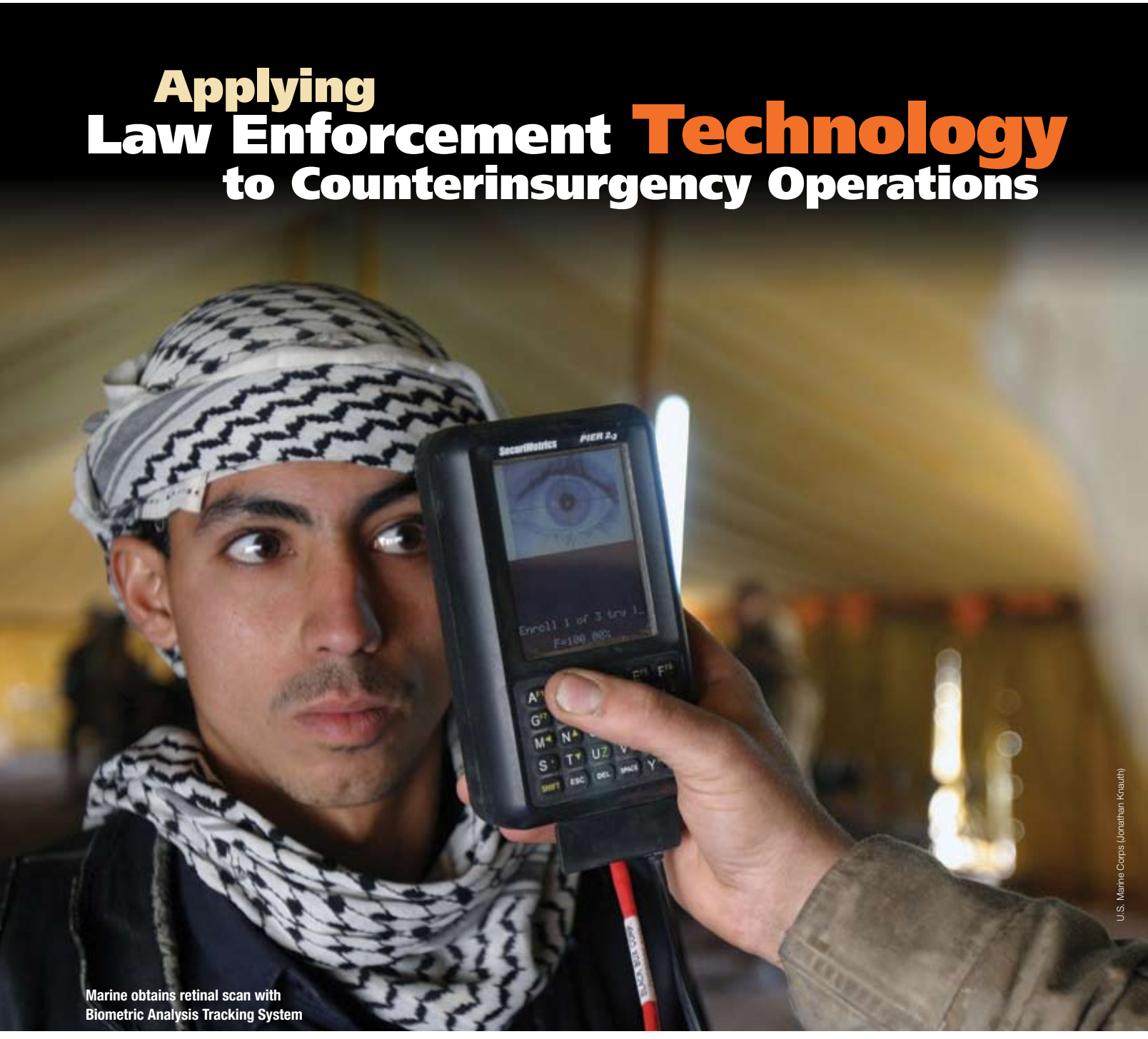
[21] Lankford, 21.

[22] See *Commander's Handbook*, figure II–2, for evidence that this solution was anticipated.

[23] Robert A. Pape, *Bombing to Win: Air Power and Coercion in War* (Ithaca, NY: Cornell University Press, 1996), 322–323, 329–330.

[24] Dennis M. Nagy, "A Military Intelligence Knowledge Base and Knowledge Management: Cultural Factors," *Defense Intelligence Journal* 9, no. 1 (2000), 41.

Applying Law Enforcement Technology to Counterinsurgency Operations



U.S. Marine Corps (Jonathan Knauth)

Marine obtains retinal scan with Biometric Analysis Tracking System

By GILES KYSER, MATT KEEGAN, *and* SAMUEL A. MUSA

Colonel Giles Kyser, USMC, is Military Assistant to the Assistant Secretary of Defense for Special Operations and Low Intensity Conflict. Matt Keegan is a Visiting Fellow in the Center for Technology and National Security Policy (CTNSP) at the National Defense University (NDU). Dr. Sam Musa is Senior Research Fellow in CTNSP at NDU.

In 1994, Rudolph Giuliani assumed duties as the mayor of New York, taking over a city with one of the highest crime rates in America—a problem he promised to address. To meet this challenge, he expanded the number of police officers on his force, surged them to neighborhood beats, and enabled them to overcome unfamiliarity with the local geography and demography by arming them with information technology solutions, providing each

beat cop with a type of "virtual longevity" normally requiring months to develop.[1]

Half a decade later, a similar situation faced the Chicago Police Department. Chicago also leveraged information technology effectively, surging the "equivalent of 300 officers on the street."[2] The Chicago system, the Citizen and Law Enforcement Analysis Reporting (CLEAR) system, created this "virtual surge" and arguably contributed to an unprecedented drop in violent crime within Chicago. At the time (October 2005), the *Chicago Sun-Times* noted that "Chicago officials and academics have credited the city's murder decline to police targeting of gangs, drugs, and guns."[3]

The parallels between the problems experienced by two major cities where gang violence, organized crime, and illicit financing overwhelmed local security forces, and the challenges facing our coalition forces in Iraq, are striking—as is one potential tool to address those challenges.

In 2007, Iraq and Afghanistan find themselves torn by insurgency, sectarian violence, and terrorism. Instead of gang violence, warlords, tribes, sectarian death squads, and terrorist cells dominate urban landscapes akin to New York and Chicago. Instead of drugs alone, terrorist financing includes narcotics, extortion, and highly developed financial networks using porous borders and symbiotic affiliations to protect major actors. Instead of just guns, the forces arrayed against the coalition include improvised explosive devices and heavy weapons. In an especially chilling development, insurgent efforts not only continue but also increasingly extend across the borders between the two countries where thugs, terrorists, and opportunists support the chaos serving as a foundation for their individual causes.[4]

In this violent no man's land between those contending for power sit our forces and the Iraqi populace whom we have sworn to protect. Our rotating, shifting, and surging forces are unable to develop their situational awareness rapidly enough to penetrate the insular demographic within which the terrorist operates, and the Iraqi people are unable to expose the enemy from within that demographic. The terrorists swim within familiar waters, not as another fish—as Mao might describe—but as predators ready to devour anything threatening their existence.

Background

Two key phrases mentioned above comprise the foundation for potential crossover of police techniques into counterinsurgency operations: *insular demographic* and *situational awareness* (SA). For the Solider in Al Anbar and the cop in Chicago, the ability to peer through the insular demographic—to know who is who, who belongs, and who does not; to see through disguises or aliases—unlocks the door to basic security. Similarly, strong situational awareness—the ability to recognize the presence of the abnormal or absence of the normal—provides an indispensable and intuitive warning mechanism.

A closer look at four factors preventing our forces from developing the intuitive and concrete sensing necessary to penetrate an enemy's defenses lends to understanding why law enforcement technology may provide a unique solution.

Force Rotation. Without technical enhancements, units require 30 to 60 days of consistent presence to develop comprehensive SA in an area in order to gauge conditions, patterns, and personalities for intuitive force protection and defensive operational effectiveness. Exploiting that SA in an offensive manner requires longer periods within one region. According to Servicemembers recently returned from in-theater, force rotations within a specific region vary from as short as 8 to 10 weeks to as long as a full rotation, depending on conditions on the ground and the requirement to reinforce success or

parallels between the problems experienced by two major cities, where gang violence, organized crime, and illicit financing overwhelmed local security forces, and the challenges facing coalition forces in Iraq, are striking

Iraqi police discuss daily patrol

1st Combat Camera Squadron (Andy Dunaway)

prevent failure—as in Baghdad today, where forces from other parts of the country moved to the capital to saturate the area of operations. Fire brigade operations such as this within a region will predictably result in some degree of defensive SA but will arguably fall short of the offensive SA necessary to challenge the enemy.

Demography/Language Unfamiliarity. Even after developing intuitive capabilities and a degree of SA, coalition forces' inability to speak the language and discern nuances of demographic patterns limits the discriminative application of force contributing to winning over the populace. In other words, a local will know by accent, dress, or actions that someone is not from that area. Accordingly, unless teamed with a local, trusted, and uncorrupted informant network or an attached military translator, coalition forces will have little to no idea who they are encountering, and the enemy will be able to continue to hide in plain sight and intimidate those they draw their anonymity from while friendly units inadvertently offend, inconvenience, and humiliate potential allies.

Insurgent/Terrorist Mobility. Highly porous borders between Iraq and Afghanistan and their respective neighbors, combined with interprovince mobility and geographic tribal striations, significantly challenge coalition force capability to limit movement of terrorist/insurgent forces. Internal examples such as residents of Mosul arrested in Takrit, of Afghani fighters in Iraq, or even the arrest of a foreign fighter once detained on the Afghanistan-Pakistan border in the United States highlight the problem coalition forces face every day.[5]

Detainee Movement Requirements. Following the Abu Ghraib incident, political pressures created the impetus for the implementation of new detainee transfer processes. Unless significant reason is established at the battalion level permitting extended interrogation, detainees must transfer to the next higher echelon facilities within a short time. Command policy sets that period, and the enemy remains well aware of it by virtue of information gathered from those released. Currently employed technology does not allow the squad/checkpoint to have a clear detain/do not detain choice because certain technology only exists at the battalion level and higher, and even then only through cumbersome processes with latency constraints. Squad/checkpoint level confirmation, aside from a lucky hit on a watch list, is rare. The operational requirements of such immediate transfer, and the limited insight into detainee history at the point of encounter (the checkpoint or arrest point), effectively limit actual opportunities for detainee interrogation and information exploitation to only that which is gathered beyond the 18-hour window. Discussions with regional veterans indicate that the aforementioned limitations are known by the insurgents, terrorists, and criminals.

With this knowledge, insurgents, terrorists, and criminals understand that waiting the prescribed period closes the coalition force's limited window of opportunity to exploit their capture. The window closes because informal and formal communications methods warn a detainee's associates, who then "go to ground." The highly perishable intelligence that a detainee may possess decays by the time higher headquarters interrogates the suspect. More importantly, those within the detainee's network go into hiding as the fact of detention becomes apparent. In effect, the process cycle time itself suboptimizes the coalition forces' ability to act on perishable intelligence.

Having examined the four factors preventing friendly ability to develop situational awareness in an offensive manner, we need to look at solutions that might help overcome those constraints. Police methods such as those used in Chicago could assist our forces in executing missions in Iraq and Afghanistan, but for this analysis, we focus on a simple police information technology solution. Biometric technology attached to a transactional database utilizing existing communications infrastructure could create a virtual surge extending the effectiveness of the individual warrior or policeman and lifting the burden of exposing the terrorist from the populace. Biometrically exposing an enemy heretofore invisible to the Western eye and protected by those around him whom he intimidates into silence offers the way to penetrate the insular demographic. Such a police solution could help to create a more secure environment for the Iraqi and Afghan people.

A Northrop Grumman proprietary system—the Biometric Automated Toolset (BAT)—provides the foundation for a technological enhancement to the current environment in Iraq and Afghanistan. However,

> *perishable intelligence that a detainee may possess decays by the time higher headquarters interrogates the suspect*

BAT currently is not available at the checkpoint/squad level, so important information is not in the hands of those who need it most: the Soldier or Marine on the checkpoint. Conversely, when one considers systems such as the one currently used in Chicago, the technological answer seems simple. But we must examine whether such successfully applied capabilities can overcome encounter-point demographic challenges, as well as the constraints imposed by rotation-driven SA

Soldier enters data gathered from patrol with Iraqi police

982d Combat Camera (Tierney Nowland)

limitations, insurgent and terrorist mobility, and detainee movement requirements.

Because many of the tactical level operations currently conducted by coalition and Iraqi forces more closely resemble police work than traditional warfighting, adopting police techniques may help overcome stability and support operations problems. The conventional force-on-force operations for which the world's (and our) militaries were designed ended within months in Afghanistan and Iraq, and force requirements migrated toward constabulary and counterinsurgency capabilities. Many conventional units found themselves functioning in a police role for which they were untrained and ill equipped. Likewise, Iraqi security forces (to include police), whose local knowledge and cultural familiarity provide instant SA, cannot yet assume full responsibility for such operations. Consequently, coalition forces continue to conduct nontraditional, nonconventional missions within a culture whose willingness to accept policing by outsiders is problematic at best.

CLEAR and Associated Techniques

Juxtaposing this background with the success of the Chicago Police Department initiative drives our problem statement: How can the integration of police database and biometric identification capabilities improve stability and support operations in Iraq and Afghanistan?

Modern American metropolitan police forces leverage information technology to overcome deficiencies in actionable intelligence when prosecuting law enforcement operations against gangs, drug cartels, and other organized crime. Biometric identification—using high-resolution hand, facial, or retinal scanning—eliminates the criminals' ability to disguise their identity regardless of demographic background or to fool captors. The complementary use of police systems and biometric scanning capability at the tactical level (squad), associated with appropriate sub-battalion level authorities and thresholds for action, will create conditions that will mitigate many limitations and act as a force multiplier for friendly units in exactly the same fashion as it has for U.S. law enforcement organizations. Such a capability, if deployed with patrolling formations, could be left with Iraqi security forces for continued use to ensure little loss of continuity once American forces begin to reduce their presence.

The Chicago Police Department's CLEAR is an example of the type of processes and technology that could enable friendly forces to enhance regional security. It comprises a database/data correlation/data mining/knowledge system based on Oracle's commercially available 9i database and the associated 9i Developer suite. It combines with a front-end biometric collection capability enabling the rapid collection, determination, and dissemination of detainee information. CLEAR utilizes commercial-off-the-shelf (COTS) software and links to multiple national identification databases such as the Federal Bureau of Investigation (FBI) Integrated Automated Fingerprint Identification System (IAFIS), which represents a proven technology in daily use with the Chicago Police Department.

coalition forces continue to conduct nontraditional missions within a culture whose willingness to accept policing by outsiders is problematic at best

Military Police dog searches for explosives in Iraq

30th Space Communications Squadron (Molly Dzitko)

A key element distinguishes CLEAR from prior systems to include BAT. Specifically, CLEAR operates/associates automatically. Predecessor systems operated in a "push" method requiring operators to take collected information and push data files manually to selected databases. Once the data arrived at the next database location/next step in the workflow, manual matching added up to 48 hours to the cycle time. Transactional design allows CLEAR to perform information retrieval, link analysis, file updates, and synchronization automatically without human intervention. This permits cycle times as low as 3 minutes from the point of encounter to the database and then back to the point of encounter while simultaneously increasing the overall accuracy and timeliness of the information.

The arrest-to-booking process constitutes CLEAR's most pertinent function to squad level operations at encounter points (whether conducting checkpoints or detaining personnel during raids or sweeps). For Chicago, using Crossmatch Technologies MV–100 as the biometric collection device, and Computer Deductions, Inc., software, an officer (or a Soldier) can collect various forms of identification from an individual. The form of identification can be any combination of inputs or a single input ranging from swiping identification cards and hand-typed information to real biometric inputs such as (facial) photographs and fingerprints (up to 10 if in concert with Homeland Security Presidential Directive 11).

Once inputs are gathered, the handheld unit transmits the information to the squad car (or Humvee), which then transmits it to higher headquarters and to databases within the FBI, such as IAFIS. Data arrival triggers transactional automatic scans of an Oracle database mining for any pertinent data on the detainee such as ticket history, fines, outstanding warrants, aliases, physical markings (such as tattoos), a list of known associates, a mapping of any crimes committed, and a multitude of other essential data points. Automatically, the data transmit back down the chain to the MV–100 within 3 to 5 minutes, enabling the officer (or Solider) to act accordingly.

Simultaneous with the transactional process, data collection continuously expands the known data universe. Much of the information gathered every day links into the data analysis tool, permitting scrutiny of daily information and development of key statistics easily portrayed through reports or overlaid onto maps. These reports and maps permit higher headquarters to evaluate near real-time intelligence associated with changing criminal activities and make appropriate force adjustments as needed—much like our units in Iraq do with far less sophisticated data. The Chicago Police Department used this to track organized crime, gang-related violence, and crime patterns in a manner that had the same effect as surging hundreds of officers onto the street. It is obvious that the technology and proven methods used in Chicago apply similarly to military decisionmakers tracking shifting patterns of terrorist, insurgent, or sectarian violence in-theater.

Civilian police train in riot control techniques

2d Communications Squadron (Joanna Kresge)

At the squad level, rapidly understanding a detainee's true identity, the threat revealed by that identity, known associates, and the areas in which he operates could trigger proactive responses. Most importantly, immediate, verifiable information provides the foundation allowing our forces to retain the initiative to a greater degree than before. That initiative arguably will prevent a predictable response that often constitutes the first step in a complex ambush. Moreover, instead of waiting 18 hours for transport to higher headquarters, the response from the system (BAT) at that level, subsequent interrogation, and manual cross-matching of data, a sub-battalion level unit could rapidly act on perishable intelligence that links the detainee to known associates located in the same vicin-

ity. "Pulling the strings" associated with such links allows friendly forces to roll up enemy networks that previously would use their cultural anonymity to hide in plain sight.

At the higher headquarters level, the inputs from a CLEAR-like system could further populate the BAT system (as well as the Defense Department's Automated Biometric Identification System [ABIS] database and the FBI's IAFIS database to assist in global counterterror operations) while generating daily analysis of field actions. This daily intelligence enables rapid redeployment to head off notable trends in insurgent redeployment as noted by detainee history from a particular area. Automated pattern presentations and superior communications among coalition forces would allow the forces to act well within the insurgents' decision cycle and force them to reconsider, change, or cancel operations to a degree only previously achieved by physical saturation of an area because they will need to expend greater resources on their own force protection.

Theory to Practice

Until recently, using a CLEAR-like system to support the arrest-to-booking process in the U.S. Central Command theater at the squad level only begged the question: *Can it work in practice?* The answer is most definitely *yes*. As depicted in the February 8, 2007, *Wall Street Journal* article entitled "Snake Eater," a subset of the CLEAR system saw action in Iraq and not only proved its direct impact on mapping human terrain, but also provided an undeniable psychological effect on a previously burgeoning insurgency.[6] Major Owen West, USMC, brought an MV–100 and COPLINK loaded on a personal computer into the Khalidaya area just north of Baghdad. From one night of operations, not only did Major West succeed in applying the MV–100 and COPLINK, but he also executed a psychological operation that made the insurgent reconsider where he was operating. Major West's replacement continues to employ the Snake Eater subset of CLEAR, while a second front saw the field testing of the system's complete functionality. From February 26 to March 1 at Camp Roberts, California, the Tactical Network Topology exercises tested CLEAR system architecture. The test assessed the ability of a CLEAR-like system (communication architecture with a layered database) to produce actionable intelligence during Marine Corps Snap Vehicle Checkpoint operations. Multiple scenarios tested the system. First, at checkpoints manned by special operations personnel, the specially configured MV–100 personal digital assistant (PDA) was used to take two fingerprints, a mug shot, and other demographic data. There were two options, Full Encounter ID or Fast ID. Major West and his squad used these same options and configurations as part of transition training for an Iraqi brigade in the Al Anbar province.

automated pattern presentations and superior communications would allow coalition forces to act well within the insurgents' decision cycle and force them to reconsider, change, or cancel operations

In the Camp Roberts exercise, the PDA had a limited number of records stored in the device for potential initial matching. If there was no match, the data transmitted to

MP shows Iraqi police officer how to use database

Fleet Combat Camera (Jeremy Wood)

a relay vehicle or Humvee, and the data then transmitted to the Tactical Operations Center and the second match took place at the server (laptop). The server had the database of the local population. The data then transmitted via virtual private network to the Biometric Fusion Center for access to the ABIS emulator database resident in the FBI's Clarksburg, West Virginia, center (home of IAFIS and ABIS). The center constituted a test database to prove capability while protecting the security of the real ABIS. The response from the ABIS emulator (match or no match plus additional data) retransmitted to the server at the Tactical Operations Center. All the information returned then to the PDA for action.

A battlefield medical scenario and a full blue-red force scenario with checkpoints established at the recommendation of the Tactical Operations Center comprised additional tests for the CLEAR-like system. Furthermore, CLEAR successfully integrated with Tacticomp,[7] which constituted the relay communications from the vehicle to the Tactical Operations Center for the latter scenario. The system continued to work well. This Tacticomp system is available in a number of the Humvees and will provide added capability to the Hand-held Interagency Identity Detection Equipment system (the PDA addition to BAT). The key point is that the Tacticomp infrastructure exists in Humvees today and comprises a proven link for the CLEAR subsystem, obviating the need for additional equipment installation in already cramped vehicles.

The response times for Fast ID from data entry at the MV–100 PDA to the ABIS emulator and back ranged from 1 minute 28 seconds to 2 minutes 47 seconds. For the Full Encounter ID, the response time ranged from 2 minutes 16 seconds to 3 minutes 35 seconds. All of these times include the time it takes to enter the data on the PDA, which ranged from 37 seconds for Fast ID to 1 minute 25 seconds for Full Encounter ID. The system provided fast response based on a single fingerprint as well as a single facial print. The special operations personnel took these measurements at the checkpoint and developed valuable feedback. This connectivity to the ABIS emulator and ultimately the real ABIS system will provide valuable information on insurgents in theater to Major West's replacement and that unit's associated Iraqi brigade. Moreover, their operations will exploit the more complete functionality of CLEAR.

The significant advantage of the CLEAR-like system is that it does not require secret-level, Secure Internet Protocol Router (SIPR) connectivity and therefore can remain with our coalition partners without concern over security. At some time in the future, this system will complement the existing BAT system and its SIPR connectivity and database and expand U.S. force capabilities through simple connectivity integration. Simultaneously, the system will retain its unclassified capability, enabling use by allied forces or members of the law enforcement community without SIPR access. This integration will incorporate the existing databases into one overall architecture that may be able to provide solutions to the squad-level Soldier and the beat-level police officer as both protect and serve.

the CLEAR-like system does not require Secure Internet Protocol Router connectivity and can remain with coalition partners without concern over security

Recommendations

Enabling the warfighter with proven law enforcement COTS technology to complete nontraditional constabulary/policing missions defines the ultimate objective. Taking a proven solution from the streets of Chicago, testing it for battle-readiness, and rapidly integrating it with existing solutions (that is, BATS and IAFIS) may be a way of spreading the small scale success that Major West had in Khalidaya across the region. No matter which system is selected, the key tenets of the path forward should be to:

- avoid confusing biometric collection capability/equipment with the essential heart of the solution, which is the database, data mining, knowledge management system that turns biometric data into actionable information without relying on human intervention
- investigate incorporating best practices in police database/information technology and associated processes into ongoing squad level operations in Iraq and Afghanistan
- populate and integrate all known criminal databases to enable all counterterrorist and law enforcement agencies to overcome terrorist demographic and mobility challenges
- test CLEAR or other similarly mature law enforcement COTS solutions in Iraq and Afghanistan
- integrate as a complementary solution to BAT (with its SIPR access), while keeping a CLEAR-like, nonsecure Internet solution segregated for use by Iraqi forces once coalition forces redeploy
- use the capability placed in Iraq and Afghanistan as a feeder for U.S.-based systems, thereby enabling another level of domestic capability to protect the United States.

After 8 years in office, Mayor Giuliani saw a dramatic drop in crime by applying his theories on countering crime in New York.[8] With 4 years already behind us in Iraq, and public opinion leaning toward a significant reduction in U.S. forces engaged there, a proven law enforcement force multiplying tool that could enhance counterinsurgency and counterterrorist activities as our troops try and police the region should be applied. The major similarity that the Giuliani situation has to Iraq is that time, money, and force levels all are stressed. Instead of losing time by recreating existing COTS capability, why not take a lesson from the streets of Chicago and apply it in the streets of Baghdad and Kabul? We have asked our troops to police the world; let's give them the proven tools to succeed. **JFQ**

NOTES

[1] See <http://en.wikipedia.org/wiki/Rudolph_Giuliani#1993_campaign_and_election>.

[2] See <www.oracle.com/customers/profiles/PROFILE4257.HTML>.

[3] Michael J. Sniffen, "Murder rate at a 40-year low: Chicago alone had 150 fewer killings," *The Chicago Sun-Times*, October 18, 2005.

[4] "Afghan rebels may have help from Iraq," Associated Press, February 17, 2007.

[5] See Paul J. Shannon, "Fingerprints and the War on Terror: An FBI Perspective," *Joint Force Quarterly* 43 (4th quarter, 2006), 78.

[6] Daniel Henninger, "The Snake Eater: Give our troops the tools our cops have," *The Wall Street Journal*, February 8, 2007.

[7] Tacticomp is a wireless, Global Positioning System-enabled military hand-held computer designed for field use. Its tactical modem allows automatic communication through field radios.

[8] See <http://en.wikipedia.org/wiki/Rudolph_Giuliani>.

China's ASAT Test Motivations and Implications

By PHILLIP C. SAUNDERS *and* CHARLES D. LUTES

ASAT fired by F–15 as part of training exercise

On February 15, 2007, the National Defense University's Institute for National Strategic Studies convened an unclassified roundtable to discuss the motivations and implications of China's direct-ascent antisatellite (ASAT) weapons test. Participants included China scholars and space experts with a range of policy viewpoints. The roundtable was intended to highlight issues and perspectives that U.S. policymakers should consider in thinking about U.S. responses to the test. This report draws heavily on views expressed at the discussion, but the authors have added further analysis to provide a fuller explication of the relevant policy issues.

China's ASAT Programs

China launched a direct-ascent ASAT weapon on January 11, 2007, which struck a Chinese FY–1 weather satellite in low Earth orbit (LEO). The ASAT's kinetic kill vehicle (KKV) was likely boosted by a two-stage launcher based on a DF–21 medium-range ballistic missile, which may be mounted on a mobile transporter-erector-launcher. China reportedly conducted several previous tests of the system; it is unclear if the same configuration was used for all the tests.[1] The successful test demonstrates a Chinese capability to destroy a number of U.S. satellites in LEO used for reconnaissance, remote sensing, surveillance, electronic surveillance, and meteorology, as well as some civilian communications satellites with military applications.[2] These satellites and the International Space Station are also at increased, although not significant, risk from the debris cloud created by the recent ASAT test.

The direct-ascent ASAT appears to be part of a larger Chinese ASAT program that includes ground-based lasers and jamming of satellite signals. People's Republic of China (PRC) analysts, scientists, and strategists have written extensively about ASAT weapons and potential means of countering U.S. military uses of space.[3] The revelation by the director of the National Reconnaissance Office that Chinese lasers have "painted" U.S. satellites indicates a capability to disrupt imaging satellites by dazzling or blinding them.[4] Jamming can disrupt U.S. military communications and global positioning system (GPS) navigation and targeting signals. The exact performance characteristics of Chinese systems are

American ASAT is loaded onto F–15

U.S. Air Force

Dr. Phillip C. Saunders and Colonel Charles D. Lutes, USAF, are Senior Research Fellows in the Institute for National Strategic Studies at the National Defense University.

U.S. Air Force

unknown, but a range of ASAT capabilities would provide flexible options to temporarily or permanently deny U.S. space capabilities. The Chinese direct-ascent ASAT program appears to be in the research and development phase, and the intent or timing of operational deployment remains unknown.

the revelation that Chinese lasers have "painted" U.S. satellites indicates a capability to disrupt imaging satellites by dazzling or blinding them


NASA Administrator Michael Griffin meets with Chinese minister of science and technology

NASA

Chinese Decisionmaking

China's ongoing pursuit of a range of ASAT capabilities in addition to the direct-ascent ASAT is evidence of senior leadership knowledge and support.[5] Some experts argued that removal of language on "preventing an arms race in outer space" from China's 2006 defense white paper and its refusal to sign The Hague Code of Conduct against ballistic missile proliferation are evidence of policy coordination across the Chinese bureaucracy on ASAT-related issues.[6] Two months after the test, Prime Minister Wen Jiabao stated that China's position on peaceful utilization of space remains unchanged and endorsed negotiation of a treaty on the peaceful use of outer space.[7] However, China's 12-day silence immediately after the test, uncoordinated messages (including a flat denial from the military), and absence of a clear communications strategy indicate a lack of internal coordination about the January ASAT test.[8] One China expert suggested that there might be a horizontal compartment (perhaps at the Central Military Commission level) of those who approve China's ASAT programs and a vertical compartment (including the General Armaments Department and laboratories involved in research and development) of those developing and testing ASAT systems. Limited overlap between the compartments might explain why China miscalculated the response to the ASAT test and was not prepared to respond to international criticism.

Participants felt Chinese President Hu Jintao almost certainly approved the overall ASAT test program; some thought he may have approved each individual test. The uncoordinated Chinese response suggests that the Ministry of Foreign Affairs (MFA) was not aware of the January ASAT test in advance. One China expert noted that the Chinese response "sends all the wrong signals" in terms of civilian control of the military, transparency, and consistency with China's "peaceful development" campaign. He contrasted the uncoordinated response with China's nuclear test in 1964, when Beijing sought to shape international reactions through carefully coordinated messages.

Most participants believe China underestimated how negative international reactions to the test would be. This may be due to the lack of protests of earlier ASAT-related tests, ignorance of the debris issue, or a Chinese cultural expectation that the United States would keep quiet about any vulnerability to ASAT weapons. Several suggested that senior leaders might not have been briefed that debris generated by the test would pose a threat to other satellites. One noted that China's ASAT test would probably accelerate U.S. investments in space weapons and empower those who see China as a threat, developments that are not in China's interest. Others questioned how much of a price China would really pay, suggesting that aside from short-term damage to China's image and the loss of civil space cooperation with the United States, the ASAT test would have limited long-term costs.

Motivations

Most analysts believed that China felt the need to test its direct-ascent ASAT in order to develop the system and confirm that it worked properly. A space expert argued that ASATs are like ballistic missile defense: "At a certain point you need to test or the program won't improve to the next level." The group agreed that the timing of the test is not significant; the important message is the fact that China is pursuing ASAT weapons and has demonstrated a certain capability. One China expert suggested that the key messages are that the United States could not expect to dominate space alone and that intervention on behalf of Taiwan would be increasingly risky and costly. Others suggested PRC motives might include warning Taiwan against seeking independence and highlighting Chinese capabilities with respect to Japan and India, both of which operate satellites.

Most of the group felt that ASAT weapons are one of a series of asymmetric capabilities that China is developing to exploit potential U.S. military vulnerabilities. Chinese strategic analysts are well aware of increasing U.S. military dependence on space; ASAT weapons can exploit this vulnerability and reduce American ability to operate in the Western Pacific. One space expert argued that ASAT weapons are a logical and relatively inexpensive response to U.S. military dominance, which rests heavily on space capabilities. Others noted that China's military modernization, which emphasizes "informationalization," would rely increasingly on space in the future, reducing the asymmetric impact of ASAT capabilities.

If deployed, Chinese antisatellite weapons would pose immediate threats to a range of U.S. military capabilities that rely on space assets and would have significant consequences for a Taiwan contingency. The United States has a range of options for countering Chinese ASAT capabilities and limiting their impact, but there is no simple or cost-free solution.

Capabilities at Risk

The direct-ascent ASAT system China tested could threaten satellites in LEO. These include U.S. military satellites used for reconnaissance, remote sensing, surveillance, electronic surveillance, and meteorology, as well as a number of civilian communications satellites with military applications. Satellites in medium Earth orbit and geostationary orbit are not vulnerable to the direct-ascent ASAT system boosted by the two-stage DF–21 launcher. Although China has demonstrated the ability to launch satellites into geostationary orbits using larger rockets, the techniques required to reach higher orbits would significantly alter the dynamics for an effective hit-to-kill KKV, making the current ASAT design unusable for such purposes.

However, laser-based ASAT weapons could potentially target U.S. reconnaissance satellites. One space expert viewed lasers as a more important threat than the direct-ascent system, while another noted that all efforts to develop high-powered lasers had been plagued with technical problems, and deployment of such capabilities was probably decades away. Jammers that degrade GPS signals or interfere with satellite communications are another means of disrupting U.S. space assets, but it is difficult to assess Chinese capabilities in this area. Experts noted that China's doctrine for employing space weapons and ability to link systems operationally were unclear.[9]

A Taiwan Contingency

Given U.S. military advantages, China's best chance of success in a conflict over Taiwan would be to delay the arrival of U.S. forces until after it forced Taiwan to capitulate, presenting Washington with a *fait accompli*. Most agreed that a PRC ability to destroy U.S. satellites in LEO would significantly increase the costs and risks of U.S. intervention on behalf of Taiwan. One China expert pointed out that ASAT weapons are only one in a range of military capabilities Beijing is developing to complicate and delay U.S. military responses. Even if any individual program had only a marginal impact, the cumulative impact could still be significant. A comprehensive net assessment of new Chinese technologies and potential U.S. counters is necessary to consider how to mitigate strategic risk.

Chinese antisatellite weapons would pose immediate threats to a range of U.S. military capabilities that rely on space assets

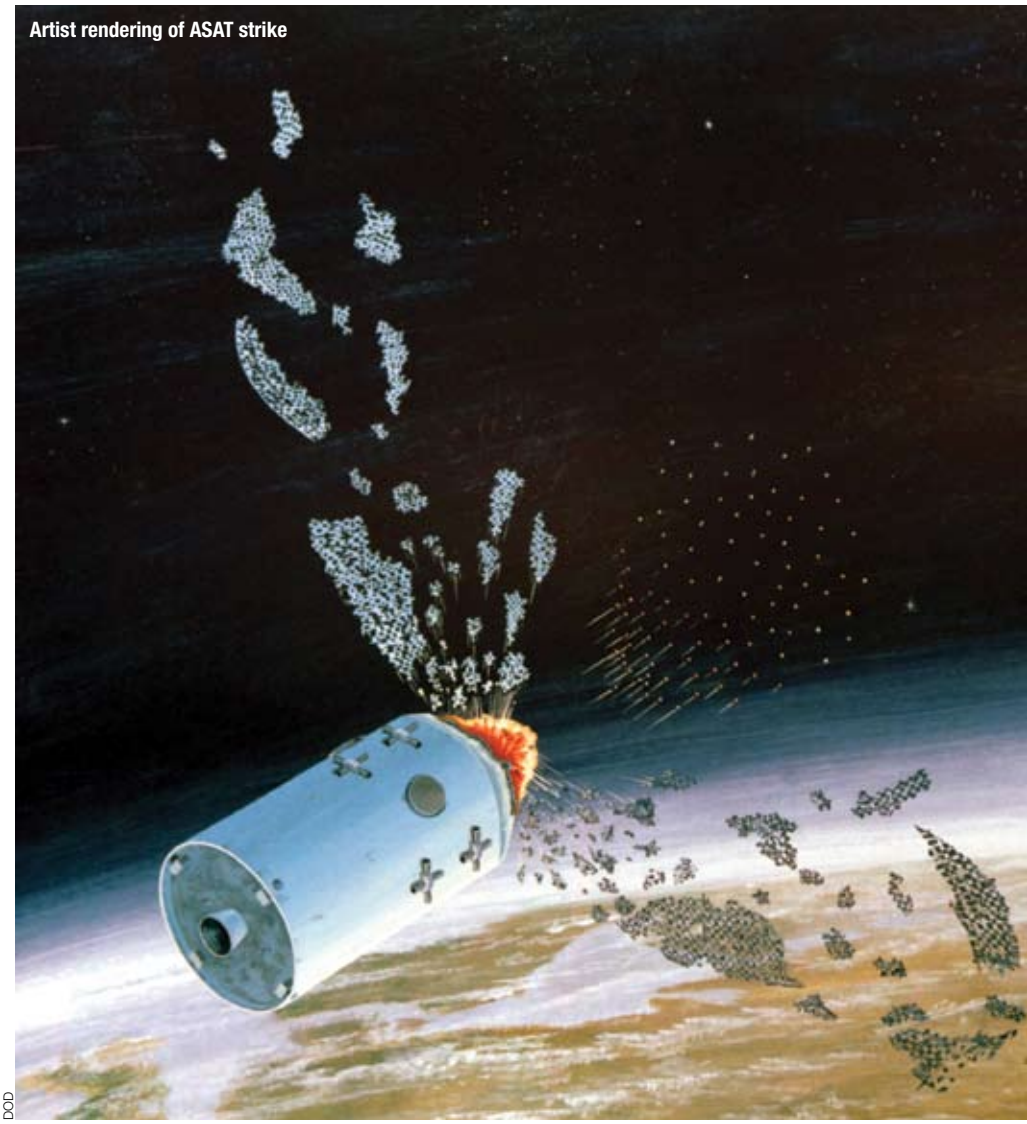
Artist rendering of Defense Satellite Meteorological Program satellite, a possible target of ASAT weapons

Lockheed-Martin

An operational ASAT capability would provide flexible options for delaying and disrupting an American response to a Taiwan contingency. The direct-ascent ASAT could be used to destroy U.S. reconnaissance satellites in LEO; at the same time, China could attempt to destroy Taiwan's Formosat-series satellites operating in LEO.[10] Chinese forces would likely attempt to temporarily blind U.S. reconnaissance and remote-sensing capabilities through lasing, while jamming U.S. communication links and GPS signals to disrupt navigation and, more importantly, precision targeting. These efforts might be coupled with cyber attacks to disrupt and delay the response of U.S. forces. This strategy could be conducted in whole or in part, and without a complete integration of systems.

One specialist noted that the assumption that China would use any and all capabilities in the event of a Taiwan conflict might be incorrect. Nevertheless, U.S. planners have to prepare for worst-case scenarios. He worried about a potential disconnect between U.S. space operators and U.S. Pacific Command planners, who might each think about the impact of Chinese ASAT capabilities only within their narrow areas of responsibility. Others agreed it was important to think through how the United States might operate in a Taiwan scenario with limited access to space; this scenario should be incorporated into future exercises to force creative responses and greater coordination.

actions that cast doubt on the U.S. ability to effectively use its nuclear force would set up a destabilizing strategic dynamic



Artist rendering of ASAT strike

DOD

Strategic Implications

A deployed Chinese ASAT capability would complicate the strategic military relationship between Washington and Beijing. Although U.S. early warning and nuclear command and control communications satellites would not be vulnerable to the current direct-ascent ASAT, they could be targeted for denial by other means. Actions that cast doubt on the U.S. ability to effectively use its nuclear force would set up a destabilizing strategic dynamic. A China expert noted that U.S. attacks on ground-based ASAT systems or components might inadvertently affect China's nuclear command and control system. A PRC perception that the United States might be attacking its nuclear command and control would be very destabilizing. A space expert also suggested that one motive for developing ASAT weapons is concern that U.S. space-based ballistic missile defenses might eventually negate China's nuclear deterrent. In this sense, ASAT weapons could be regarded as defensive in that they could prevent China from becoming vulnerable to a potential U.S. nuclear attack.

The possibility of a U.S.-China space weapons race was discussed. A strategist noted that Beijing probably exaggerates current U.S. space capabilities and overstates the likelihood that Washington will develop and deploy an extensive space weapons arsenal. Statements by U.S. advocates of space control or space weaponization coupled with U.S. reluctance to accept constraints on future space options encourage this misperception. One China expert noted that Beijing is probably sincere in proclaiming that it has no intention of engaging in an arms race. However, China is also unwilling to lock itself in a position of permanent vulnerability to the United States.

Several experts highlighted China's lack of transparency as a factor that aggravates the negative impact of the ASAT test on U.S.-China strategic relations. One China expert noted that the Foreign Ministry and Defense Ministry both initially claimed to be unaware of the test. China did not acknowledge the test publicly for 12 days. An MFA spokesman then gave a bland statement that "this test was not directed at any country and does not constitute a threat to any country"—a line repeated in March by Prime Minister Wen Jiabao.[11] China's reluctance to discuss its military

modernization frankly may strengthen its efforts to deter the United States from intervening in a Taiwan crisis, but it also reinforces U.S. suspicions about Chinese intentions and creates the possibility that the United States will overestimate future Chinese space capabilities and respond accordingly. Lack of transparency also heightens U.S. doubts about whether agreements with Beijing to limit space weapons or to ban ASAT weapons could be verified.

One space expert suggested China may be using a competitive strategies approach against the United States. Space may become an "offensive dominant" arena. By demonstrating a relatively inexpensive response to U.S. space dominance, China may calculate that the United States will pursue costly options that divert resources from other areas. China could avoid an expensive arms race by minimizing reliance on space assets and developing a relatively inexpensive set of asymmetric capabilities. Conversely, other China experts suggested Beijing's dependence on space for military purposes is likely to increase dramatically over the next 5 to 10 years. Foregoing space capabilities would greatly limit China's ability to fight an "informationalized war." The shift toward more symmetrical U.S. and Chinese dependence on space may create opportunities for arms control or restraint in the development of space weapons.

smaller satellites that incorporate stealth technology, employ countermeasures, or have the ability to maneuver would be harder for China to target

Countering ASAT Weapons

Most felt that China is unlikely to be able to permanently disable most U.S. space assets in the near- or midterm. However, it may soon be able to use ASAT weapons to gain advantages in a Taiwan contingency. The group discussed a range of technical and operational means that might help counter potential Chinese ASAT capabilities:

■ Launch direct attacks against Chinese ASAT systems: Attacking ground-based ASAT systems or components prior to launch or use might be effective against known high-powered lasers but would have only limited utility against possible mobile ASAT systems that would likely be dispersed, hard to find, and located deep in China's interior. China experts noted that attacks inside Chinese territory would significantly escalate any conflict.

■ Use space-based weapons to attack Chinese ASAT systems or space assets: Some participants believed space-based weapons could help protect U.S. satellites by attacking some types of Chinese ASAT weapons. Others disagreed and suggested that space-based weapons could create even greater insecurity. These systems would take years to develop and deploy and could cause the United States to embark on a costly path both economically and politically. Some space experts suggested that China might hope to divert U.S. military modernization down this path.

■ Replenish damaged satellites rapidly: The ability to launch replacement satellites quickly could limit the military advantage from ASAT attacks. This is likely to be expensive and might be negated by increased Chinese deployment of less-expensive ASAT weapons.

■ Make satellites harder to find and hit: Smaller satellites that incorporate stealth technology, employ countermeasures, or have the ability to maneuver would be harder for China to target and attack.

■ Employ constellations of small satellites: Dispersing capabilities among a number of small satellites would reduce the vulnerability to the loss of any single satellite and complicate efforts to target U.S. space capabilities. It would also increase the robustness of the system by creating redundancies. This would require a shift in design philosophy and might not be applicable to all military space capabilities.

■ Make greater use of nonspace tactical reconnaissance systems: Aircraft and unmanned aircraft systems could substitute for some space-based assets and would potentially be harder to target. However, they may not be able to loiter in critical or contested airspace, rendering them ineffective.

■ Use foreign satellites to increase the political costs of attacks: Some space experts suggested the United States could make greater use of Russian, European, or commercial communications or imagery satellites to take advantage of Chinese reluctance to attack commercial or foreign space assets. Others questioned the willingness of countries to take sides in a conflict, given their increasing economic stake in relations with China.

U.S. officials should also consider some broader military and policy options:

■ Learn to fight without satellites: The modern American way of war depends heavily on space capabilities. Learning to fight without them would take a concerted effort to develop and exercise alternate contingency plans and field redundant capabilities. Some China experts noted that this would return the U.S. Navy to a 1970s style of fighting with carrier battlegroups and strike aircraft. A military expert noted that the United States needs to rethink the assumption that precision strike, intelligence/surveillance/reconnaissance, and bombers would always translate into military superiority, especially with a contested space environment.

■ Consider diplomatic solutions: Diplomatic approaches, including arms control, offer the potential to deal directly with the strategic issues posed by ASAT weapons. These approaches might range from formal treaties on preventing an arms race in space or banning ASAT weapons to informal understandings about proper military uses of space. Most participants felt that negotiating and verifying a formal ban on ASAT weapons would be extremely difficult. Some believed that other arms control approaches might be more practical and still have considerable value.

■ Adopt an international code of conduct on space behavior: Establishing a code of conduct or rules of the road would reinforce international norms about the right of countries to use space for peaceful purposes.[12] This could limit China's ability to conduct future ASAT tests and to develop more effective systems. Both arms control and code of conduct approaches would impose limits on U.S. freedom of action in space. In addition, a ban against actions that produce space debris would not address strategic issues associated with ASAT weapons or prevent the development of capabilities that could deny or disrupt satellite services. However, the space debris issue could be helpful in mobilizing commercial interests to actively oppose ASAT weapons or actions that interfere with the operations of satellites.

■ Establish international partnerships to support peaceful uses of space: The Proliferation Security Initiative offers an example of partnerships among like-minded nations to counter malevolent international behavior. A Space Security Initiative could be developed to discipline actors that seek to limit international uses of space. The goal would be to enlist government and nongovernment users in efforts to prevent and penalize actions that might threaten the operation of satellites, including issues such as ASAT weapons, space debris, nuclear accidents in space, jamming of satellite communications, or intrusions into satellite broadcasts. The partnership could offer benefits such as shared surveillance of space debris and also serve as a vehicle for sanctions against countries or entities that violate a space code of conduct, whether they are signatories or not. All space-faring nations, including China, could become members of the partnership by agreeing to the code and enforcing its norms.

Dissuasion and Deterrence

Another approach is to try to dissuade China from developing ASAT capabilities and to deter it from using them in a conflict. Successful dissuasion would require the United States and other countries to impose costs on China if it continues efforts to develop and deploy ASAT weapons. A space expert noted that the lack of U.S. response to earlier tests may have led China to underestimate the costs of pursuing ASAT weapons. A China expert noted that U.S. complaints about earlier tests might have helped overcome the compartmentalized Chinese system and forced Chinese leaders to consider the full costs and benefits of the ASAT program. A strong response from the international community would reinforce dissuasion efforts, but most felt that China was currently paying relatively low costs for its ASAT test and program. Dissuading Beijing from deploying ASAT capabilities would require greater efforts to raise the costs of deployment and to assure China that it can meet its security needs without deployment. The possibility of conflict over Taiwan greatly complicates this effort.

a few space experts argued that China prefers a treaty banning space weapons, although such an agreement would be difficult to negotiate and verify

Most participants believe China will probably continue developing ASAT weapons, although it might not test the direct-ascent ASAT system again (or might do so only in a suborbital mode that would limit debris). Most felt the strategic value of ASAT weapons was high enough that China would likely deploy them. A few space experts argued that China prefers a treaty banning space weapons, although such an agreement would be inherently difficult to negotiate and verify (especially because some PRC experts consider space-based surveillance assets to be space weapons). Most of the group dismissed the argument that Beijing tested its ASAT weapon to encourage Washington to negotiate about space weapons. Most felt China's primary motive in testing was to demonstrate a military capability that could increase the costs and risks of U.S. intervention in a Taiwan conflict. One participant suggested that although China would continue to champion a treaty banning space weapons, it might well support a code of conduct as an interim measure. Others noted that a code of conduct might address space debris but would do little to address the vulnerability of U.S. space assets.

Deterring the use of ASAT weapons also poses difficult challenges. China experts noted that China does not share the U.S.-Soviet experience with arms control, deterrence, mutual satellite reconnaissance, or dealing with incidents at sea. The U.S. military has internalized these norms into its doctrine and operations, but China does not necessarily accept them. While U.S. thinking about deterrence has traditionally focused on conventional and nuclear aggression, deterrence might work differently in the space and cyber domains. The different context may complicate attribution and require rethinking thresholds for response.

There was a consensus that lack of a clear declaratory policy made it harder to deter attacks on satellites. Some U.S. officials have stated that an attack on an American satellite would be an act of war, but the United States did not respond to China's lasing of an American satellite, diminishing the credibility of that declaration. Most participants felt the United States needed a clearer declaratory policy and that effective deterrence would also require the will to respond to attacks on U.S. satellites or computer systems. The American response need not be tit-for-tat; the group discussed the possibility of asymmetric responses to jamming or lasing of U.S. satellites. These options raised complicated legal and operational issues that deserve further study.

U.S.-China Relations

The group also discussed what impact China's efforts to develop ASAT weapons—which most felt were aimed primarily at the United States—should have on U.S.-China relations. Some felt China's decision to conduct an ASAT test that generated space debris and efforts to develop other asymmetric capabilities that could reduce U.S. military advantages raise questions about whether Beijing's behavior is consistent with Washington's policy goal of making it a "responsible stakeholder" in the international system. Most in the group felt that ASAT

weapons would be a militarily significant capability if the United States and China ever fought over Taiwan, but were uncertain how heavily to weight that contingency in the broader calculus of bilateral relations.

One China expert noted that if Washington wants to maximize the chances of dissuading Beijing from deploying and using ASAT weapons, then it should hold broader political and economic cooperation at risk. However, this would be costly for other important U.S. interests. Others agreed that economic interests and the need for cooperation with China on issues such as North Korea limit the degree to which the United States could make China pay a price for developing ASAT weapons. While international criticism of China for conducting the test and for heightening the risk to other satellites through space debris has had some impact on Beijing, calls for responsible behavior in space are unlikely to address the underlying strategic issues. A China specialist noted that the United States is still reluctant to accept a nuclear deterrent relationship with China that constrains U.S. freedom of action; a similar dynamic applies with respect to space. A strategist argued that this constraint is not wholly negative; it presents an opportunity to reexamine U.S. objectives and strategy in Asia and ensure that strategy is consistent with national interests.

The Chinese direct-ascent ASAT test raises difficult questions about China's intentions, U.S. responses, and the impact on broader U.S.-China relations. The United States has a range of potential responses to Chinese efforts to develop ASAT capabilities. Unfortunately, none of the available options is simple, cheap, or likely wholly effective. U.S. policymakers should consider both policy initiatives to limit Chinese deployment of ASAT capabilities and technical and operational measures that would mitigate the impact on U.S. military capabilities if China does deploy ASATs. Deterring the use of ASAT weapons may pose new challenges that differ from previous U.S. experiences with conventional and nuclear deterrence.

Both China and the United States will have important choices to make. Beijing will have to weigh the potential military benefits of developing and deploying ASAT weapons against the likely damage to bilateral relations and to its carefully cultivated image as a responsible country focused on peaceful development. Washington must balance the importance of its broader relationship with Beijing against the need to maintain access to space for both military and commercial purposes. These considerations could lead both countries to exercise some degree of restraint in deciding how vigorously to pursue ASAT weapons and other counterspace capabilities.

the direct-ascent ASAT test raises questions about China's intentions, U.S. responses, and the impact on broader U.S.-China relations

However, strategic and bureaucratic imperatives could also create a negative dynamic that affects the broader U.S.-China relationship. The direct impact might take the form of heightened military competition as the United States responds to Chinese efforts to develop asymmetric capabilities such as ASAT weapons. The indirect impact might be felt if each side comes to view the other as a strategic threat and the competitive dimensions of their relations overshadow the importance of cooperation in pursuit of common interests. This outcome is not inevitable, but the extension of competition into the space domain will complicate efforts to build a stable and constructive bilateral relationship. **JFQ**

NOTES

[1] For background on the Chinese ASAT test, see Geoff Forden, "A Preliminary Analysis of the Chinese ASAT Test," Massachusetts Institute of Technology, undated, available at <http://web.mit.edu/stgs/pdfs/A Preliminary Analysis of the Chinese ASAT Test handout.pdf>. A public mention of three previous tests came from CNN Pentagon correspondent Jamie McIntyre. See <http://transcripts.cnn.com/TRANSCRIPTS/0701/18/ldt.01.html>. The possibility that China's ASAT is mobile is mentioned in Stuart Slade, "Chinese ASAT Programs," *Forecast International*, January 25, 2007, available at <http://emarketalerts.forecast1.com/mic/eabstract.cfm?recno=131967>.

[2] For a description of satellites in low Earth orbit, medium Earth orbit, and geosynchronous orbit, see Marco Caceres, "Orbiting Satellites: Beancounter's Heaven," *Aerospace America*, August 2001, available at <www.aiaa.org/aerospace/Article.cfm?issuetocid=122&ArchiveIssueID=17>.

[3] See Phillip C. Saunders et al., "China's Space Capabilities and the Strategic Logic of Anti-Satellite Weapons," Center for Nonproliferation Studies Research Story of the Week, July 2002, available at <http://cns.miis.edu/pubs/week/020722.htm>; Michael P. Pillsbury, "An Assessment of China's Anti-Satellite and Space Warfare Programs, Policies and Doctrines," Report for the U.S.-China Economic and Security Review Commission, January 19, 2007, available at <www.uscc.gov/researchpapers/2007/FINAL_REPORT_1-19-2007_REVISED_BY_MPP.pdf>; and "PRC Experts Discuss Countering Reconnaissance Satellites with Jamming, Camouflage," Open Source Center CPP20070111465001.

[4] Warren Ferster and Colin Clark, "NRO Confirms Chinese Laser Test Illuminated U.S. Spacecraft," *Defense News*, October 2, 2006, available at <www.defensenews.com/story.php?F=2141128&C=airw>.

[5] Dean Cheng makes this point in "China's A-Sat Test: Of Interceptors and Inkblots," *Space News* 28, no. 6 (February 12, 2007), 17, 19.

[6] The coordinator of China's defense white paper has told U.S. scholars that language on preventing an arms race in outer space was not included because China published a separate white paper on arms control and nonproliferation in 2005.

[7] See PRC Ministry of Foreign Affairs, "Premier Wen Jiabao's Press Conference 2007/03/17," available at <www.fmprc.gov.cn/eng/zxxx/t304313.htm>.

[8] For an exploration of the Chinese decision-making process on the ASAT test, see James C. Mulvenon, "Rogue Warriors? A Puzzled Look at the Chinese ASAT Test," *Chinese Leadership Monitor*, no. 20 (Winter 2007), available at <http://media.hoover.org/documents/clm20jm.pdf>.

[9] One useful analysis is Kevin Pollpeter, "The Chinese Vision of Space Military Operations," in *China's Revolution in Doctrinal Affairs: Emerging Trends in the Operational Art of the Chinese People's Liberation Army*, ed. James Mulvenon and David Finkelstein (Alexandria, VA: CNA Corporation, 2005), 329–369.

[10] Taiwan's remote sensing satellites can photograph objects as small as 10 feet in size, a capability sufficient to count cruise missiles pointed at Taiwan from the Chinese mainland. See Craig Covault, "China's ASAT will intensify U.S.-Chinese faceoff in space," *Aviation Week and Space Technology*, January 21, 2007, available at <www.aviationweek.com/aw/generic/story_generic.jsp?channel=awst&id=news/aw012207p2.xml>.

[11] Chris Buckley, "China confirms satellite test, says no threat," Reuters, January 23, 2007.

[12] See Henry L. Stimson Center, "Code of Conduct for Space-Faring Nations," February 2007, available at <www.stimson.org/?SN=WS200702131214>.

DOD

General James E. Cartwright, USMC, is Commander, U.S. Strategic Command.

An Interview with

James E. "Hoss" Cartwright

JFQ: *How do you rate the ability of U.S. Strategic Command* [USSTRATCOM] *to carry out the mission of combating WMD* [weapons of mass destruction], *and does the command have all of the authorities and policy guidance essential to this mission?*

General Cartwright: Combating WMD was the last mission area given to the command in sequence, and so from the standpoint of time to mature, it's had the least. This is a mission area that in the last Presidential election was the only area that both candidates agreed on, and they both agreed that it was the most important thing—a heretofore unassigned mission area. That gives you a sense of the importance that the National Command Authority puts on the mission, but over time it has not been something that we probably have paid a commensurate amount of attention to. I can say that and people will not like it, but I can't see that you can really argue with it. So we have tried to understand, first, who are the logical partners in this activity.

The three key pillars associated with the mission are the consequence management piece, which is, "Okay, you've failed at everything else, now it's time to clean up," which actually can be a deterrent, particularly against someone who is a terrorist or a martyr: if you take their objective away, you have a chance of affecting whether or not they decide to get up in the morning and strap bombs onto their body and go into a crowded place. If you remove that objective, if they can't get the effect they desire, you have a chance of affecting a terrorist. So it still is a very valuable weapon; it has deterrent value.

The other two pillars are probably more readily identified. Nonproliferation is that activity that says that the country you are dealing with agrees with you and wants help figuring out how to divest itself of anything that is of WMD class—they've seen the light, they've decided it's not appropriate.

Counterproliferation is more challenging. Here, you don't have a willing partner; you hope to develop a willing partnership with others to build an alliance that says, "This is just not the right way to do business, if you're going to continue on this path, then we would like to offer all types of deterrence to change your mind." But the two key pillars that were called out in our tasking in counterproliferation were elimination and interdiction. In those two areas, elimination is the idea, particularly in the course of conflict: you come across weapons of mass destruction, you have to have the capability, one, to isolate it—to "triage" the activity—and then move to an elimination activity, and the challenging part of this is when it's in the course of a conflict. So you're uncovering it as you move forward, you come across the cache, you say, "Oh, I've got this." You don't want to leave that front line unit there guarding it; you want to have a system that allows you to close, the technical experts recognize immediately what it is, then the triage activities—then people who know how to handle it as quickly as possible do, and we let fighting forces continue to fight. What we have not had in the past is a coherent command and control for that activity, the way to reach back and close, the technical skills along with the general purpose skills to isolate the area and then process it so it can be eliminated. That is what we're off to do.

We're working with forces that have been assigned in the 20th Support Group on the Army side that have the technical expertise. We're leveraging them for command and control and the breadth of, "How do I close the problem and set up the opportunity?" We've partnered them with the Defense Threat Reduction Agency, which is my component in this area because they have the technical skills. So by putting the operational skills together with the technical skills, building an overarching joint construct and then having that as a service that we provide to a regional combatant commander, a regional combatant commander deciding to prosecute some sort of a war plan or a contingency would then say, "Okay, there is some expectation that this could occur." We give them the cell for command and control; that cell has the inherent skills to reach back for technical expertise and the ability to discern, "What is it I just ran into? Is it a chemical, is it fissile, what am I dealing with here, what kind of experts do I need?" and then the lift and everything associated with closing the problem. It could be that we do this in conjunction with SOF [Special Operations

On March 22, 2007, Col David H. Gurney, USMC (Ret.), and Dr. Jeffrey D. Smotherman of *Joint Force Quarterly* interviewed General Cartwright at his Pentagon liaison office.

Forces]; it could be that we do it in conjunction with general purpose forces—it depends on the scenario. But that's the skill we're trying to develop.

The nonproliferation side of the equation is really where I would like to spend a lot of time, because nonproliferation represents that you've built the deterrent capability in your strategy and people are recognizing that it makes no sense to have these weapons; let's be partners and get rid of them. Most of that work heretofore has been done under Cooperative Threat Reduction in the Nunn-Lugar construct, which was really associated with the former Soviet states. We're in a dialogue now with Congress to understand how we can broaden this construct to a more global capability and start to allow regional combatant commanders to reach into this capability, to allow them to help their nation-states to help themselves: how do you build a border that can detect these things, how do you know in your country where this is, what's moving around, what got introduced that you didn't know about, how do you ask for help if you can't take care of it yourself, how do you interact with your neighbors in this activity, particularly if you start to think about bio[logical] problems, etcetera—and start to build these cooperative defensive capabilities that keep you from getting to elimination and having to worry about it in an uncooperative way. So we're trying to put a lot of effort into nonproliferation activities.

JFQ: *Do you have all the authorities and policy guidance now?*

General Cartwright: We've been given everything people can think of. But as we develop the CONOPS [concept of operations] and as we start to exercise, we'll start to understand where those authorities fall short. One area that we know already is habitual relationships in the interagency [community]. You don't want to put on the interagency process crisis decision activities; you'd like to set up and say, "Here's what we think are the range of activities associated with counterproliferation and nonproliferation," as an example, and "Here are the key actors that have to be working on a day-to-day basis in real-time." Our interface with the National Counterproliferation Center, our interface with the National Counterterrorism Center—that can't be only in a crisis, that's got to be a day-to-day thing, we've got to set up [the Department of] State as the lead for the PSI [Proliferation Security Initiative], which is a combination of the willing, so to speak. So we've got to have a relationship there because you don't want Defense to be something that's over here on the wall, and "break this glass if necessary," and by the time you do, the problem's already gone. So you have to have a day-to-day relationship. That's not standard in the way we do business in the interagency. We have JIATF [joint interagency task force]-type constructs, particularly in the [Department of] Homeland [Security]. This is similar to that, but it is day-to-day, what are the problems in the world, which ones are starting to bubble up and go in an adverse direction, what tools do we have to drive them in the other direction.

our interface with the National Counterproliferation Center, our interface with the National Counterterrorism Center—that can't be only in a crisis, that's got to be a day-to-day thing

You initially want to start with non-force-type tools, but if this doesn't go the right way, let's get the planning going right now about how we do it, who should do it, and what are the right authorities. Do you want to use a Justice authority, do you want to use an Intelligence authority, do you want to use a Title 10 authority? Maybe you want to use a different country because it's more appropriate, and that's what PSI lets you do: start to look cross-country and say, "Who's got the right authorities to match up to the problem?" And so doing that in a proactive way rather than a reactive way is what we've got to get to. That means we've got to have relationships in the interagency that are normally reserved only for OSD [Office of the Secretary of Defense] and the Joint Staff. We're trying to understand what those authorities are, what our left and right limits are so we stay in the boundaries, and we do subject ourselves to the appropriate oversight, but we also don't cut off the reaction times that we might need to go after something that could have a high regret factor—if we don't do this, a weapon is inside your border, or something like that—how do you start to understand, and that's part of the exercising, and the tabletop work is to get the interagency relationships right so that we don't violate checks and balances, we don't violate individual interagency head prerogatives, but yet we posture ourselves in a way that we can be successful.

JFQ: *Does the United States have adequate declaratory policy to deter new and emerging WMD threats, particularly with regard to potential rogue states' nuclear transfers to state and nonstate actors hostile to the United States and to a potential state actor's employment of nuclear weapons in an EMP* [electromagnetic pulse] *attack against the United States?*

General Cartwright: Declaratory policy is but one tool in a broad set of tools that go all the way from friendly interaction to kinetic force. Declaratory policy is like dealing with kids, saying, "Don't you dare do that or I'm going to spank you." That's appropriate at a certain level of behavior. What you'd like to do is set the conditions and the learning such that you don't get to declaratory policy. When do you need to invoke declaratory policy, when is it an appropriate tool, a critical activity? I'll take you back to the last question, because where I want to be dealing here is in nonproliferation and have that be successful so that we don't get to counterproliferation or to a case where we are going all the way, in a conventional sense, to phase II of a conflict where we're flowing force deterrent options out there to make them behave in a way that's appropriate and then coupling that with declaratory policy. So you'd really rather start a relationship based on, "Here's the way we think we ought to behave, here are the incentives to go in this direction, if you start to have inklings about going in a different direction, what's driving you there? What is it about your national security and sovereignty that you're uncomfortable with that drives you to a decision to have this capability? Can I do something about that? Can I do it early enough that you don't have to get to this point?"

If you get to this point and you start to posture, usually what we use is warning time in this scenario, so you get inside a certain amount of time where I can react if you act badly, you can react and surprise, now we're going to start posturing, and now we're working our way through an escalatory

chain in which there is a declaratory policy in which I tell you, "If you go any further, then I'm going to act in a certain way, and you can count on it." That should be a stick; I'd like to start with carrot, but if you force me to stick, this is the beginning of stick. So using it as a tool that you have for each of the countries is probably not the best use of declaratory policy. You'd really rather be working down here in nonproliferation, understanding what has driven that country to that, where do they want to end up, what can you do to help them help themselves go back to a position of comfort.

This is a campaign, this goes back to strategic communications, "Here's how we think it ought to go, we're starting to understand what's affecting you, why you believe what you do, it's either in our behavior or your behavior, but let's understand that, come to an agreement on it, and now what can we do to start to shape that in an appropriate way to get you more comfortable and us more comfortable." If I get to declaratory policy, that's in line with force deployment options and things like that. You're starting to posture, and you're way inside my comfort zone now. You've done something that I don't like, and it's making me nervous, and if you keep going in this direction, here's the stick that I'm going to hold.

JFQ: *Concerning your observation about the huge percentage of American businesses directly interfaced in a cyberworld and emerging cyber threats that are only 300 milliseconds away, is it necessary and possible for USSTRATCOM to influence changes in the architecture of the Internet?*

General Cartwright: The "Internet" is kind of a pseudonym for "networked environment," and the Internet tends to represent a more commercial application of the networks that has to do with information exchange, and generally, it's more social information. But networks at-large, whether commercial in nature, military in nature, governmental, etcetera, are where the bulk of American business is conducted, and they have huge implications in intellectual capital, people, in dollars and cents capital—on a daily basis, the transactions are huge.

They [networks] are global in nature; they tend to be self-policing to some extent, and the architecture is flexible enough that it will merge and morph in ways that protect it. But I'm going to give you two examples of, probably, the power and the unintended consequences side of this question. You go back to 1999, and a fellow in Saudi Arabia by the name of bin Laden is tossed out, and he goes to Afghanistan, and everybody goes, "Gee, bad guy, but what can he do from a cave?" At the same time, a student from Northeastern University by the name of [Shawn] Fanning is trying to figure out, "How can I use this peer-to-peer capability?" By most accounts, he takes around 25 percent of the music industry's profit in something called Napster. You can use this [technology] for good, or you can use this for bad; it depends on how you apply it. Do you change the architecture as a result of that? How do you treat this activity: as freedom of speech, or as a commodity that, when it crosses your border, you have the right to inspect? It all goes across the same kinds of pipes, it all gets intermixed. It doesn't pay much attention to geographic borders. Because of the Internet protocol activities, some of it may go through one country, and another part of the conversation or packet of information may go a different way—space, or someplace else. It goes extremely fast. So, "What is it and how do we treat it?" is a lot of the debate that's out there.

we probably erred on the conservative side to protect the use of the Net for everybody

I would say that we probably erred on the conservative side to protect the use of the Net for everybody. But let's equate that to the sea. When we did that on the sea, we tried to make sure that everybody could use the sea for commerce and have access and passage and a common set of rules, so we don't run into each other for the most part. But everybody had a right to be there, and we ensured that by creating a navy to have a presence on the sea. How do you look at this as an analogy—and is it a good analogy? Some of that debate is still going on, but you look at how the network has policed itself—in the case of Napster, in the case of intellectual property rights and how you treat them in the network—we haven't quite yet solved the problem of physical location. We've got some challenges in law because an American company operating on the network overseas has to be treated like it's an American company. Google, Yahoo!, MSN—those are American companies. If bin Laden wants to use them, he has every right to do it, and he's protected then by American law, not by Title 10. So how do these competing titles work in this network that just kind of throws all of that together in a hodge-podge? That's a challenge that's out there. But our principal activity is one of, when you talk about the architecture, is this is for Title 10 and for DOD [Department of Defense] and for STRATCOM, this is a weapons system. That helps us decide what the appropriate architecture is.

We have some advantages that the general business world won't have. If I tell Lance Corporal Cartwright, "You're not taking [your laptop] home, you're not plugging it in to those networks that are private, you're going to use this kind of a firewall, you're going to protect it in these ways, you're going to change your password, you're going to use some other type of identification or token," I can do that to Lance Corporal Cartwright. I'm not necessarily able to do that to the Cartwright on the street or in high school. And so what we're trying to do is stay inside the current construct, which says Homeland [DHS] is responsible for the United States Northern Command from a DOD standpoint.

When you start to spread out from the United States, then the layered defense capabilities belong to DOD, and we start to build a defense capability inside the United States, our bases, stations, places where we live are under DOD, so they are "dot-mil." We can start to have some control over it, we can standardize what's going on, we have the right to have a presence everywhere and know and see what's happening, so if there is a virus, or if there is an attack, or if there is exfiltration, we want to be able to start to register it, because we can be somewhat more intrusive on our military people than we can be on the general public. But what we're doing is building a domain that is more protected, so that when an attack occurs, we've got something to fall back on. Some of those practices are likely to be moved out to "dot-gov," and then "dot-edu," and on and on, to "dot-com." But they're probably going to be more driven by commercial practices.

My sense as an individual is that we hit that point in industry where they can no longer stand to absorb the losses of an attack while they wait for a patch and pass that financial burden on to the consumer. They are convinced they're going to have to be more aggressive about defending their networks and their intellectual property. That means there has to be a construct for the country. Usually what we try to do—this is the military—is to build a layered defense: get yourself out there far enough so that you can detect adversary activities that are coming toward you and have time to react. This millisecond thing is saying that from the other side of the world to this side of the world to that side of the world—it takes milliseconds. So how do we start to build a system in which we have presence in the littorals, so to speak, and out on the open sea or in the air, but really here in cyber[space]? How do you have a presence out there to see and know what is going on technically—how do you get yourself out there to the point where you can see at the speed of light what went by you, whether it was good or bad, report back, and reconfigure yourself for a defensive posture appropriate to that threat, before it gets there?

Those are the technologies that need to start to emerge both in the commercial sector and in the national security sector because that moves us from the idea of purely defending a terminal to registering the fact that there's a threat, doing something about it, and then deciding whether you want to take some action about it and acquiring attribution of who did this to you. That technology is where we've got to start to move to manage this medium in a way that is analogous to air, space, sea, etcetera, and thereby allow it to fit into the construct that we have, which is pretty much based in law, based on property, geographic boundaries, things like that.

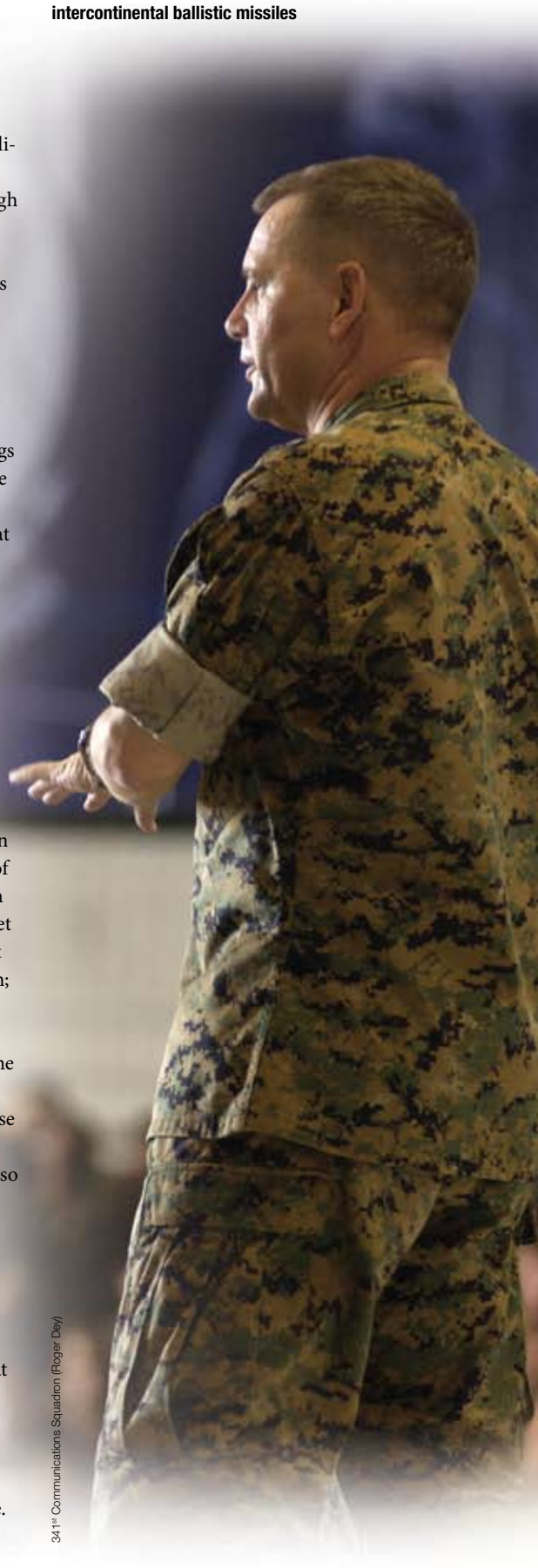
JFQ: *Building support for expensive military space programs is difficult when information about the space threat is shrouded in secrecy. How can we address the implications of the January 11, 2007, Chinese destruction of a weather satellite when we cannot easily communicate the enormity of the threat to the public?*

General Cartwright: In doing this in public fora, which we've done now in hearings and in the press, the activity is to forewarn, to understand that the Chinese have a defensive capability, a continuum capability that is a very deliberate plan on their part all the way from what we call temporary and reversible effects through this type of direct ascent, which is an expensive and forceful way of doing business, on up to more sophisticated and all the way to potentially nuclear capabilities to disrupt space and anything that flows through it. They're working their way through that continuum; they feel that's in their best interests.

To be fair, we've done this, the Russians have done this—we did this last in 1985, when we launched a direct ascent ASAT [antisatellite weapon] against a cooperative target. There are other things you get out of that: maneuvering guidance, navigation, the sophistication of boost, and all of those things start to come together; they [the Chinese] are on that same track. The difference here was, one, we had a couple of countries around that probably would have told you, "This doesn't make a lot of sense," and we abandoned it several years ago, as did the Russians, for a lot of good reasons. Two, if you're going to conduct those tests, there are collateral damages—the debris caused by such a test. The last test we did was in the 1985 time frame, and we did it down at the bottom of the belt of low Earth orbit, and we did it in a descending way, so that the debris would go down into the atmosphere and burn up. Even doing that, it was 2004 before the last piece of debris deorbited. So you're talking twentyish years for something that was optimized to get out of there quickly. Back then, there weren't quite as many assets in space. This is up high; it's going to have to migrate down through the International Space Station's altitude, it's going to have to migrate down through all the other parts of space, you're going to have to worry about it. If you want to—as the Chinese have said they want to do—go to the moon, you're going to have to go through this now, so manned flight is imperiled.

It's also a watershed event. You've now got another country that's decided to enter this activity, that, on the outside has said, "I don't want an arms race in space, I don't want to go to an armed space activity," and yet they're out there blowing things up. What should we do about that, what are the implications for United States space capabilities? Generally, the first question people ask us is if we need to go to an arms race. No, there's no reason to do that at this stage of the game. Just because you have a threat in space does

General Cartwright discusses the future of intercontinental ballistic missiles



341st Communications Squadron (Roger Dey)

not necessarily mean you have to address that threat in space. There are all sorts of other ways to get at that kind of a problem. When you go back to the continuum starting down at the nonkinetic stage, diplomatic activities and on up, there are plenty of ways to address that type of threat.

What we need to do now is to be more proactive in our situational awareness in space. Who's up there? We're going to have to have better awareness; we can't take a look at these things once a month and say, "It looks like it's okay, and the orbit is going to be in the same place when I go back again next month." There are too many objects now in the physical sense, and too much of the spectrum is used up in space, so interference in an electromagnetic way is also a problem. So we've got to become more proactive in that activity rather than just a cataloguing type of mindset.

Point two is, just going back to the analogy of the sea or air, the systems we put up there are going to have to be more aware of what's going on around them because you can't detect everything from Earth, and you want to be able to know that something's going on, having a sense of whether it's a natural phenomenon, or just a debris phenomenon, or whether it's something with intent. Usually it's electromagnetic in nature—people stealing time on cell phones, stealing entertainment channels—but piracy just like it occurs on land and in the air goes on up there. So we can start to build a collective awareness of what's going on in space. Those are the vectors that we need to be on.

JFQ: *A new National Space Policy was recently released in which uninhibited access to, or freedom of action in, space is a crucial prerequisite for all U.S. space activities. Realistically, can this policy be achieved when we are simultaneously committed to the peaceful use of space?*

what we need to do now is to be more proactive in our situational awareness in space

General Cartwright: Because we patrol the sea and have a presence there does not mean people can't get on it for peaceful purposes. It does not mean that if you have a border on the sea that you do not have rights to declare that border and treat it like any other border. Space shouldn't be any different. We should have the access, we should be able to operate up there to the extent that as the population goes up in space, so to speak, that we need rules like we have in driving, that we'll pass left to left or right to right, that we'll give each other a certain boundary of separation based on our ability to maneuver and see and perceive. Those ought to be brought in to ensure safe passage and somehow have to be enforced. It doesn't mean that you go up in space and you've got a little siren and a bubble light and you pull up, but it does mean that I'll call you if I sense that you're too close or if your spectrum is overlapping onto ours. But that doesn't mean that you go to space and you are a traffic cop or you have a weapon up there or something like that. I don't see those as being compelling activities that we need to move toward now. It's easy enough to call up two different owners in a spectrum dispute and say, "Somebody's stepping on the other guy. Go look at your health and maintenance data and see if your system is operating normally, and report back," and both of them say, "Yeah, we are," so somebody here is not working.

That's a lot easier than some of the other scenarios where, potentially, two parties build satellites. One is able to hold station physically in space better than the other, but they both have a slot that is X number of kilometers apart. If one is wandering around and can't be controlled, you're going to come to a decision that every time I turn around, I'm having to move mine because you're unable to hold station—those are the kinds of things that are likely to be harder to solve. What is the international body that we're going to use to have that conversation? How are we going to understand ground truths? Do we set standards before you go? If you violate standards once you're there and you put others at risk, how do we address that? We haven't gotten to a point yet where the activity is that driven, but you can see that that's going to happen, and it's no different than the naval example where you get, say, in straits, where it's got to be left to left, you've got to have a certain amount of distance because of maneuvering speed. We're not there yet, but you can see that's coming, both in the electromagnetic side and in the actual physical stationholding side.

I think we're moving in the right direction, we're probably moving as fast as the threat is emerging in that kind of a construct. There is money in space, there is commercial advantage in space, and usually when that happens, you have mischief. Thus far, it's been associated more with piracy-like activity of stealing signals, stealing bandwidth, potentially sliding into someone else's physical spot, something like that. You hope that that's

General Cartwright meets with Lieutenant General Robert J. Elder, Jr., USAF, Commander 8th Air Force

2d Communications Squadron (Sonya Padilla)

where it stays, but at some point, it could go differently. Those slots and that bandwidth are getting smaller and smaller, and they're in bigger demand, and the price is going up. Then you start creating haves and have-nots, and that's going to lead to some conflict eventually. We're not there yet, we're not even in a position, in my mind, where we need to posture ourselves for that kind of activity. We'd rather keep it at a low level, find the appropriate venue by which you can adjudicate those issues, and then do that down here on Earth.

JFQ: *Finally, sir, many in recent years have emphasized the critical importance of achieving unity of purpose and effort among diverse combatant commands and U.S. Government agencies and departments. How important is such cross-cutting collaboration for STRATCOM, and what are you doing to achieve it?*

General Cartwright: It's critical to us. Let me start first with kind of the emergence of global commands: TRANSCOM [U.S. Transportation Command], SOCOM [U.S. Special Operations Command], JFCOM [U.S. Joint Forces Command] to a certain extent, and STRATCOM, versus the geographic combatant commands. Each is unique, but the global commands tend to see things differently than a geographic command does. If you use a business analogy, the global commanders can provide scale to a problem but are not well positioned at the point of transaction in a business sense but at the point at which you interface with another country out there in a region. The geographic commander is going to have the nuance associated with a personal relationship, close observation, cultural expertise, etcetera, that a global commander won't have on a normal basis. So trying to provide him with the scale and breadth of capability that a global commander can bring to the table, and to move it to him when he needs it and to have it available for someone else when they need it, is more the model that we're trying to follow.

We're providing services of scale. Use intelligence, use space, use any of our mission areas. The geographic combatant commander has a certain amount of capability, but when things start to heat up, he's going to want to reach back for scale. He is still the best person positioned for the agility of day-to-day transactions and activities, whether that be in trying to defuse a crisis or in trying to defeat an adversary. What we're trying to do is provide in a service construct the ability to move scale to him for whatever objective he's trying to do, whether it's to defuse or to defeat. If we do it that way, that tends to keep the unity of command and unity of effort intact.

The challenge that's emerging today is that many of our sensors and capabilities are global in nature. Let's just take as an example the sensors associated with missile defense. Let's just use North Korea as an example, since we went through that with the Taepo Dong. If it launches from North Korea, that is a problem for USFK [United States Forces in Korea], but it immediately becomes a problem for PACOM [U.S. Pacific Command]. In its flight path, it will fly over Russia—that's EUCOM [U.S. European Command]. If NORTHCOM [U.S. Northern Command] decides the United States is threatened and decides to launch an interceptor, that's going to occur over Russia, and that's EUCOM again. So who's in charge? Who decides what sensors are aligned to that problem? Who decides when they're in maintenance and when they're being used? And some of those sensors belong to the Department of Defense, some belong to the Director of National Intelligence, some belong to other countries. How do you integrate that kind of activity?

The main kneejerk reaction was to give it to a global commander. But now you've taken a global commander who is not at the point of transaction of any of those things and inserted him into that activity. Our approach is to provide each one of them with the situation awareness they need for the function they're performing. If they're managing sensors, the launch of the vehicles, the basing, if they're the source of the attack, they need to know certain things to be able to function.

slots and bandwidth are getting smaller and smaller, and they're in bigger demand, and the price is going up

Build a command and control system that gives them that awareness, but don't rush to centralization of the activity. Try to find a tactical and command and control relationship that allows each of them to perform their function inside their area of regard.

The missile defense system was not initially designed that way. It was designed to have one person in charge, and their belief was that it was the person being attacked who ought to be in control. But is that where you're going to fight, or is the fight going to occur at the point where it [the attack] was initiated? What about this guy that was a third party and had a weapon of mass destruction destroyed over his head? So how are we going to do this? This is a big challenge. Our belief, though, is that the technology is there to devolve this down as far as you can to the person who is at the scene. Make them the strategic corporal; give them the tools to do what they need to do at that level. If there needs to be integration across this global activity that just crossed nine time zones and four combatant commanders, okay; provide the tool set and the CONOPS to work in that environment, but don't just take the control and centralize it immediately. It doesn't serve us well; it doesn't give us the agility at the point of activity that we're going to want to have. We did that, and we do that, at STRATCOM with nuclear weapons, but that's a little bit different in the regret factor, number one, and number two, the idea here is that we don't want to have to use those things. If somebody attacks you, you want to be able to defend yourself immediately, you don't want to negotiate that; self-defense is not negotiable. Much of command and control ought to put us in the mode of being able to do this work and not have to be in negotiation for the guy that's affected. You've got to be able to disperse this in a way that makes sense.

That's what that command and control system has got to bring to the table. But the guy who can best decide what to do is the guy at the site. That's the way we've got to design the system. Are we there technically? Technically, I think we've got it. Culturally, I think we've got to work our way through this—CONOPS, things like that, are just not ready for that kind of sophistication, but they're getting there. I believe that over the last year, the commands have come a long way in understanding how they can get their equities addressed and preserve unity of command in their AOR [area of responsibility], where they're responsible and accountable for the activities.

JFQ: *Thank you, sir.*

B–2 Spirit and F–15E Strike Eagles participate in U.S. Pacific Command's Global Strike

36th Communications Squadron (Cecilio Richardo)

Global and Theater Operations Integration

By ROBERT J. ELDER, JR.

Lieutenant General Robert J. Elder, Jr., USAF, is Commander, 8th Air Force, and Commander, Joint Functional Component Command for Global Strike and Integration, U.S. Strategic Command.

The Joint Functional Component Command for Global Strike and Integration (JFCC GSI) plays a critical role in integrating U.S. Strategic Command (USSTRATCOM) global capabilities into theater operations. JFCC GSI provides our leadership with a unique ability to command and control global strike capabilities, as well as to build a plan rapidly to integrate all military capabilities and quickly bring them to bear on the battlefield. During previous conflicts, commanders worked hard to deconflict, or synchronize timing of, effects on the battlefield to ensure safe passage of assets and efficient use of combat power. Now commanders need more. They need true integration of effects planning and execution, from situation identification, to early engagement shaping the environment, to rapid response and effects generation, to the long-term endurance that continues through conflict resolution and redeployment.

In today's global, information-dominated environment, effects tend to span all levels of conflict, from strategic to tactical. Simply synchronizing these effects is an incomplete approach; the words or actions of one individual on the battlefield or at a press conference can change the operational environment as never before. The U.S. military must focus on integrating its capabilities to ensure that all effects support objectives, from the lowest tactical level to the highest national level of policy.

That reality has USSTRATCOM focused on advocating new capabilities, such as rapid, global conventional weapons delivery, as well as deploying options that generate precise, predictable effects. Additional efforts to secure cyberspace and to upgrade existing capabilities through programs such as the Reliable Replacement Warhead will provide benefit to the GSI mission set. The JFCC GSI staff retooled USSTRATCOM operational processes and planning mechanisms to integrate the command's knowledge better. GSI has worked tirelessly to improve situational awareness through universal sharing of information, standardizing command and control capabilities, and focusing all command components on delivering the entire range of global effects.

JFCC GSI leads Global Strike planning for USSTRATCOM. Global Strike delivers timely effects against fleeting or high-value targets at global ranges. When theater forces are not in position to respond rapidly to a crisis situation, Global Strike is a readily available tool that fills a wide variety of needs, from flexible deterrence options designed to alter an adversary's decision calculus to a rapid strike capability designed to deliver devastating effects against adversaries of the United States and its allies. JFCC GSI, with direct support from the USSTRATCOM Combined Air Operations Center (CAOC) at Barksdale Air Force Base, Louisiana, is ready to plan and execute Global Strike missions today. GSI is the supported command for planning Global Strike and is capable of executing these missions in a lead role when directed. However, the command anticipates that most Global Strike missions will be executed by other combatant commanders with GSI in a supporting role. For that reason, GSI's ability to collaborate with combatant command staffs and their component commanders is of critical importance to the USSTRATCOM mission. GSI is using new collaborative, Web-based tools to lay the foundation for rapid, integrated theater input to the Global Strike planning process. In this way, GSI ensures that theater commanders are fully integrated with and able to take advantage of all USSTRATCOM Global Strike capabilities.

Global Strike delivers timely effects against fleeting or high-value targets at global ranges

JFCC GSI also leads the way with a pilot program to make a broad array of previously stovepiped data accessible, searchable, tailorable, and useable to warfighters at all levels. During Exercise Global Lightning 2007, USSTRATCOM utilized a Web-based tool to bring together people from multiple combatant commands, functional and Service components, mission areas, and scenarios in a fully collaborative environment. The command's situational awareness application, SKIweb, recorded 250,000 hits per minute on its server during the exercise. Warfighters were posting and pulling information constantly, enabling them to perform time-sensitive missions while keeping everyone within the environment on the same page and contributing. Certainly, more information is not always better. To quote General "Hoss" Cartwright, commander of USSTRATCOM, "If [the warfighter] needs a little [data] from here and a little from there, then [he] becomes the integrator [of that information] and that is fundamentally wrong. [The warfighter should not have to] integrate on the fly." JFCC GSI has taken on the challenge of integrating JFCC efforts. The goal is seamless, constant integration of processes and products, preventing the user from ever having to integrate "on the fly."

GSI has developed integration tools to help the warfighter discover and use actionable knowledge. The Global Operations Center Collaborative Environment (GOC–CE), based on commercial, off-the-shelf technology, is such a tool. GOC–CE maintains situational awareness, gathers information, and assembles it in one place for planners and decisionmakers alike. GOC–CE provides leadership with a dynamic, always current view about specific issues and provides other users with decisions already made. Planners can create editable spaces in a Web environment where specific information can be posted and acted upon. Others, from inside or outside the command, can add to this space, creating a useful, collaborative Web space for anyone with appropriate access. Within the command, GSI's Director of Intelligence utilizes collaborative tools and GOC–CE to bring together a wide array of knowledge and

expertise from the USSTRATCOM functional components and the national Intelligence Community. This allows the command to maintain a minimal intelligence staff and to leverage the expertise where it exists rather than duplicating it in multiple locations.

GOC–CE was used effectively in Global Lightning 2007 and is creating positive momentum toward Defense Department and USSTRATCOM network-centric objectives. Ongoing efforts to increase machine-to-machine data feeds will further reduce the time needed to gather and integrate information, create knowledge, and speed the decision cycle. Of course, all this information is useless without the proper means to display it to the warfighter. USSTRATCOM is working on a Blue Force Tracker application that will use a "Google Earth"–like capability to display forces in near real-time on everything from a desktop computer down to a hand-held device. Warfighters in theater can display what is needed and access a host of related data if they choose.

the goal is to enable the command to work seamlessly to deliver tailored effects, anywhere and anytime, across the globe

USSTRATCOM command and control capabilities previously were focused primarily on the nuclear mission. Today, General Cartwright's vision is to have a command and control structure that is modern, secure, and flexible, yet robust and broad enough to handle all of the command's missions—including intelligence, surveillance, and reconnaissance, integrated missile defense, space, network operations, combating weapons of mass destruction, and Global Strike. The goal is to enable the command to work seamlessly to deliver tailored effects, anywhere and anytime, across the globe. The mechanism includes networking with all other combatant commands and their components, as well as with the Defense Department and other government agencies.

JFCC GSI is providing flexible, responsive command and control via increased airborne bandwidth, distributed ground infrastructure, and enhanced data transfer capabilities. Additionally, GSI is leveraging USSTRATCOM CAOC capabilities during time-sensitive planning efforts. Soon, we will create a Global CAOC by deploying the capability to link all theater air operations centers (AOCs) with the CAOC, allowing shared data, applications, and solutions around the globe in a virtual environment. This will provide all theaters with access to better global situational awareness, Global Strike planning, and operations from 8th Air Force. It will also provide forward-located AOCs with resources not readily available in theater. These data initiatives, situational awareness tools, and effective command and control coupled with traditional and non-traditional Global Strike systems enable GSI to produce integrated global effects for the President or geographic commanders at an ever faster pace. This command and control initiative is a requisite for efficient and effective weapons system employment once a precise, prompt, conventional global-range strike capability is fielded.

Support Battle Staff operates during Exercise Global Guardian

DOD (Jeffrey Viano)

As we reduce the time required to decide and act, we also shape the future battlespace. In today's environment, we need to give warfighters in every theater a range of responses executable in minutes or milliseconds. The fast pace requires us to integrate our actions and get inside our adversaries' decision cycles. Providing joint force commanders with the tools and processes necessary for decisive action is critical, and GSI is delivering both of these today. Linking our AOCs virtually, standardizing operations data, and facilitating efficient collaborative arenas are all key to sharing information and reaching quick decisions, all of which help bridge the global and theater spectrum of operations at a moment's notice. **JFQ**

Joint Functional Command for Intelligence, Surveillance, and Reconnaissance

By JAMES L. DENTON

Intelligence, surveillance, and reconnaissance (ISR) operations continue to perform a vital role in the war on terror and promise to remain integral to current and future wars. That our military can execute the ISR mission has never been in question; the challenge is the efficiency, flexibility, and agility of that execution. The U.S. Strategic Command (USSTRATCOM) Joint Functional Component Command for Intelligence, Surveillance, and Reconnaissance (JFCC–ISR) is engaged in that challenge.

E–2C Hawkeye launches to conduct operations over Iraq

U.S. Navy (Liliana Verde)

Major James L. Denton, USAF, is Chief of the Joint Functional Component Command for Intelligence, Surveillance, and Reconnaissance Commander's Action Group.

Authorities

On January 10, 2003, President George W. Bush endorsed the reality that ISR touches every mission area from combating weapons of mass destruction to integrated missile defense to small unit operations. On that date, he signed Unified Command Plan 02, Change 2, which gave USSTRATCOM the responsibility for Department of Defense (DOD) ISR. This responsibility has transferred without change in subsequent plans, making the commander of USSTRATCOM responsible for the execution of the global ISR mission, which he chose to do through the creation of the JFCC–ISR. To meet those responsibilities, JFCC–ISR develops strategies and plans; integrates DOD, national, and international partner capabilities; and executes DOD ISR operations to satisfy combatant command and national operational and intelligence requirements.

Location

The JFCC–ISR uniquely integrates national and theater ISR expertise, forming an organization representing the entire DOD ISR enterprise. Located in the Defense Intelligence Analysis Center at Bolling Air Force Base, in Washington, DC, JFCC–ISR has ready access to all 16 agencies of the Intelligence Community. Toward that end, JFCC–ISR hosts ISR-associated mission partners to create integrated ISR planning and operations teams that perform the envisioned integration and synchronization. These partners include the Defense Intelligence Agency (DIA) Office for Collection Management, National Geospatial-Intelligence Agency, National Security Agency, National Reconnaissance Office, and representatives from the Service staffs.

The JFCC–ISR central location and access make it a valuable ISR focal point for DOD by helping to ease the frustration in communicating between the different Intelligence Community organizations and geographic combatant commands, thereby building trust within these organizations. Thousands of government and military professionals across these organizations are doing great work; JFCC–ISR helps to bring all of that effort together.

a benefit of the Defense Intelligence Agency location is the "across the hall" proximity to the Defense Joint Intelligence Operations Center

Defense Intelligence Analysis Center at Bolling Air Force Base, home of the JFCC–ISR

DOD

Relationships

A great benefit of the DIA location is the "across the hall" proximity to the Defense Joint Intelligence Operations Center (DJIOC). In fact, the two organizations are in the process of integrating their operations centers. Within 6 months, a call to either center will reach personnel from both organizations who, in turn, will work an ISR solution with the resources that the DJIOC, JFCC–ISR, and their mission partners bring to bear.

While the DJIOC handles "big picture" integration of our military's intelligence effort, the JFCC–ISR, including its mission partners, serves as the ISR arm of the DJIOC. The JFCC–ISR Operations Center keeps an enterprise-wide watchful eye on all assets using the ISR common operating picture. With future upgrades, the operations center will eventually monitor collection plans as they unfold in real time, signal deviations to those plans, instantly realign assets to the most important collection gaps, and export that same capability to key customers.

Operations

The JFCC–ISR theater teams work closely with the combatant commands, Services, national agencies, Joint Staff, and the DJIOC to make national and regional ISR integration happen daily. These regional teams operate on their respective regions' battle rhythm to develop courses of action and options to mitigate ISR capability risks and gaps to meet the geographic combatant commands' collection plans. They provide a single point for regional specific management questions.

Also focusing on our nation's ISR effort is the JFCC–ISR Assessments Division, which looks across the entire ISR enterprise to determine if there are better ways to optimize integration and allocation. This division recognizes that the ISR community is stressed; people and platforms are tired, saturated, and busy; and no one has the opportunity to step back from the day-to-day operations to ask, "Is there a better way?" That is the Assessments Division's responsibility: to help find a better way to do business and to get more out of limited resources as the intelligence demand continues to increase exponentially. Additionally, the division assists the USSTRATCOM commander's advocacy effort for capability investment. The division develops metrics to determine where the most value lies in current assets and activities, as well as where real gaps exist. These, in turn, inform the USSTRATCOM J8 recommendation about where to put the next ISR dollar.

the ISR Global Force Management model allocates forces to combatant commands based upon priorities of the war on terror

Integrating new and emerging capabilities into mission activities is the responsibility of the Special Access Division. This division monitors/leverages underutilized capabilities in the Special Access program arena that could answer our nation's ISR questions.

Shattered Molds

In keeping with the search for new business practices and using the expertise of its personnel and mission partners, the JFCC–ISR launched two ambitious initiatives to redefine ISR allocation and management. The first is a new ISR Global Force Management model that uses a mission-based approach to allocating ISR assets as opposed to a calendar-based one. This model allocates forces to combatant commands based upon priorities of the war on terror. It also provides a rotational force that moves through theaters during times when a combatant commander can anticipate an increased demand for ISR assets (such as yearly exercises or during political elections of countries of interest). This is in contrast with previous calendar-based allocation in which ISR assets rotated into theaters on an inflexible yearly basis and went underutilized during lulls in requirements.

In addition, the construct provides reserve response force assets, which are located at their respective home stations, meeting the important annual training requirements until a significant event occurs requiring a sudden, short duration plus-up of a combatant commander's ISR assets.

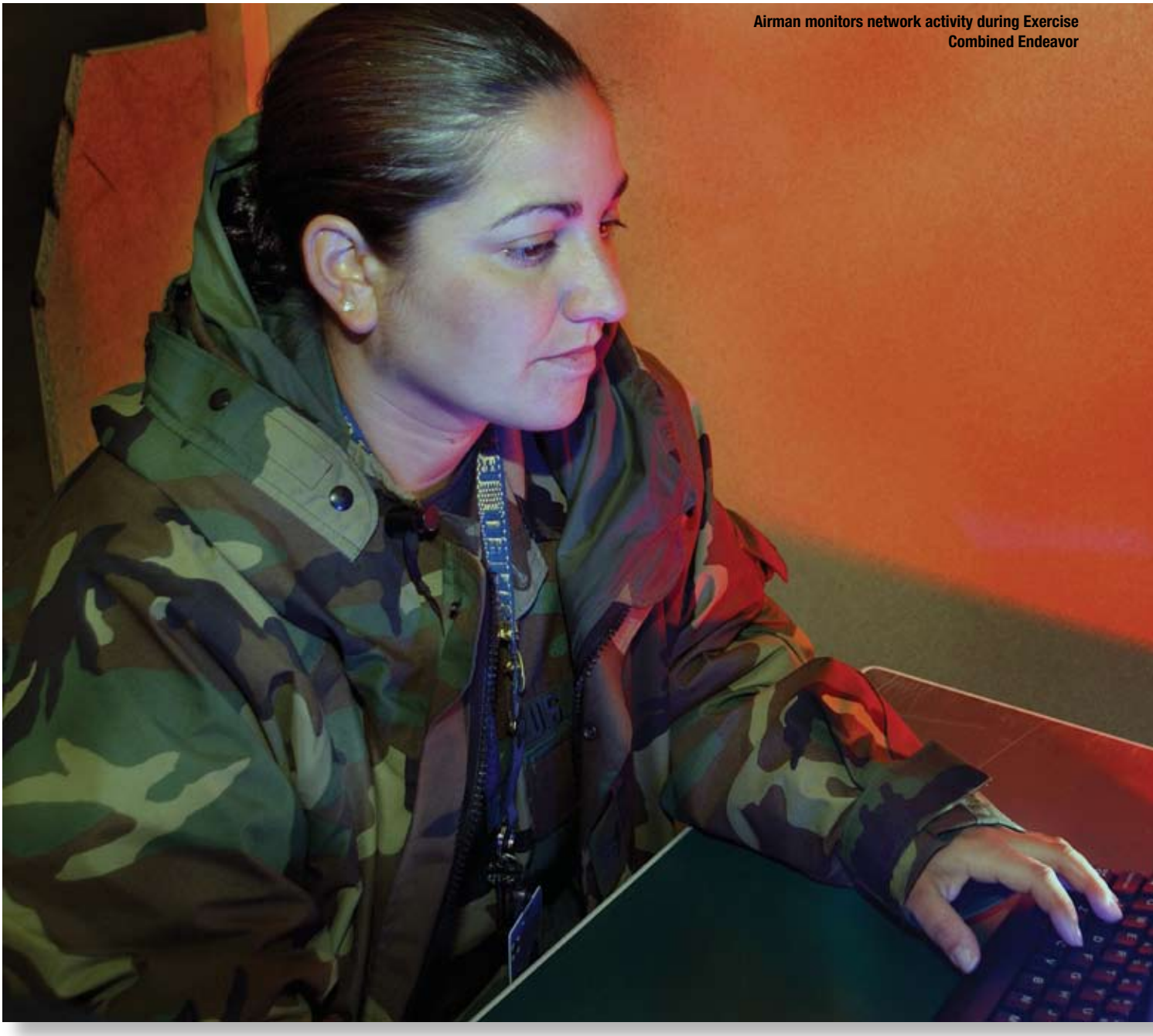
The second effort is the ISR transition. Knowing that no amount of money will equalize the disparity between capability and requirements for the overburdened ISR enterprise, JFCC–ISR is investigating ways to manage the global enterprise more effectively. On January 1, 2007, the ISR Transition Team launched an initiative to develop well-understood, practical, and executable best practices for operationally phased ISR support to the combatant commands. It will accomplish this by developing, testing, and implementing a set of coordinated ISR activities, processes, and tools designed to help combatant commands better meet their intelligence needs. The ISR Transition Team will use a spiral development process that examines discrete activities to address the areas of managing requirements, decisionmaking processes, force management, data-sharing capabilities, and assessments—areas where the potential for improvement is the greatest. The endstate of the ISR transition will be a commonly accepted, responsive global ISR management process based on DJIOC prioritization and flexible global force management that benefits the combatant commands and enables operations that are more effective.

Endstate

JFCC–ISR will continue to investigate better ways to manage the DOD ISR enterprise—from better relationships with members of the Intelligence Community, to combatant command–focused integration teams, to instant modification and reflowing of collection efforts, to new ISR business models. All of that effort focuses on satisfying our nation's significant and growing demand for intelligence. **JFQ**

Warfighting in Cyberspace

By KEITH B. ALEXANDER



Airman monitors network activity during Exercise Combined Endeavor

Lieutenant General Keith B. Alexander, USA, is Director, National Security Agency, and Commander, Joint Functional Component Command for Network Warfare.

Secretary of the Air Force, Michael W. Wynne, discusses creation of Cyberspace Command

U.S. Air Force (Cohen Young)

U.S. Air Force (Thomas Menequin)

Our current and potential adversaries clearly understand the military potential of cyberspace and the expansive power of the medium. Terrorists employ the Internet for recruiting, training, motivating, and synchronizing their followers. They can operate essentially unrestrained and are free to innovate, unbound by law, policy, or precedent. Nations such as China and Russia are developing their own "cyberspace warriors." China, for instance, has formed cyberspace battalions and regiments, the primary purpose of which is to identify and exploit weaknesses in our military, government, and commercial networks.[1] In November 1999, the *PLA Daily* stated, "Internet warfare is of equal significance to land, sea, and air power and requires its own military branch," and that "it is essential to have an all-conquering offensive technology and to develop software and technology for net offensives . . . able to launch attacks and countermeasures."

The threat from these forces is credible and real. While the time-tested principles of war will ultimately apply in cyberspace, its characteristics are so radically different that they demand significant innovation and changes to the way we organize and conduct military operations and tactics in this domain.

Many within the U.S. Government and private sector are beginning to recognize the importance of cyberspace (and operations within it) to national security. The March 2005 National Defense Strategy identified cyberspace as a new theater of operations and assessed cyberspace operations as a potentially disruptive challenge, concluding that in "rare instances, revolutionary technology and associated military innovation can fundamentally alter long-established concepts of warfare."[2] The Chairman of the Joint Chiefs of Staff concluded in the 2004 National Military Strategy:

The Armed Forces must have the ability to operate across the air, land, sea, space and cyberspace domains of the battlespace. Armed Forces must employ military capabilities to ensure access to these domains to protect the nation, forces in the field and U.S. global interests. . . . Along with technological solutions to improve joint war fighting, we must also examine our doctrine, organization, training, materiel, leadership and education, personnel and facilities to ensure military superiority.[3]

Despite this emphasis, however, we can argue that, while we have ample national level strategies, we have yet to translate these strategies into operational art through development of joint doctrine for cyberspace. Through the doctrine vetting process, we can develop a common understanding of what it means to conduct warfare within and through cyberspace. The ultimate strategic objective of these operations is to ensure U.S. freedom of action in cyberspace and to deny the enemy the same.

Development of cyberspace doctrine is a complex task; the only doctrine that currently addresses operations within the cyberspace environment is contained within two subsets of information operations (IO): computer network operations and electronic warfare (EW). Since computer network operations and EW are exclusively conducted through "the use of electronics and the electromagnetic spectrum," there is an overlap between IO activities and what our national strategy defines as military capabilities in the cyberspace domain (that is, cyber warfare). Although the defensive elements of IO and cyber warfare are important, to narrow the scope of our thesis, the remainder of the argument will principally focus on the offensive elements.

through the doctrine vetting process, we can develop a common understanding of what it means to conduct warfare within and through cyberspace

Joint Publication (JP) 3–13, *Information Operations*, defines *IO* as "the integrated employment of electronic warfare, computer network operations, psychological operations, military deception, and operations security, in concert with specified supporting and related capabilities, to influence, disrupt, corrupt, or usurp adversarial human and automated decisionmaking while protecting our own."[4] JP 3–13 also states "for the purpose of military operations, computer network operations are divided into computer network attack, computer network defense, and related computer network exploitation enabling operations."

Cyberspace as a Warfighting Domain

The common theme that runs through IO doctrine is its focus on affecting the human or automated cognitive or intellectual processing of information. JP 3–13 states, "The focus of IO is on the decisionmaker and the information environment in order to affect decisionmaking and thinking processes, knowledge, and understanding of the situation." Since the "ultimate strategic objective" of IO is "to deter a potential or actual adversary . . . from taking actions that threaten U.S. national interests," then to be successful, IO must encompass all actions taken by the U.S. Government. Even though the recent revision of JP 3–13 narrows IO doctrine to "five core capabilities," it still seeks to employ other "supporting and related capabilities" that in effect encompass nearly all Government actions.[5] Under IO doctrine, any statement we make, any movement of U.S. forces, or any bomb we drop could be considered a form of fires in an information operation if its principal intent is to influence adversary decisions away from taking action against our will.

Now, let us contrast IO doctrine with what we propose for cyber warfare. The focus of cyber warfare is on using cyberspace (by operating within or through it) to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability, while protecting our own. Instruments unique to cyber warfare are narrowly confined to those activities described in the definition: EW and computer network operations. When we conduct any military operation, we must integrate and synchronize all available instruments of warfare in all domains. It is clearly understood that land, maritime, air, and space warfare are, in and of themselves, important warfighting activities that ensure the U.S. military's ability to maintain freedom of action while denying an adversary the same. Although it is understood that land, maritime, air, and space warfare will be employed to deter (for example, influence) an adversary, no one believes that warfare within these domains is uniquely "information operations." Where the principal effect of IO is to influence an adversary *not* to take an action, the principal effect of cyber warfare is to deny the enemy freedom of action in cyberspace. Granted, by denying enemies' freedom of action in cyberspace, we will also influence them; however, influence is not the intended primary effect—denying freedom of action is the intended primary effect.

Airmen monitor Internet traffic

U.S. Air Force (Jack Braden)

It may seem that we are arguing to remove EW and computer network operations from IO doctrine. We are not. What we are arguing for is that just as we have now come to recognize cyberspace as a new warfighting domain, so too must we recognize that it is equal to the other warfighting domains and doctrine should reflect such. Now is the time to update our doctrine to establish fundamental cyber warfare principles that guide employment of EW and computer network operations forces in support of our national objectives.

Operationalizing Cyberspace Warfare

U.S. Strategic Command (USSTRATCOM) has already begun to implement this shift. The commander, beginning in Unified Command Plan (UCP) 2002 and carried forth in subsequent UCPs, was given the responsibility for "integrating and coordinating [Department of Defense] IO that cross geographic areas of responsibility or across the core IO capabilities, including identifying desired characteristics and capabilities for computer network attack and conducting computer network attack in support of other combatant commanders, as directed."[6] USSTRATCOM is moving to shift operational focus from the cognitive effects, described

the principal effect of cyber warfare is to deny the enemy freedom of action in cyberspace

within IO, to a common planning framework for the Defense Department to achieve specific cyberspace objectives. We have redefined our cyberspace mission area in terms of offensive–network warfare (NW) and defensive–network operations (NetOps)—and established JFCC–NW and JTF–GNO to address each of those mission sets, respectively.

As directed by the USSTRATCOM commander, the Joint Functional Component Command for Network Warfare (JFCC–NW) was established to "optimize planning, execution, and force management for the assigned missions of deterring attacks against the United States, its territories, possessions, and bases, and employing appropriate forces should deterrence fail, and the associated mission of integrating and coordinating [Defense Department] CNA [computer network attack] and computer network defense as directed by headquarters USSTRATCOM."[7] The command further defines *network warfare* as "the employment of computer network operations with the intent of denying adversaries the effective use of their own computers, information systems, and networks."[8] This mission statement recognizes the primacy of the strike or attack aspects of computer network attacks as a military fire, not merely as an enabler for cognitive effects.

USSTRATCOM has also begun to develop tactics, techniques, and procedures and other concepts designed to integrate cyberspace capabilities into cross-mission strike plans. We are developing concepts to address warfighting in cyberspace in order to assure freedom of action in cyberspace for the United States and our allies while denying adversaries and providing cyberspace-enabled effects to support operations in other domains.[9] These concepts, and the cyberspace effects that they focus on, are clearly based on the military concepts of strike, fires (supporting and suppressing), and defense.

While the concepts of NW and NetOps are a good start, they represent only a small subset of the elements of military power available within or enabled by cyberspace. In order to fully engage in the development of joint doctrine within the cyberspace domain, it is also necessary to develop a definition of exactly what warfare within cyberspace—or cyberspace warfare—is.

JP–1 describes a joint doctrine development process that starts with a project proposal and then moves through a program directive, developing and staffing drafts prior to receiving approval from the Chairman of the Joint Chiefs of Staff. We need to engage this process to codify the planning, operational, and support systems required to execute this rapidly emerging form of warfare that focuses on how we will plan and execute operations within the arena. Our challenge is establishing recognizable doctrine that will include definitions and fundamental principles to guide the employment of military forces and weapon systems for operations within the cyberspace domain.

In coming to grips with military operations in cyberspace, we face many challenges that are strikingly similar to what our military faced during the Interwar Years from 1919 to 1938. During this period, the military struggled with mechanization and the revolution in military affairs that it fostered. Airpower in particular came into its own, but not without great frustration and sacrifice on the part of visionary airpower advocates. Despite significant advances in air combat during World War I, the Army, which controlled most U.S. airpower, was hesitant to move forward. Only after nearly 20 years of struggle and the high-profile court martial of Billy Mitchell were airpower advocates able to make the advances in operations, tactics, and materiel in the air domain that proved crucial to the Allied victory in World War II.

The speed at which the cyberspace domain is evolving and its ever-growing impact on national security make this potentially as critical a period as that faced by Mitchell, Claire Chennault, and their contemporaries as they realized the potential of the air domain and sought to develop airpower doctrine. Unfortunately, we do not have the luxury of 20 years to develop strategy, tactics, and doctrine to deal with this revolution and maintain U.S. superiority in this rapidly changing environment. The trends for advances in technology, often (correctly or incorrectly) related to Moore's Law and derivative theories, such as the Law of Accelerating Returns proposed by Ray Kurzweil in his 2001 essay, dictate that we must move quickly.[10] If one examines the advances in Internet and computer technology in just the last 5 years, it is readily apparent that we could find ourselves behind or even militarily irrelevant in cyberspace.

USSTRATCOM has also begun to develop tactics, techniques, and procedures and other concepts designed to integrate cyberspace capabilities into cross-mission strike plans

It is imperative that we capture the lessons learned associated with previous revolutions in military affairs and move quickly and decisively. We must make a dedicated joint effort to develop the forces that will fight and defend our national interests in cyberspace, and we must diligently develop the training and doctrine that will guide them as they execute their critical missions in this new military domain. **JFQ**

NOTES

[1] Timothy L. Thomas, *Dragon Bytes, Chinese Information War Theory and Practice* (Fort Leavenworth, KS: Foreign Military Studies Office, 2004), 52–74.

[2] *The National Defense Strategy of the United States of America* (Washington, DC: Office of the Secretary of Defense, March 2005), 4.

[3] *The National Military Strategy of the United States of America* (Washington, DC: Office of the Chairman of the Joint Chiefs of Staff, 2004), 18, 23.

[4] Joint Publication 3–13, *Information Operations*, February 13, 2006, available at <www.dtic.mil/doctrine/jel/new_pubs/jp3_13.pdf>.

[5] Recent changes were driven less by operational need to adjust doctrine than by bureaucratic politics. It was principally an effort by individual communities of interest to maintain their hegemony over their domains and not be absorbed into the burgeoning "information operations" bureaucracy. Hence, their new definition of "five core capabilities" and other "supporting and related activities."

[6] Unified Command Plan 2004, March 1, 2005.

[7] JFCC–NW Implementation Directive, January 20, 2005.

[8] Ibid.

[9] USSTRATCOM Brief, January 11, 2007.

[10] Ray Kurzweil, "Law of Accelerating Returns," 2001, available at <http://lifeboat.com/ex/law.of.accelerating.returns>.

Space Operations

By WILLIAM L. SHELTON

The commander, U.S. Strategic Command (USSTRATCOM), established the Joint Functional Component Command for Space (JFCC SPACE) to optimize planning, execution, and force management of Department of Defense space operations. The commander, 14th Air Force, was designated as the commander, JFCC SPACE, to conduct space operations, exercise operational control of designated space and missile warning forces on behalf of the USSTRATCOM commander, and act as the Global Space Coordinating Authority. As coordinating authority, the commander of JFCC SPACE ensures unity of effort by developing, coordinating, and conducting operational-level space campaign planning and strategy development in support of U.S. Strategic Command and other combatant commands.

Through the planning and execution of space control, support, and force enhancement operations, the JFCC SPACE commander produces effects for combatant commanders, such as providing positioning, navigation, and timing for military and civil use; providing communications to remote locations beyond the line of sight of terrestrial communication systems; and supporting battlespace awareness and characterization

Accessing satellite information at the Space and Missile Systems Center

U.S. Air Force (Jose Hernandez)

Titan IV–B rocket launches carrying a National Reconnaissance Office satellite

U.S. Air Force (Pamela Taubman)

through space systems. The desired JFCC SPACE endstate is unity of command and effort in the unimpeded delivery of full-spectrum joint space effects to supported commanders and the ability to deny the benefits of the space medium to adversaries for purposes hostile to the United States. In order to reach this desired endstate, the United States must have robust, efficient, and effective space-based capabilities. Also, our operations centers (the Joint Space Operations Center and the Air Operations Centers) must work closely together to deliver the space effects that combatant commanders demand.

To ensure that the United States and its allies have the freedom to operate in space, the JFCC SPACE commander focuses first and foremost on attaining more persistent, predictive space situational awareness that is integrated with all-source intelligence. By extending battlespace awareness into the medium of space, this space situational awareness gives the commander access to the indications and warnings that can characterize an adversary's capability and intent. With improved space situational awareness as a foundational capability, the commander can build a campaign plan, based on combatant command objectives, to execute tactical-level operations related to satellite operations, missile warning, defensive space control, and offensive space control. Space situational awareness thus enables command and control of space resources to achieve desired space effects.

The successful integration of space-based capabilities into U.S. military operations increases reliance on, and demand for, those capabilities. The 2006 National Space Policy highlights the fact that the Nation "is critically dependent on space capabilities, and this capability will grow." Growth in the use and exploitation of space increases the threat in the space medium, following the historical precedent of the use of ground, air, and cyberspace media. Protecting space assets against attack and characterizing and assessing anomalous events as potential attacks on space assets are extremely complex undertakings. But they are absolute prerequisites for ensuring that space capabilities are available to further U.S. national security, homeland security, and foreign policy objectives.

space situational awareness gives the commander indications and warnings that can characterize an adversary's capability and intent

With an eye to the future, the JFCC SPACE commander's priorities include improving space situational awareness capabilities, strengthening Defense Department partnerships, and developing tactics, techniques, and procedures to execute defensive space control operations, thereby protecting our vital space capabilities. Near-term milestones include collocating the Space Control Center, currently located at Cheyenne Mountain, Colorado, with the Joint Space Operations Center at Vandenberg Air Force Base, California; advocating upgrades to improve space situational awareness; and providing the command and control capability that produces timely space effects for combatant commanders. **JFQ**

Major General William L. Shelton, USAF, is Commander, 14th Air Force, Air Force Space Command, and Commander, Joint Functional Component Command for Space, U.S. Strategic Command, Vandenberg Air Force Base, California.

Standard Missile–3 interceptor launches from USS *Shiloh* as part of AEGIS Ballistic Missile Defense test

U.S. Navy

Integrated Missile Defense

By KEVIN T. CAMPBELL

The Joint Functional Component Command for Integrated Missile Defense (JFCC–IMD) was established in January 2005. Its primary mission is to conduct functions for global missile defense to protect the United States, its deployed forces, friends, and allies from ballistic missile attacks. Because of the missile defense infrastructures available in Colorado Springs, Colorado, JFCC–IMD established its operations center at the Joint National Integration Center at Schriever Air Force Base. Both the Center and the base were specifically chosen to enable JFCC–IMD to leverage the plethora of developmental and test resources from the Missile Defense Agency, as well as to afford direct access to the Army's Ground-based Midcourse Defense Missile Defense Element and U.S. Northern Command. By collocating at the Joint National Integration Center, JFCC–IMD is uniquely positioned to provide seamless collaboration between the warfighters and developers to operationalize ballistic missile defense system (BMDS) capabilities and to facilitate transition of dual-use and multi-mission capabilities to service various operations and development missions.

This past year has seen operational achievement for integrated missile defense. JFCC–IMD, in partnership with the Missile Defense Agency and various geographic combatant commands (GCCs), activated limited defensive operations, a significant milestone for the integrated missile defense. The declaration of limited defensive operations was unprecedented in many ways; for the first time, the United States is protected from ballistic missile attacks. JFCC–IMD meticulously manages these capabilities to service multiple missions and the GCCs while facilitating a smooth transition of these shared assets between multiple operations and research and development missions to ensure that U.S. interests around the world are afforded the highest protection level. Additionally, we have experienced unprecedented integration of various intelligence capabilities to enable timely and responsive indication and warnings to support missile defense readiness.

JFCC–IMD allowed warfighters to participate in the first distributed ground tests on the actual operational system, geographically spread from Colorado to Alaska and from Washington, DC, to Japan. These tests demonstrated the sophistication and complexity of BMDS assessments that are

Lieutenant General Kevin T. Campbell, USA, is Commander, U.S. Army Space and Missile Defense Command, and Commander, Joint Functional Component Command for Integrated Missile Defense, U.S. Strategic Command.

increasingly relevant. They included the increased numbers of AEGIS tracking and engagement ships, ground-based interceptors in Alaska, and the Forward-Based X-Band-Transportable and Sea-Based X-Band radars.

These and other system-level tests also underscored the warfighter's need to expedite development and deployment of the concurrent test training and operations capability to enable conduct of realistic tests without sacrificing operational readiness of the integrated missile defense capability. The need for the concurrent test training and operations capability is especially pronounced for the unique assets shared by the warfighter, developer, and trainer communities.

The July 4, 2006, North Korean missile launches helped streamline planning and operations. We learned that the system, procedures, and personnel performed well and demonstrated an initial operational missile defense capability for homeland defense. These actions validated our concept for ballistic missile defense and created worldwide interest and increased allied commitment. Initial investments by the North Atlantic Treaty Organization in the construction of a ballistic missile defense command and control system, along with growing interest by countries throughout the world in hosting both radar and interceptor bases, are testaments to this success, demonstrating a deterrent value to near-peer and emerging nations. Japan has accelerated an expanded cooperation program with the United States for ballistic missile defense, and South Korea has committed to developing short-range ballistic missile defenses.

The JFCC–IMD global missile defense exercise program also extended internationally through synchronizing various exercises involving key allied partners to maintain our commitment for mutual defense and to experiment with new methods and technologies in order to maximize collective effectiveness. These international exercises further bolstered allies' resolve in conducting combined missile defense operations and extending partnership into codevelopment of future capabilities.

JFCC–IMD is actively engaged in Weapons Release Authority development and execution, Global Force Management, Global Sensor Management (including intelligence and space), Single Integrating Authority for cruise missile defense, and development of plans and procedures (for example, concept of operations and tactics, techniques, and procedures) for emerging systems. A global concept of operations for missile defense will be coordinated in collaboration with the GCCs early this year. The valuable experience and the lessons learned from the past 2 years of BMDS activation and operations formed the basis of this strategic plan.

We are increasing the sophistication and integration capability of the Command Control Battle Management and Communication System to provide essential information to key warfighters in order to plan and execute missile defense missions in near real-time. We look forward to extending the Command Control Battle Management and Communication capability to further the "all sensors–all shooters" principle to implement the integrated missile defense policies and doctrines.

As we move forward in the next year, much work remains to be done. We will continue to integrate and conduct cross-GCC plans and exercises, integrate new capabilities, and increase ally involvement in global missile defense. Our continuing goal is to develop a seamless missile defense capability that integrates all available capabilities to deter and dissuade proliferation of missile threats—and to defeat them in order to protect our nation, deployed forces, friends, and allies. **JFQ**

we have experienced unprecedented integration of various intelligence capabilities to enable timely and responsive indication and warnings

Sea-Based X-Band Radar used for ballistic missile detection

U.S. Navy (John Jackson)

A New Era in Combating WMD

By JAMES A. TEGNELIA

French sailors train as part of multinational Proliferation Security Initiative exercise

U.S. Navy (Justin Thomas)

The President's *National Strategy to Combat Weapons of Mass Destruction* describes such weapons in the hands of hostile states and terrorists as one of the greatest security challenges facing the United States. This strategy reinforces the need for the Department of Defense (DOD) to continue developing an integrated and comprehensive approach to counter the weapons of mass destruction (WMD) threat. As an essential step toward that approach, the Secretary of Defense assigned the commander, U.S. Strategic Command (USSTRATCOM), as the lead combatant commander for integrating and synchronizing DOD efforts in combating WMD.

The combating WMD mission entails the integration and synchronization of DOD-wide efforts across the doctrine, organization, training, materiel, leadership, personnel, and facilities (DOTMLPF) spectrum. The President further codified responsibilities and authorities assigned to the USSTRATCOM commander in the Unified Command Plan of May 5, 2006. In answer to this assignment, the commander established the USSTRATCOM Center for Combating Weapons of Mass Destruction (SCC–WMD), which is collocated with the Defense Threat Reduction Agency (DTRA) at Fort Belvoir, Virginia. To support this vital mission further, the Secretary of Defense dual-hatted the director of DTRA as the director of the SCC–WMD. This mission and collocation allow USSTRATCOM and SCC–WMD to leverage DTRA's vast technical expertise.

At the strategic level, preventing hostile states and nonstate actors from acquiring or using WMD is one of the four priorities identified in the 2006 Quadrennial Defense Review (QDR). This is the first time a QDR has devoted such attention to the threat of WMD. Also at the strategic level, the Chairman of the Joint Chiefs of Staff on February 13, 2006, issued the first-ever *National Military Strategy to Combat Weapons of Mass Destruction*. This strategy builds on the three-pillar structure of the 2002 national strategy. As defined in the national military strategy, these pillars are:

- *Nonproliferation:* actions to prevent the proliferation of WMD by dissuading or impeding access to, or distribution of, sensitive technologies, materiel, and expertise
- *Counterproliferation*: actions to defeat the threat or use of WMD against the United States, U.S. Armed Forces, allies, and partners
- *Consequence Management*: actions taken to mitigate the effects of a WMD attack or event and restore essential operations and services at home and abroad.

At the next level, the national military strategy identifies eight mission areas that span the pillars in the national strategy: offensive operations, elimination, interdiction, active defense, passive defense, consequence management, security cooperation and partner activities, and threat reduction cooperation. This new strategic framework is the DOD vehicle for dividing the broad combating WMD mission into specific, definable military activities that better address the DOTMLPF spectrum with more focus on the budget, training, doctrine, and policy processes.

Initially established in August 2005, the SCC–WMD develops and maintains global situational awareness of WMD activities, advocates for combating WMD capabilities, and assists with WMD planning, while shifting emphasis from a DOD-centric approach toward interagency solutions.

The SCC–WMD has faced and overcome many of the challenges associated with standing up a new organization and is making significant progress. It continues to forge enduring relationships throughout DOD and other governmental organizations and has embraced DTRA's existing capabilities and expertise by capitalizing on its traditional areas of chemical, biological, radiological, and nuclear expertise and its longstanding relationships with the combatant commands, Services, national agencies, and other governmental organizations.

the 2006 Quadrennial Defense Review is the first time a QDR has devoted such attention to the threat of WMD

The SCC–WMD was declared "fully operational capable" on December 31, 2006, with initial emphasis on the WMD elimination and interdiction mission areas. *Elimination* supports the systematic seizure, security, removal, disablement, or destruction of a

Dr. James A. Tegnelia is Director of the Defense Threat Reduction Agency. He is also Director of the U.S. Strategic Command Center for Combating Weapons of Mass Destruction.

hostile state or nonstate actor's capability to research, develop, test, produce, store, deploy, or employ WMD, delivery systems, related technologies, or technical expertise. *Interdiction* is defined as operations to track, intercept, search, divert, seize, or stop trafficking of WMD, delivery systems, related materials, technologies, and expertise to/from state or nonstate actors of proliferation concern.

SCC–WMD successes in the elimination mission area include the development of a concept of operations that describes the overarching mission area at the strategic level and defines the desired capabilities for both a Joint Task Force–Elimination and the Joint Elimination Coordination Element. A capabilities-based document designed to support policy and combatant command planning in the near term (2–7 years), the elimination concept of operations enumerates the roles and responsibilities of DOD components and interagency partners while outlining a construct for operational planning for the elimination mission. The elimination concept is currently out for final general officer/flag officer review and should be published as a handbook in the spring or summer of 2007 by the director of the Joint Staff.

The 2006 QDR directed DOD to establish a deployable joint task force headquarters for WMD elimination that is able to provide immediate command and control for forces executing those missions, as well as expand the Army's 20th Support Command's capabilities to enable it to serve as a joint task force capable of rapid deployment to command and control WMD elimination and site exploitation missions. In support of this task, the SCC–WMD successfully executed the Joint Capabilities Integration and Development System DOTMLPF Change Recommendation process to gain Joint Requirements Oversight Council recommendation for the Joint Elimination Coordination Element, which will be a rapidly deployable, 30-person command and control component capable of augmenting either an established joint force component command or joint task force headquarters specifically tasked to conduct WMD elimination operations. It will also coordinate with combatant commands, components, Services, Defense agencies, and units that may conduct WMD elimination missions on a day-to-day basis for WMD elimination training and exercise support.

the combating WMD common operational picture will provide a Web-based forum for community planners, analysts, and decisionmakers

The SCC–WMD is also leading USSTRATCOM support for the WMD interdiction mission and Proliferation Security Initiative activities. In support of the WMD interdiction mission, center personnel provide support to the Office of the Under Secretary of Defense (Policy), Chairman of the Joint Chiefs of Staff, and combatant commands to implement the 2006 QDR unity of effort paradigm in coordination with the National Counterproliferation Center and several National Security Council–established interagency forums focused on the WMD interdiction mission. The center also provides operational and exercise support for Proliferation Security Initiative activities and exercises, most recently as a participant in Exercise Leading Edge 07, which focused on maritime interdiction.

To track all of these efforts, the SCC–WMD maintains 24-hour situational awareness of critical combating WMD efforts and information. Combating WMD situational awareness is achieved through fusing regional expertise, open source knowledge, and technical information; connecting evidence, knowledge, and information related to past and current events; then applying analytical rigor to anticipate future events. The DTRA Operations Center's 24/7 collaborative environment supports the SCC–WMD and facilitates tracking of WMD operations by depicting these events globally through a common operational picture, which went online at the classified level in the spring of 2007. The combating WMD common operational picture will provide a Web-based forum for community planners, analysts, and decisionmakers to increase awareness of global combating WMD activities and to serve as a one-stop shop for global combating WMD situational awareness.

As the threat of WMD proliferation grows, the SCC–WMD stands ready to meet the challenges. Through innovation and collaboration, the center is helping members of the WMD community to anticipate, counter, and respond to threats. The SCC–WMD leadership and personnel understand the need for constant vigilance, and they share the President's vision to protect the United States, its forces, and allies from weapons of mass destruction. **JFQ**

U.S. Navy (Stephen Weaver)

USS *Gonzalez* participates in exercise as part of Proliferation Security Initiative

Guarding

Airman loads security updates for network at Balad Air Base, Iraq

31st Communications Squadron (Michael Holzworth)

Cyberspace
Global Network Operations

By CHARLES E. CROOM, JR.

President George Bush's *National Strategy to Secure Cyberspace* (NSSC) describes cyberspace as the nervous system of our country. The NSSC outlines—for all Federal, state, and local governments, private companies and organizations, and individual Americans—a framework to deter adversaries and assure cyberspace freedoms.

Today, instant cyberspace communication has forever changed and flattened our world. Cyberspace provides unprecedented access to goods, services, and information in a world that is fundamentally more complex than ever before. It drives the global economy and connects people in ever-changing contexts. It also creates *dependencies* in every element of a society's infrastructure: transportation, banking, public utilities, education, governance, diplomacy, and national defense. And no nation is more dependent on cyberspace than ours.

Dependence creates vulnerability, and nothing is more inherently vulnerable than cyberspace. Like previous eras, ours is populated by outlaws and charlatans, thieves and pirates, who threaten the viability of the domain in the name of greed, political or ideological hegemony, or military advantage. What is required is a change in our view of cyberspace: as a matter of national interest and national security, it must be viewed as *battlespace*.

With that operational perspective, cyberspace becomes a warfighting domain—akin to land, sea, and air—where we are engaged in defending our national interests and security. Our society is linked in cyberspace. We are network-centric: network-dependent and network-defined. This "net-centricity" must be defended, just as any other element of our society must be defended.

The weapons system leading the battle is the Department of Defense Global Information Grid (DOD GIG).

Basic to this notion is the integration of cyberspace capabilities across the full range of military operations. The designated military lead for cyberspace operations,

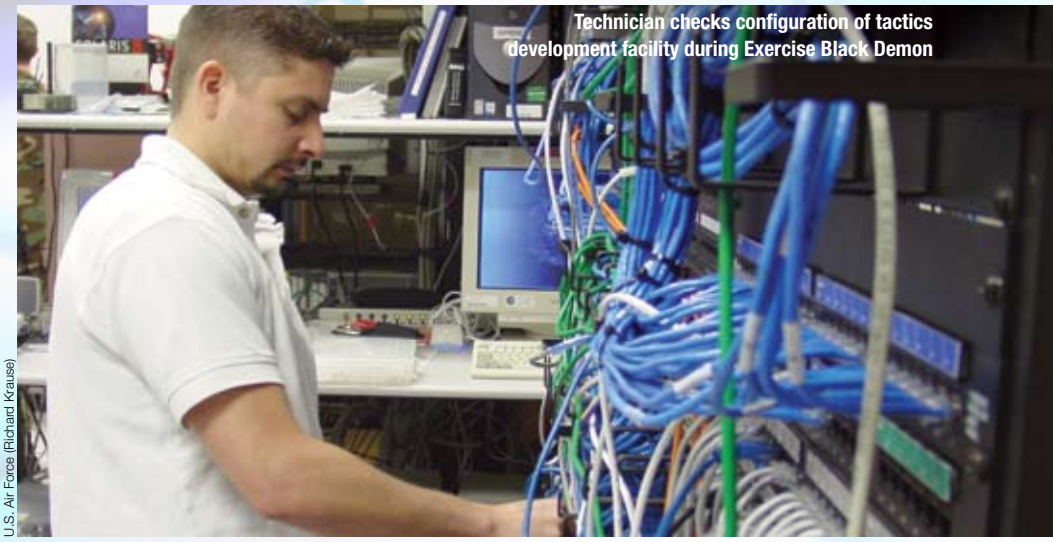
> *as a matter of national interest and national security, cyberspace must be viewed as* battlespace

U.S. Strategic Command (USSTRATCOM), directs the operation and defense of the DOD GIG to assure timely and secure net-centric capabilities in support of the full spectrum of warfighting, intelligence, and business missions. This is the frontline of the new battlespace.

USSTRATCOM's agent for this action is the Joint Task Force–Global Network Operations (JTF–GNO), which was created out of a series of real-world cyber events in 1997 that targeted DOD networks. Those events clearly showed two things: the vulnerability of DOD mission-essential computer assets and the need for a single organization with the appropriate levels of authority to defend these globally interconnected networks, associated information capabilities, processes, and information.

The JTF–GNO manages four overarching concerns: *who* is on the GIG, *what* does the GIG look like, *where* are the vulnerabilities, and *how* can risks be mitigated? The JTF–GNO addresses those concerns by serving as the fusion point for its mission partners and producing alerts, bulletins, assessments, and tasking orders. In addition, it manages the status of Information Condition (INFOCON), the alert system governing the defensive tactics and policies that users of the GIG need to follow.

The GIG is hit with millions of scans every day, and while the vast majority are deflected, each must be treated as a potential intrusion attempt. Complicating this effort



Technician checks configuration of tactics development facility during Exercise Black Demon

U.S. Air Force (Richard Krause)

Lieutenant General Charles E. Croom, Jr., USAF, is Director, Defense Information Systems Agency. He is also Commander, Joint Task Force–Global Network Operations, U.S. Strategic Command.


Airman checks SIPRNET security at Ramstein Air Base, Germany

U.S. Air Force (Latonia Brown)

is the fact that our information management systems are largely based on commercial software—the same software available to adversaries and malicious actors. Advances in computer information technology are available *globally*, making the threat to the GIG extensive, pervasive, and increasingly sophisticated.

This battlespace demands a proactive, preventive capability; a flexible, layered defense; rapid detection; robust response options; shared situational awareness across cyber domains; timely warning of impending attacks; effective defensive tools; and measures to defeat attacks as they occur. Cyberspace is the only domain where all instruments of national power (diplomatic, informational, military, and economic) can be exercised simultaneously, yet it is also the only place where our infrastructures can be attacked from obscure launching sites at the speed of light.

As a consequence, the JTF–GNO must provide guaranteed availability of systems and networks, assured delivery, and protection of information. By bringing this balance of capabilities to the DOD information environment, with potentially vast implications for mission success, the JTF–GNO unites all users of the GIG with common standards and processes through a doctrinal construct known as the Joint Concept of Operations for GIG Network Operations (NetOps CONOPS).

The USSTRATCOM commander articulated the specifics of the CONOPS, which provides the operational framework and command and control structure to combine the disciplines of enterprise systems and network management, network defense, and content management. These three essential tasks, as well as command and control and situational awareness, are the fundamental components of NetOps.

Each essential task has a specific body of objectives. Where network management is concerned, NetOps relies on the understanding, application, and integration of information technology, technology standards, and standard processes that provide traditional systems and network management (fault management, configuration management, accounting management, performance management, and security management). NetOps enterprise management consists of the many elements and processes needed to communicate across the full spectrum of the GIG and includes enterprise services management, systems management, network management, satellite communications management, and electromagnetic spectrum management.

content management seeks to make data visible, discoverable, and understandable

At the same time, network defense includes USSTRATCOM's operational responsibilities for information assurance, computer network defense, critical infrastructure protection, and other GIG defense tasks. NetOps is not intended to replace institutional practices of information assurance and computer network defense but to enhance them through a comprehensive process of protection, monitoring, detection, analysis, and response.

Finally, content management involves the ability to "maneuver information across GIG terrestrial, space, airborne, and wireless environments." It supports the broad DOD data strategy that seeks to make data visible, discoverable, and understandable.

NetOps puts a combatant commander in charge of the GIG end-to-end; it surpasses basic network management and computer network defense practices in net-centric military operations. NetOps includes not only balancing GIG responsibilities between theater and Service components but also establishing and sharing GIG situational awareness across DOD. NetOps does not mean that network providers or frontline defenders relinquish their responsibilities for their respective combatant command, Service, or agency; it does require that all synchronize their efforts to maximize efficiency, ensure data availability, and enhance protection of the network at large.

Operating in this unique and dynamic area of responsibility, the JTF–GNO has command relationships with all DOD commands, Services, and agencies. Its mission partners include allied nations, other U.S. Government departments, the National Cyber Response Coordination Group, the U.S. Computer Emergency Response Team, law enforcement agencies, the Intelligence Community, and the private sector, including telecommunications, banking and finance, transportation, and information technology.

As well as delineating the day-to-day activities of the GIG, the NetOps CONOPS defines the way ahead and establishes a working vocabulary of GIG activities and components. The JTF–GNO vision, according to its strategic plan, is to "lead an adaptive force that assures the availability, delivery, and protection of the GIG."

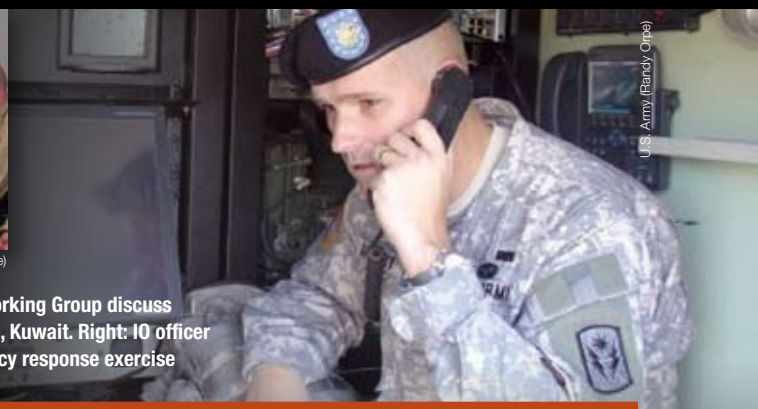
The JTF–GNO is facilitating the operational environment in which net-centricity can thrive, and it helps guarantee the free and open use of cyberspace for everyone to embrace the opportunities offered by a globally connected world. **JFQ**

Contesting the Information Battlespace

By JOHN C. KOZIOL

It is clear from the events of this decade that we live in a world filled with global security challenges that will not go away—from terrorism to countering weapons of mass destruction to nation-states bent on challenging peace and stability. The battlespace for dealing with these challenges extends in many directions. One of the most important is the information battlespace, where hearts and minds are either won or lost. Within U.S. Strategic Command (USSTRATCOM), the commander, General James Cartwright, sounds the alarm that we must challenge adversaries in contesting this battlespace: "Our enemies know how to operate there. We've got to be able to do it, too. We've got to contest that battlespace!"

55th Signal Company (Jane Laroque)



U.S. Army (Randy Orpe)

Above: Members of V Corps IO Working Group discuss critical missions at Camp Virginia, Kuwait. Right: IO officer conducts checks during emergency response exercise

With an incredibly dynamic operations tempo, commanders of joint force commands (JFCs) employ information operations (IO) and related capabilities to contest this information battlespace. IO capabilities range from technical warfare means such as computer network operations and electronic warfare to more cognitive capabilities such as psychological operations and defense support to public diplomacy. Key to successful information operations is the presentation and integration of these capabilities within an overall campaign plan and their synchronization with related activities of the U.S. Government.

For its part and based on its unified command plan tasking, U.S. Strategic Command works to grow IO capabilities for commanders and to pull together IO capabilities across plans, regions, and functions. USSTRATCOM and joint force commanders turn to the command's Joint Information Operations Warfare Command (JIOWC) to integrate IO capabilities.

Headquartered in San Antonio, Texas, the JIOWC accomplishes its mission by growing and sustaining qualified IO experts to support each geographic combatant commander, U.S. Special Operations Command (USSOCOM), and the USSTRATCOM joint functional component commands (JFCCs). Additionally, over the course of the past 2 years, the JIOWC has stood up four capability centers to enable electronic warfare, specialized IO planning, operations security, and strategic communication support planning. Support to strategic communications, in particular, is an area that the JIOWC is focusing on at the behest of commanders.

critical to building confidence in the area of information operations is an ability to predict and assess effects

Beyond its San Antonio–based experts and capability centers, the JIOWC partners with Service IO organizations and other capability centers, such as USSTRATCOM's JFCC for Network Warfare and USSOCOM's Joint Psychological Support Element, to bring the best capabilities forward into IO and strategic communications planning.

As a presenter of global force capability, the JIOWC is focused on moving more and more IO knowledge "to the edge" for best supporting JFC commanders. Key to this effort is increasing the understanding of what IO and related strategic communications assets are available and ready to support JFC planning and operations. Rather than always sending experts forward to commanders in the field, the JIOWC is developing portals and asset visibility approaches to move knowledge rapidly to the commander and warfighter. Working with geographic and functional planners, JIOWC experts then help to match available assets to requirements, develop courses of action, and deconflict requirements.

Critical to building confidence in the area of information operations is an ability to predict and assess effects. For its part, the JIOWC is again partnering with others in the Defense Department, the U.S. Government, and the commercial sector to pull together best practices for understanding the information battlespace and to target audiences operating in this space. In developing metrics for this effort, the JIOWC is working with planners to predict and measure effects. Modeling, simulations, polling, foreign media analysis, and red teaming are all activities that feed this assessment methodology and support measurement of local, regional, and transregional activities.

In looking back over the past year, General Cartwright notes, "We made progress in growing Information Operations into core military competencies. We will continue to develop these and related Strategic Communication planning capabilities to ensure that all Joint Force Commanders gain and maintain the information advantage over our adversaries through the entire spectrum of regional and trans-regional engagement. As we move beyond today, the JIOWC will be a critical enabler for all JFCs to contest this information battlespace." **JFQ**

Major General John C. Koziol, USAF, is Commander, Air Intelligence Agency; Commander, Joint Information Operations Warfare Command, U.S. Strategic Command; and Deputy Commander for Information Operations, 8th Air Force.

USSTRATCOM

The Global Innovation and Strategy Center at the University of Nebraska

The Global Innovation and Strategy Center

By KEVIN WILLIAMS

The terrorist attacks on September 11, 2001, clearly demonstrated that adversaries do not distinguish between America's military, commercial, and civilian interests. The logical response to the attacks was to combine the Nation's diverse experiences and intellects to seek answers to tough questions. Not long after 9/11, business leaders came together with their military and government counterparts in a relationship called the Partnership to Defeat Terrorism in order to look at issues involving the security and safety of American interests at home and abroad. The Global Innovation and Strategy Center (GISC) at U.S. Strategic Command (USSTRATCOM) gives the Partnership to Defeat Terrorism (now called Partnership Group) a permanent home along with two other groups, Innovation and Strategy.

The Partnership Group is made up of a core of subject matter experts who bring in the best and brightest thinkers and problem-solvers to address specific problems. Currently, the Partnership Group has experts on finance, academia, transportation, information networks, and the media. The Innovation Group, which also has its roots in 9/11, delivers technological solutions through contacts with traditional Department of Defense (DOD) organizations, as well as industry and academia. The Strategy Group builds teams of world-class experts to facilitate creative thinking and to deliver new strategies and courses of action. Together, the Partnership, Innovation, and Strategy Groups combine in a collaborative environment for solving difficult problems for USSTRATCOM and other customers.

The GISC officially opened its office space in September 2006. Located on a state university campus, it is far from Washington, and both military and civilian staff members work in business casual attire. While the building itself is a 21st-century, secure facility, it has a decidedly non-Pentagon feel. It features open collaborative spaces with comfortable chairs and easy computer access to facilitate informal and extemporaneous exchanges. The look is modern and commercial rather than DOD standard issue.

What is unusual about USSTRATCOM's new "solution incubator" is the effort under way to broaden the sphere of discovery. In addition to existing time-tested sources, the GISC is tapping alternate networks of academic and private sector expertise to find nontraditional solutions to some of the military's most difficult and sensitive problems.

Leaders in private industry generally recognize one of the major obstacles to innovation as slow development time. Similar to rapidly changing consumer demands compelling high-speed product development, the current international security environment requires rapid solutions. Consider the improvisational speed of improvised explosive device design changes, terror tactics, and adversary technological advances. One of the GISC's top priorities is improving the ability to adapt and change with the fast pace of today's world. Just as USSTRATCOM is transforming command and control, network-enabled operations, and intelligence, surveillance, and reconnaissance, the GISC is brokering partnerships for new ideas to support the command's ability to accomplish its missions by tackling problems in ways never thought of before.

Kevin Williams is Director of the Global Innovation and Strategy Center, U.S. Strategic Command.

The GISC mission requires a willingness to take risks with resources and time to create innovative approaches. This rapid-solution method, coupled with an incubator-like model, makes the GISC unique. The business model involves experts swarming around each problem. After a short turnaround time, GISC recommendations, products, and solutions go back to USSTRATCOM or other customers for implementation or further development. Successful transition of great ideas equals victory.

The problems taken on by 36 GISC staffers are directly linked to USSTRATCOM's diverse global mission set. The work equation is simple: innovation equals the sum of creative thinking plus a rapid, nontraditional problem-to-solution process. This concept rests on two modes of thought encouraged within the GISC. The first is a combination of unbounded imaginative thinking and openness to ideas regardless of the source. The second is rigorous critical and analytic thinking, to include questioning assumptions and prevailing wisdom. The result is an ability to choose and act on the best ideas.

The GISC puts this concept into practice by creating a work environment that breaks down stovepipes and fosters an innovative corporate culture. This approach not only allows for but also rewards cross-functional and integrative thinking by every GISC employee, regardless of position or rank. GISC initiatives include an internship program for exceptional graduate and undergraduate students that began in January 2007. This program is designed as a collaborative and multidisciplinary team effort that draws on in-depth research and intellectual exchanges between student interns, GISC mentors, and subject matter experts from academia and the private sector to provide a fresh look at some of the military's toughest problems.

The GISC has been operational for less than a year but has already completed a number of projects, including assessing the vulnerability of electrical grids, evaluating distributed ground network security, examining nuclear counterproliferation measures, and developing a machine-to-machine target identification processing capability to enhance maritime domain awareness.

the business model involves experts swarming around each problem

The Center's unclassified work on public health surveillance supports USSTRATCOM's mission to combat weapons of mass destruction—specifically biological threats. It also illustrates the GISC partnership approach to problem-solving. At the request of the Centers for Disease Control (CDC), for instance, a GISC team set out to find a way to enhance detection, surveillance, and situational awareness of catastrophic public health emergencies, such as a bioterror attack or an avian flu–like infectious disease pandemic. After bringing together computer science professors, data visualization specialists, physicians with expertise in public health and infectious disease outbreak, commercial transportation companies, local health officials, school districts, and medical test laboratories, the team identified a research and development gap between pure predictive and identity-based surveillance models and tools. In just 90 days, the GISC-led collaborative team produced an operational, dynamic, Web-based prototype that integrates real-time data feeds of symptomatic indicators (for example, medical lab tests, veterinary illness reports, emergency medical technicians, and physician reports) with identity-based indicators (for example, unusual patterns in adult workforce absenteeism). The model, along with a statewide vaccination distribution plan developed by a GISC team, industry partners, and the Nebraska National Guard, has been enthusiastically received by the CDC, as well as the lieutenant governor and chief medical officials of the state of Nebraska.

The GISC welcomes suggestions, ideas, and tasks—along with critiques and complaints—because America's security demands that we combine military, commercial, and academic brainpower. All of us together are smarter than any one of us alone. **JFQ**

USSTRATCOM

General Cartwright presides at opening of the Global Innovation and Strategy Center

The George C. Marshall European Center

Proven Model or Irrelevant Prototype?

By TIMOTHY C. SHEA

The George C. Marshall European Center

Marshall Center

Statue of General George C. Marshall at entrance gate to Marshall Center

In a rush to "do something" after the demise of the Soviet Union and the Warsaw Pact, the Department of Defense (DOD) created the George C. Marshall European Center for Security Studies—the first of what would become five regional centers and a self-described "model" for the others.[1] Reinvented on the remains of the disbanded U.S. Army Russian Institute in the beautiful Bavarian resort of Garmisch-Partenkirchen, Germany, the Marshall Center's original raison d'être was to help the postcommunist states of Eastern Europe and Eurasia grapple with civil-military relations, democracy, and human rights.

The Marshall Center was initially envisioned as a single, stand-alone institution answering to the Secretary of Defense through U.S. European Command. Of the five DOD regional centers, it has several unique characteristics: it is a bilateral organization located on foreign soil, it supports three combatant commands as well as the German ministry of defense, it assumes Army Title 10 responsibilities to train foreign area officers, and it operates in parallel with adjacent North Atlantic Treaty Organization (NATO) educational institutions.

These distinguishing features, along with the geopolitical evolutions and revolutions of the past decade, have created a complex regional security landscape in the Marshall Center footprint. However, because its strategic objectives have not been rigorously evaluated over the last decade, the Center cannot clearly articulate them. It has achieved notoriety over the years and has frequently been the focus of scandal. Critics have accused it of being a waste of money, where no serious academic work occurs for either students or faculty.[2] With its practical autonomy, minimal oversight, and the absence of functional rivals, this DOD regional center has never had its survival seriously challenged. Certainly, the Marshall Center has a broad supportive constituency—

Colonel Timothy C. Shea, USA, is a Eurasian Foreign Area Officer and has served as the Army Attaché to the Russian Federation since July 2005. He previously served as the U.S. Army Chair and Military Professor of International Security Studies at the George C. Marshall European Center.

after all, who is actually *against* promoting democracy, human rights, and enduring partnerships?[3] Therefore, 10 years later, in the face of glaring gaps and overlaps, a hard look at the overall mission and objectives of the Marshall Center is essential and urgent, given the changes in the political-strategic environment in the post-Soviet space.

mission creep began to infect the Marshall Center when it unilaterally added "neighboring states" to its mission statement

Mission Accomplished—or Avoided?

Government bureaucracies are formally charged with specific missions and usually have considerable freedom in defining their tasks and the capabilities they need to pursue. "Mission creep" occurs when an organization moves from well-defined or achievable missions to ill-defined or impossible ones. Faced by an unclear or unstated shift of objectives, mission creep often begins at the strategic level in an environment of gradual and perhaps unclear or unrecognized modification. These adjustments are often not stated explicitly, nor is the organization involved (or its assigned tasks) formally reevaluated.[4] Mission creep also occurs from the bottom up when the situation on the ground changes dramatically. Moreover, it can serve as a means of survival to sidestep more difficult challenges in favor of chasing easier tasks to manage. Mission creep began to infect the Marshall Center when it unilaterally added "neighboring states" to its mission statement, even though its guidance was to focus on Europe and Eurasia. By absorbing Mongolia into its portfolio, the Center further diluted oversight by dragging the U.S. Pacific Command into the equation and concurrently blurring boundaries and responsibilities.

This identity crisis contributes to the unsuccessful struggle to attract quality participants from its assigned region and inspires the Marshall Center to seek growth by becoming a global center. Located in the middle of an enlarged 26-member NATO, the Marshall Center usurps, replicates, and overlaps many educational functions more effectively and appropriately carried out by the Alliance.[5] Rather than evolve programs to meet the complex needs of the post-Soviet space, the Center has sought new audiences by encroaching into the portfolios of the other incognizant DOD regional centers. It has been unwilling to perform needed missions because it continues to focus on traditional activities that are unrealistic, unnecessary, and unwanted. The lack of geographical boundaries between the regional centers makes it difficult to pinpoint responsibility for a particular issue and inadvertently encourages expansion and replication. The German ministry of defense de facto endorses this encroachment because Berlin lacks such a forum outside of the Marshall Center. Defense Secretary guidance to "transform the Regional Centers from their original post–Cold War status to 21st century organizations capable of meeting the challenges of the post-9/11 world" has substantively been ignored.

The Regional Situation

Although the post-Soviet space is a disintegrating zone, with countries and subregions drifting in various directions, security developments remain interrelated in important respects. They are hinged together by strategic triangles and security complexes connected to a continuous periphery on the Russian border. This region has split into two camps—revolutionary pro-Westerners and conservative traditionalists. Dimitri Trenin stated that Russia's leaders have given up on becoming part of the West and have started creating their own Moscow-centered system.[6] Kremlin mistakes in regard to Ukraine bitterly disappointed those who regarded Russia as a possible counterweight to America's "regime change" strategy.[7] Meanwhile, these traditionalists will be doing their utmost to prevent "orange" (and other) revolutions from proliferating. Expect them to suppress domestic opposition and even interfere in the activities of some international and nongovernmental organizations. The Marshall Center has not developed a strategy to deal with this schism in its footprint.

The call for further democratization has become a real challenge for existing autocracies and semidemocratic regimes, such as Belarus, Russia, Moldova, Armenia, Uzbekistan, and Azerbaijan. This is a delicate balancing act between promoting democracy, on one hand, and supporting forces in a combustible but strategically important part of the world, on the other. Regime change by means of political manipulations poses a threat to all Commonwealth of Independent States (CIS) nations, particularly Russia. As CIS Executive Committee chairman Vladimir Rushailo stated, "The techniques aimed at toppling national authorities are fit to be on the list of challenges and threats of the 21st century."[8] Political leaders in the region fear that Western-educated youngsters could be turned into revolutionaries. Embattled elites want to manipulate nationalistic tendencies and to create an alternative to mass democracy movements. Viewed through this prism, one might suppose that the Marshall Center's unstated mission is to create a cadre of believers who will oppose undemocratic practices when they return to their respective countries.

Validating the Assumptions

To plan an effective strategy, assumptions must be formulated and clearly stated. Once assumptions are scrutinized and validated, any plan has a chance to succeed. Objectivity is usually ensured by making assumptions explicit enough to be examined and challenged. The Marshall Center does not formally state any planning assumptions. Coercion and the adoption of submissive, uncritical attitudes create an organizational environment vulnerable to manipulation and the promotion of dogma from above. There is consistent reference to two "implied" assumptions: one is that the sheer quantity of participants will promote change in the region through "critical mass"; the other is that it is possible to change minds and (hardened) post-Soviet attitudes. It would be encouraging to encounter a substantial body of research that provides support for this thesis of achieving critical mass, but it does not exist.

Can one really *change* attitudes? Nicholson Baker sees a mind change resulting from a slow, almost unidentifiable shift of viewpoint rather than any single argument or sudden epiphany.[9] As he sees it, these so-called jolting insights are usually things that we discern only after the fact, becoming stories that we eventually tell ourselves and others to explain our change of mind. He identifies seven factors that can aid in changing minds but acknowledges the paradox that while it is easy and natural to change one's mind in the first years of life, it becomes difficult to alter one's mind as the years pass. One can never predict with certainty whether attitude shifts

will take place, but it seems safe to say that mind changes are only likely to occur when all seven factors pull in a mind-changing direction—and are most unlikely to occur when all or most of those factors oppose the mind change. Effecting enduring changes in a particular mind, or thwarting backsliding, is extremely difficult.[10]

Why do governments expose military officers to foreign military education in the first place? Fear of military intervention in politics prompts some governments to educate soldiers. Research has demonstrated that "coup-proofing" by emphasizing technical expertise in professional military education can help to isolate officers from undue interest in the civil sector.[11] Transferring values about military professionalism, human rights, and civil-military relations is difficult to measure but is probably not effective unless other institutions in the client country also support change. A paternalistic approach by the United States at the Marshall Center to an unequal power relationship with client countries further supports such unflattering views of American programs. Values consistent with those taught by the United States are unlikely to be much influenced.

a paternalistic approach by the United States at the Marshall Center with client countries further supports unflattering views of American programs

In a related study outlined in William Easterly's new book, the author suggests that the world's official aid agencies have been recycling the same unworkable aid plans for the last 50 years.[12] The do-gooders' fundamental flaw, he argues, is that they are "planners," who seek to impose solutions from the top down, rather than "searchers," who adapt to the real life and culture of foreign lands from the bottom. The planners believe in the "Big Push"—that is, an infusion of foreign aid and advice that will lift poor countries past the poverty trap and into prosperity. In promoting change, the planners are almost always wrong, according to Easterly, because they ignore cultural, political, and bureaucratic obstacles.

Easterly's most powerful criticism is reserved for the planners who advocated "shock therapy" free-market reforms in Eastern Europe and the former Soviet Union. Free markets cannot be imposed from outside, he insists, citing the example of the inefficient Soviet-era plants that survived their entry into the market era via their communist bosses' genius for bartering and cronyism. "The Soviet-trained plant managers at the bottom outwitted the shock therapists at the top," he writes. Other studies show that U.S. assistance projects designed to strengthen civilian control of the military have not made much progress in addressing goals, primarily due to a lack of interest by former communist governments.[13]

Certain other concepts are key. Consider the distinction between the words *training* and *education*. One might argue that the terms are synonymous, but there is a significant qualitative difference. While training is more concerned with teaching what to think and what the answers ought to be, education is about teaching how to think and what the questions ought to be. But the Marshall Center believes that the primary purpose of its courses is neither education nor training but instead a "networking" opportunity for the international audience to build internal relationships. While the length of an educational or training course is usually tied to desired outcomes, the pseudoscience of this "networking opportunity" requires approximately 12 weeks to break down barriers and to establish relationships. The Marshall Center confuses the purpose of networking, which is to create strong bonds between the participants and their ministries with the U.S. Government, not between the individual participants who befriend each other over the course of 12 weeks in Garmisch.

Students at Marshall Center library

Marshall Center

Bilateral Approach

The Secretary of Defense assigned priorities to the five DOD regional centers. Serving as a strategic communications tool, the regional centers are tasked to counter ideological support for terrorism, harmonize views on common security challenges, and educate on the role of defense in civil society. But this tasking presents a serious dilemma. If the purpose of the Marshall Center is to educate participants on security and defense issues, then pooling resources with like-minded European Union countries makes good sense. If the mission is to promote U.S. policy as a strategic communications platform, then there is a problem, which undermines the rationale for a "unique German-American Partnership." As the only *bilateral* regional center located outside the territory of the United States, the Marshall Center has fallen victim to the increasing divergence of opinion and contradictory policies promoted by the United States and Germany; many countries today are looking for ways to counter global U.S. dominance. While boasting of an international faculty from several European nations, the Marshall Center's ability to accomplish its stated

mission to explain and promote U.S. policies is often undermined by European nationals who are directed by their governments to *challenge* American security policies in the seminar room. Under the guise of a bilateral partnership, each time the United States presents its opinion on an issue, the alternate German point of view is presented to the audience. As a "unique" bilateral institution, it must achieve consensus with German policies, thereby representing U.S. interests less forcefully. Rather than focusing on the needs of a largely Russian- and English-speaking audience, it squanders substantial translation and interpretation resources on a largely nonexistent German participant pool. A bilateral agreement requires Germany to fund 11.5 percent of operating costs even though it gets "50 percent" of the time on the podium.

Propaganda or skewed information does not effectively change attitudes. Information that appears to be propaganda may not only be scorned but may also turn out to be counterproductive if it undermines a country's credibility. Consider Charlotte Beers, a former advertising executive who, when tasked in late 2001 by the State Department to promote American values to Muslims, devised several naively perky advertisements featuring American Muslims extolling U.S. multicultural tolerance. The ads were a public-relations disaster and have been ridiculed with some justification by Muslims and Westerners alike.[14]

Missing the Target

A key measure of success is reaching the target audience. The Marshall Center recruitment strategy focuses mostly on demographics. It boasts that military, older, and male is less desirable than civilian, young, and female. Yet there is no candid assessment to determine if applicants are really agents of change. The Center often trains retirees, secretaries, relatives of previous participants, and others without promotion or influence potential. Candidates often lie about their actual employment or job title, which are rarely checked. Supply exceeds demand, yet quotas continue to increase, and the quality of participants steadily falls. A survey of graduates would indicate serious questions on their qualifications. The Marshall Center vigilantly hides this reality behind anecdotes, sound bites, and flashy Web sites. The absence of priority countries such as Russia, which has not elected to participate seriously, reflects a disturbing trend in the suspect pool of graduates in recent years.

Marshall Center

Left: Second Mediterranean Dialogue conference included representatives from 27 countries
Right: Marshall Center professor speaking at Senior Executive Seminar to participants from Europe, Eurasia, and the United States

To maintain the artificial demand, the Marshall Center retains a generous budget to shuttle its leadership practically full-time to regional capitals. This activity is not coordinated with higher headquarters and is conducted independent of any theater security cooperation plan. No other DOD security cooperation program requires this type of expensive self-promotion. The stated goal is to meet with government officials to bolster and diversify recruitment for Marshall Center residence courses, solicit ideas for future Marshall Center projects, meet with senior U.S. and German embassy staff in order to engender closer cooperation in recruiting participants, and host a reception for alumni in order to maintain and solidify contact with the existing graduate base. During these trips, the consistent opinion of countries visited is that they cannot support the quotas they are given.

under the guise of a bilateral partnership, each time the United States presents its opinion on an issue, the alternate German point of view is presented

Drive to Reduce Oversight

The typical bureaucracy is much less happy if it must do things that are difficult and especially if it must do them under the watchful eyes of countless oversight bodies. Because planning and supervisory responsibilities for the Marshall Center are not clearly defined, ill-considered objectives are implemented largely without control at substantial cost. The absence of politico-military expertise at the Center increases the severity of the problem. Although the lack of oversight has directly benefited infrastructure expansion and the steady growth of annual budgets, it has also contributed to wasted resources, needless redundancy, questionable priorities, and possibly even strategic failure. The Defense Security Cooperation Agency has assumed responsibility for managing all regional centers and is struggling to implement badly needed reforms. Part of the problem is that the Marshall Center has deliberately insulated itself from urgent political and strategic pressures to resist transformation by "discounting" what it hears from the field: the governments, the ministries, and the U.S. Embassy country teams located in the region.

FAO Interns

During the Cold War, the U.S. Army Soviet foreign area officer (FAO) was the best among his peers.[15] He had to be; the stakes were high, and the Soviet Union was not available for hosting in-country training. When the Marshall Center was established, it absorbed the U.S. Army Russian Institute and its Title 10 mission to train FAOs. Today's successor to the Soviet FAO training conducted at the Marshall Center pales in comparison. The mission has evolved from educating potential FAOs on-site to "coordinating" their education in the field throughout Eastern Europe and Eurasia.

The Marshall Center confuses its mission to train officers in FAO skills with supporting combatant command theater security cooperation goals. It is not accountable to

able to the U.S. Army for the quality of FAO training and uses FAOs mostly as training aids in its international student seminars. Without the FAO program, American officers generally would not participate in Marshall Center resident courses. At less than 5 percent, U.S. representation in resident courses is mostly limited to FAO interns or Marshall Center employees.

Results fail to impress; FAO Russian language skills atrophy while based in Garmisch as reflected in test scores.[16] Instead of focusing on Eurasia, FAO interns waste valuable training time learning about their own country and its security policies. FAO interns have distinctly different demographics than those of their foreign counterparts in the resident courses. The FAO program is tasked to prepare officers to serve the interests of DOD and the U.S. Army, while the Marshall Center educates foreign nationals on national security issues, allowing those individuals to return to their home country with a better understanding of Western civilian and military issues. The trend over the past 3 years averages one to two FAO interns arriving at the Marshall Center every 6 months for the 18-month program. In 2002, even the Marine Corps stopped using the Marshall Center for its FAO training. This Cold War legacy approach to Army FAO training and its associated U.S. faculty overhead continues in Garmisch, instead of progressing to in-country training opportunities that already exist in Russia, Ukraine, and other locations. In-country training programs offer Eurasian FAO interns (with their families) complete language immersion, regional travel, and the critically important opportunity to attend resident professional military education institutions.

A Potemkin Village?

Imagery often trumps substance. What bureaucrats and courtesans want us to believe often has little to do with reality, but the Marshall Center would humble Grigori Aleksandrovich Potemkin. He built elaborate fake villages in order to impress Catherine the Great on her tours of Ukraine and the Crimea in the 18th century. Preoccupied senior officials and delegations are invited to conduct short, scripted "fly in–fly out" visits to the Marshall Center. Upon arrival, they are whisked through the beautiful gold-plated facilities, provided a cursory glance at students, presented briefings taking liberal credit for every possible success, and then sent on their merry way, never suspecting that they, like Catherine the Great, may have been duped. The point here is that these junkets are largely superficial, and because of time and space constraints, the busy visitors are not presented with any opportunity to challenge the accuracy of the rosy picture being presented. Distinguished visitors are deceived into believing that the Marshall Center is a serious platform to convey important messages, when in fact the audience is rarely attentive and frequently incoherent.

Recommendations

The Marshall Center has failed to adapt and transform in the face of disruptive change in the strategic environment in which it operates. Incentives and constraints have pushed it to overstate benefits and understate costs. Under pressure to ignore and discount disturbing indicators of ineffectiveness, it has worked relentlessly to create a myth of progress and impact but remains a lost opportunity in practice. The failure has everything to do with its early successes, conventional wisdom, and institutional memories that continue to proffer the myth of success. These shortcomings affect the Center and its ability to coordinate, implement, and synchronize strategic objectives effectively with its many higher headquarters. The Center is an obsolete prototype but, if transformed, can make a major contribution in supporting DOD security cooperation goals. Following are 10 recommendations that could make the Marshall Center relevant again.

without the foreign area officer program, American officers generally would not participate in Marshall Center resident courses

Relocate and Discontinue the Bilateral U.S.-German Partnership. The significant long-term differences and contradictions in political-military perspectives make the U.S.-German partnership vis-à-vis the Marshall Center obsolete. Eliminating requirements for German translation/interpretation could free up more resources for Russian. Eliminating the bilateral nature of the Marshall Center would reduce the pressure from Berlin to overlap with other DOD regional centers on global issues and improve the focus of programs important to the United States. The legacy of the U.S. Army Russian Institute in Garmisch inhibits its serious participation from the Russian Federation.

Disinvest and Shift Eurasian U.S. Army FAO Training to Eurasia. Better, cheaper, and shorter training opportunities already exist in Russia and Ukraine. Eliminate FAO faculty overhead and focus on Marshall Center core competency to conduct programs with international elites and potential future leaders.

Refocus Core Competency on the Russian-speaking Region. Too much of what the Marshall Center does replicates the activity of NATO educational institutions. Much of what NATO offers is not useful to Russian-speaking officers because of the language barrier. The Marshall Center should move away from subsidizing NATO country participation and focus on the Russian-speaking niche, which would reduce wasteful and redundant encroachment into the footprints of other regional centers.

Right-size the Budget. The other regional centers deserve an equitable slice of the budget to support the war on terror. By shifting the focus from resident courses 12 weeks long to traveling teams with strategic agility, the Marshall Center could increase its impact at a fraction of the current cost. This transformation would eliminate the "tyranny of empty seats" that drives down the quality of international participants while increasing costs. Terminate budgets for autonomous marketing trips to regional capitals and for unauthorized liaison with Congress for funding.

Reduce the Length of Courses. Combatant commands, U.S. Embassies, and the countries in the region have tried to communicate the futility of attracting the right participants to courses exceeding 4 weeks in duration. By shortening programs, the Marshall Center might begin to attract quality. Reduction in resident courses can free up faculty to conduct high-impact programs in the region in support of theater security cooperation objectives, while improving prospects to obtain U.S. military participation.

Focus on Interoperability. DOD security cooperation guidance requires all activities to yield demonstrable significant benefit toward achieving U.S. security objectives. It directs

that DOD should discontinue or deemphasize activities with nations where cooperative activities are unlikely to provide benefits and concentrate on those nations that are likely to participate in coalition efforts. A focus on supporting interoperability as opposed to achieving "critical mass" or "attitude changes" might sell itself and eliminate the need for the vast marketing and public relations apparatus.

Shift Emphasis from Resident Education to Outreach Events. The poor quality of Russian-speaking participants begs for a shift in bringing faculty and other tools into the region. It should expand outreach and reduce focus on tired resident programs. The Marshall Center could function as a coordinating body for organizing events such as bilateral wargames and other high-impact security cooperation activities. Curtail the "push" of pet outreach events that are not needed or wanted, and instead collaborate with combatant commands and country teams to address real requirements.

Consider Efforts to Reform Military Education in the Post-Soviet Space. To break the grip of old culture, one must seize control of the schools. Many countries in the post-Soviet space are suffering from arrested development in their military educational systems, which perpetuate Soviet mindsets. The Marshall Center could serve as a coordinating body for U.S. senior Service colleges to leverage their substantial expertise in order to transform professional military education curricula in the region. Merely sending professors to lecture on their favorite topics in the region has not, and will not, effect change.

Establish an Interagency Center for Security Cooperation Lessons Learned. Through study and collaboration with other organizations, the Marshall Center might provide recommendations on how best to use limited resources for maximum effect. This analysis could improve definitions and clarify demand. Such an organization could study which programs across the interagency community (including allies and NATO) really get results and why. There is a great need to develop a systematic approach to determining strategic goals for international education programs and a strategic plan to achieve those objectives.

End the Endemic Mismanagement and Strategic Confusion. Start over. Integrate Marshall Center activity into theater security cooperation planning at the combatant command. Shift Mongolia to the Asia-Pacific Center and reduce the number of combatant commands interacting with the Marshall Center by one-third. Eliminate the cronyism and patronage that has plagued Marshall Center hiring and promotion practices. Reduce the number of non-U.S. personnel on the faculty and increase military billets. Prevent repetitive assignments of military officers and deny requests for serving military officers to retire and remain on the payroll. Review the conditions originally set forth in the Marshall Center charter for mission accomplishment—and consider that an exit strategy might be a good thing. **JFQ**

NOTES

[1] Regional centers as defined under Section 184 of Title 10, United States Code, are operated and designed by the Secretary of Defense for the study of security issues relating to specified geographic regions and serve as forums for bilateral and multilateral communication and military and civilian exchanges with regional nations. They have been established for all major regions of the world and, in addition to the Marshall Center, include the Africa Center for Strategic Studies, Asia-Pacific Center for Security Studies, Center for Hemispheric Defense Studies, and Near East-South Asia Center for Strategic Studies.

[2] Ken Silverstein, "Police Academy in the Alps," *The Nation*, October 7, 2002, accessed at <www.thenation.com/doc.mhtml?i=20021007&s=silverstein>. See also Deborah Parson, "Marshall Center story" (letter to the editor), *Stars and Stripes* (European edition), October 16, 2002, available at <www.estripes.com/article.asp?section=125&article=12417&archive=true>; Chuck Finch, "Watchdog group enters Marshall Center Fray," *Stars and Stripes*, December 18, 2000, available at <http://pstripes.com/dec00/ed121800g.html>; and Chuck Vinch, "Former Marshall Center Employees Detail Complaints," *Stars and Stripes*, December 16, 2000, available at <http://pstripes.com/dec00/ed121600p.html>.

[3] See James Q. Wilson, *Bureaucracy: What Government Agencies Do and Why They Do It* (New York: Basic Books, 1988), 195.

[4] Adam B. Siegel, "Mission Creep or Mission Misunderstood?" *Joint Force Quarterly* 25 (Summer 2000), 112–115, available at <www.ndu.edu/inss/Press/jfq_pages/1825.pdf>.

[5] For example, the mission of the nearby NATO School in Oberammergau, Germany, is to conduct courses, training, and seminars in support of NATO's current and developing strategy and policy. The NATO Defense College in Rome is the Alliance's premier academic institution and offers an array of academic courses, research projects, and outreach programs. Its core competency is the Senior Course and associated shorter courses tailored to specific audiences. It concentrates on high-level political-military issues that confront both civilian and military leadership at the Alliance and national level and strives to promote debate, seek consensus, and master the skills needed to succeed in a multinational environment.

[6] Dmitri Trenin, "Russia Leaves the West," *Foreign Affairs* 85, no. 4 (July/August 2006).

[7] Viktoria Panfilova and Dosym Satpayev, "The Leading CIS Country Damages Its Reputation by Backing Political Losers," *Nezavisimaya Gazeta*, no. 1, January 2005. See also Igor Pulgaterov, "*Vozvrasosheniye Bladnogo Uzbekistana*," *Nezavisimoye Voennoye Obrozrenoye*, no. 33, September 2006.

[8] "CIS Leaders Apprehensive of Rerun of Georgian and Ukrainian Scenarios," Moscow, RIA Novosti, available at <www.interethnic.org/EngNews/280105_5.html>.

[9] Nicholson Baker, "Changes of Mind," in *The Size of Thoughts: Essays and Other Lumber*, ed. Nicholson Baker (New York: Random House, 1996), 5–9.

[10] Howard Gardner, *Changing Minds: The Art and Science of Changing Our Own and Other People's Minds* (Boston: Harvard University Press, 2004), 17, 62, 66.

[11] James T. Quinlivan, "Coup-Proofing: Its Practices and Consequences in the Middle East," *International Security* 24, no. 2 (Fall 1999), 152–153.

[12] William Easterly, *The White Man's Burden: Why the West's Efforts to Aid the Rest Have Done So Much Ill and So Little Good* (New York: Penguin, 2006).

[13] U.S. General Accounting Office, "Promoting Democracy: Progress Report on U.S. Democratic Development Assistance to Russia," (Letter Report, February 29, 1996, GAO/NSIAD–96–40), available at <www.fas.org/man/gao/ns96040.htm>.

[14] Steven Simon and Jonathan Stevenson, "Thinking Outside the Tank," *National Interest* 78 (Winter 2004/2005), 90.

[15] Army foreign area officers are warriors who provide focused regional expertise to the joint warfighter. They possess expert military knowledge of the region, advanced language skills, and a studied cultural and political understanding, which enable them to increase success and reduce risk across the full spectrum of operations from major combat to stability operations. They operate decisively in uncertain environments, often independently, as a valuable force multiplier to commanders and senior leaders from the tactical to the strategic level. Above all, they are Soldiers.

[16] See Defense Language Proficiency Test scores for Marshall Center FAOs from 2002 to present. Almost half fail to achieve graduation standards.

American Military Culture and Strategy

By PHILLIP S. MEILINGER

DOD

General Creighton W. Abrams briefs President Lyndon Johnson on the military situation in Vietnam

Culture is generally defined as socially transmitted behavior patterns, beliefs, and institutions that shape a community or population. These beliefs and behavior patterns influence the way a people fight, affecting not only goals and strategies but also methods, technologies, weapons, force structures, and even tactics. There is no denying that cultural analysis is exceedingly difficult; even a limited analysis of one's own culture is a complex endeavor with elements that are impossible to quantify even if they are not changing over time. Nevertheless, analysis must be attempted because the influence of culture is fundamental to a vast panorama of military art—from strategic communication to order and discipline.

The U.S. military subculture has obviously been shaped by American culture writ large. Although partly inherited from its European forebears, our approach to war has developed in its own distinctive way. Events since the Cold War have made our contemporary military culture more finely tuned to the demands of domestic and international politics than ever before. Increasing sensitivity to the use of force has shaped the way Americans fight today, emphasizing speed, precision, power projection, and information fusion to produce decisive results in a short period of time with low casualties—to both sides. In addition, the tension between a professional military and one composed of citizens—a national guard—continues to be a subject of intense political debate. Finally, civilian control of the military, the bedrock of American military culture, must be offered loyal opposition from military professionals to avoid political decisions to employ military power in ways that are antithetical to sound grand strategy.

Colonel Phillip S. Meilinger, USAF (Ret.), served in the U.S. Air Force for 30 years. After military retirement, he worked for both Science Applications International Corporation and Northrop Grumman. He holds a Ph.D. in history from the University of Michigan.

Observations

Outside observers have stressed certain themes in American culture and their impact on military organization and strategy. Alexis de Tocqueville noted that Americans emphasized equality and democracy and believed they had a God-given mandate to further those concepts throughout the world, prompting him to write in exasperation: "Nothing is more embarrassing in the ordinary intercourse of life than this irritable patriotism of the Americans."[1] A heightened ethnocentrism would become an American trait.

Regarding the military, Tocqueville noted that geography, in the form of a huge land mass bounded by oceans and weak neighbors, meant that a standing army was unnecessary. As a consequence, military affairs were little discussed by the average American or his politicians. This, in turn, led to naiveté and lack of preparedness when a crisis did arise: "There are two things that a democratic people will always find very difficult, to begin a war and to end it."[2] This was a prescient observation.

Another foreigner observer was Alfred Vagts, who served in the German army during World War I but fled to America when Hitler came to power in 1933. A military historian, Vagts defined two related but fundamentally different terms. The *military way* sought to achieve specific war objectives with efficiency and dispatch. The military way was limited in scope and inherently scientific in its methods. *Militarism*, on the other hand, was a combination of "customs, interests, prestige, actions and thought associated with armies and war and yet transcending true military purposes." Militarism was an evil, focused on "caste and cult" rather than science, and was often antithetical to the military way.[3] Germany was militaristic, but Vagts' adopted country was not: "The American system at the outset was a military system, not a militaristic system. It conceived of the army as an agent of civil power, to be organized and disciplined with that purpose in view, not as an end in itself."[4]

The most influential authority on the culture of the American military has been Samuel Huntington. In *The Soldier and the State*, Huntington covered a wide range of topics including the nature of a profession, military professionalism, and civilian control

of the military. He too noted the distinction between the military way and militarism, the profound security of the United States for over a century that stunted strategic thought, and the tension between professional Soldiers and the National Guard. Regarding this last item, he noted that the Guard is an inherently political instrument. Commanders are appointed by state governors (or in some cases are elected), so these positions are often seen as a form of patronage.[5] Once appointed, senior officers have a dual loyalty to their state and to the Federal Government. In short, because the regular military force was small and the Nation had to rely on its Guard, there arose continual tension regarding the political nature and influence of the U.S. military.

In sum, observers identified several factors that characterize American military culture.[6] First was the fear of a standing army that might prove dangerous to the liberties of a free people. Related to this fear was an affinity for the citizen-soldier. It was a strongly held belief that every able-bodied man in America was capable of taking up arms to defend his home. At the beginning of the colonial era, this was not an unreasonable assumption. Colonial America was a dangerous place, and most men, especially in frontier areas, had to be proficient with firearms for their own safety. By the time of the Revolution, the English were also aware of this latent military capability. As one magistrate warned London, these were "a people numerous and armed."[7] The United States was born in conflict—to secure its independence and survival—and this had a defining effect on its military culture.

Strategy and U.S. History

At the same time, Americans were not particularly militaristic in that the rigid discipline characteristic of European armies was not present in the colonies. General William von Steuben, who helped train George Washington's Continental Army, noted that Americans wanted to be told why they were doing things—orders were not sufficient.[8] This trait meant that American military personnel were imbued with an unusual amount of independence and initiative. This independent streak would also be a lasting cultural trait.

A–10 Warthogs strike targets in Kosovo as part of Operation *Allied Force*

The United States was founded on law, so the role of the military was carefully circumscribed. The law similarly governed the way the military conducted itself. It is significant that one of the first legal treatises governing the conduct of an army in war, in any country, was drawn up by Francis Lieber for the U.S. Army in 1861.[9] This mandate to follow the law has become even more pronounced today.

Isolationism, to a great extent fostered by geography, has long been a characteristic strain in the American spirit. George Washington warned of foreign entanglements in his "farewell speech" of 1796, and it was not until 1948 that the United States joined a military alliance in peacetime. Americans, therefore, viewed war as an aberration not to be taken lightly. This total commitment often led to a policy of unconditional surrender—anecdotally what the initials of U.S. Grant stood for.[10] If wars were thus total and the subjugation of the enemy was necessary, then it followed that the aftermath of war—indeed its goal—should be the spread of the American spirit of democracy and an abhorrence of war. Democracy was the desired endstate for Mexico in 1847, for Cuba and the Philippines in 1898, for Europe through Woodrow Wilson's Fourteen Points of 1918, and for Germany and Japan after World War II. Even in Korea, Vietnam, Afghanistan, and Iraq, free and democratic societies were the ultimate U.S. policy goals. Unfortunately, it was also a characteristic of the "aberration" mentality that when wars ended, things were expected to return quickly to normal. The troops would come home and be demobilized, the defense budget would be cut, America would return to its isolationist shell, and the budding democracy in the defeated enemy country would be left to fend for itself. Postconflict pacification and stabilization efforts were often given short shrift.[11]

Tocqueville noted that a huge land mass bounded by oceans and weak neighbors meant that a standing army was unnecessary

The military strategies followed by U.S. leaders over the past 2 centuries have been shaped by these varied characteristics. One of the most respected historians of the American military has been Russell Weigley, who argued that through the end of World War II at least, American Soldiers held a narrow definition of the term *strategy*. To them, the term merely meant "the art of bringing forces to the battlefield in a favorable position," and generals did not consider broader issues, such as the political, economic, or social implications of battle. Using this narrow definition, Soldiers tended to see battle as an end in itself.[12] Carl von Clausewitz had said precisely the same thing, so American Soldiers could at least claim a dubious pedigree.[13] The art of American strategy therefore focused on how the battle should be set up, and how it should then be fought. Much time was spent on logistics, command and control, staff work, and battle tactics. The goal was to get there fast, get there first, and get there heavy. If one did so, annihilation might result: the enemy would be decisively defeated, and peace, whatever politicians meant by that term, would ensue. This meshed with an American military culture that saw war as an aberration to be quickly ended and then forgotten.

A corollary of this emphasis on annihilation was that America would rely on its massive industrial and natural resources to overwhelm an enemy. For America, there would always be an unlimited supply of weapons, ammunition, fuel, and steel. Technology could substitute for manpower.

And so, American strategy was an attempt to mass forces for a decisive battle that would lead to enemy defeat. Some generals got quite good at this; by the end of the Civil War, Grant was battering Robert E. Lee's army to bits—as well as his own. In World War I, John Pershing followed the same unimaginative strategy used by the British and French—a series of bloody frontal assaults against German lines. As for World War II, many believe that Eisenhower's refusal to move beyond the Elbe River toward Berlin was the epitome of myopic strategic thinking. To him, taking the German capital would cost many lives, and they were not worth the seizure of the city for "mere" political ends.[14]

Korea was a turning point because the world had changed. The American and Soviet colossi faced each other, armed with atomic weapons, across the devastated but invaluable landscape of Europe. When North Korea moved south in June 1950, American leaders saw the attack as a feint dictated by Moscow that was intended to distract America from Europe. Chinese intervention a few months later aggravated these

1st Combat Camera Squadron (Greg Davis)

fears. Such concerns were either not shared or not understood by the commander in Tokyo; Douglas MacArthur believed that his mission was to destroy the enemy's forces. The lessons of Clausewitz and his own experiences in two world wars had taught him that there was no substitute for victory. Harry Truman thought otherwise, and the Old Soldier faded away.

American military leaders learned from MacArthur's experience in Korea: they learned to keep quiet and not argue with their civilian superiors. Unfortunately, the more vital strategic issues were not grasped. Vietnam was the result.

Presidents John Kennedy and Lyndon Johnson saw Vietnam, and indeed all of Southeast Asia, as another proxy war pushed by Communist leaders in Moscow and Beijing to distract attention from Europe. To avoid falling into this trap, the Presidents decided that there would be no attempt to annihilate or overthrow the enemy. There would be no invasion of North Vietnam. Johnson confined himself to throwing some bombs at North Vietnam, although never enough and seldom at the right targets.[15] In an unusually candid passage, Johnson explained his reasoning for a military strategy that offered something less than victory:

I saw our bombs as my political resources for negotiating a peace. On the one hand, our planes and our bombs could be used as carrots for the South, strengthening the morale of the South Vietnamese and pushing them to clean up their corrupt house, by demonstrating the depth of our commitment to the war. On the other hand, our bombs could be used as sticks against the North, pressuring North Vietnam to stop its aggression against the South. By keeping a lid on all the designated targets, I knew I could keep the control of the war in my own hands.[16]

Unfortunately, Johnson's stick was never big enough to stop the North Vietnamese from stealing the carrots.

General William Westmoreland was thus heavily constrained. As the heir to the tradition of decisive battle and annihilation, he struggled to reconcile divergent goals and the means to achieve them. Denied the option of moving north, he devised a strategy of attrition that emphasized body counts, search and destroy operations, free fire zones, and an astonishing use of firepower. The Air Force dropped 5 million tons of bombs on South Vietnam, while the Army and Marines fired an even more astonishing 8 million tons of artillery rounds.[17] And South Vietnam was on our side. Had the enemy been the German army of 1944, this kind of strategy might have made sense; in 1968 against the Viet Cong, it most certainly did not. The political and cultural components of strategy were barely considered, largely because American military leaders had never been educated to worry about such things.

Exacerbating this, wars now took place far off and, for the United States at least, for limited ends. These small wars had international repercussions that had to be understood by military leaders, but it was a lesson slow to take root. America would need to use its military power in a most circumspect fashion. American strategy needed to be reexamined.

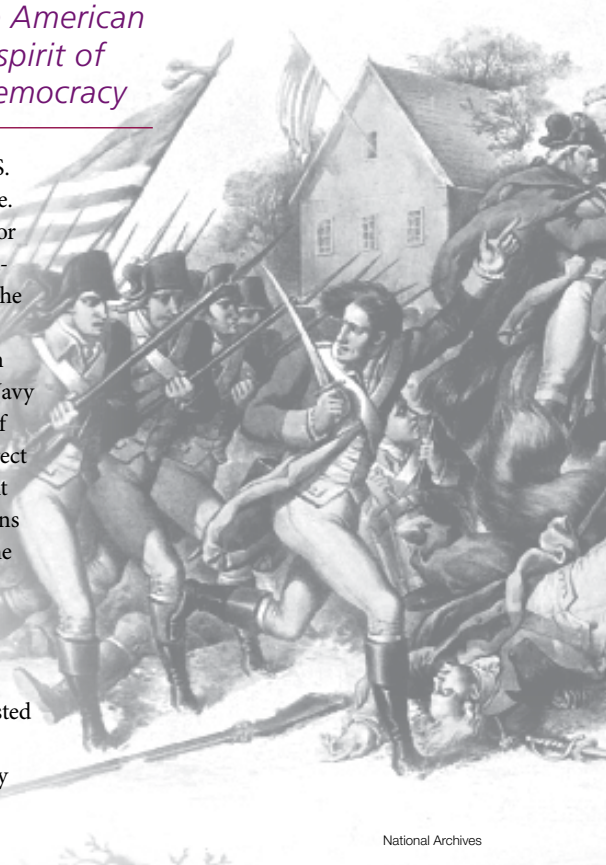
Service Cultures

In the face of this context, it should be noted that the Services themselves have differing views of strategy. During the first century and a half of our nation's history, the Army tended to dominate strategic military thinking. Those officers who entered the political arena—and thus had further influence on strategy—almost exclusively were Soldiers.[18] With the advent of serious global and joint warfare during World War II, as well as the addition of airpower as a new dimension to military operations, U.S. strategic thought necessarily began to evolve. Culture—the beliefs, traditions, and behavior patterns that shape any country or organization—also shaped the American military. The result of these factors has made the Services unique. Carl Builder wrote a classic work on the subject, arguing, for example, that the Navy has a tradition of independence as a result of virtual autonomy while at sea and out of direct contact with Washington. This led to a spirit of initiative, but also an aversion to politicians who attempted to "meddle" in its affairs. The Army, on the other hand, saw itself as an obedient and willing servant of the people. Although often neglected by its masters, it remained steadfastly loyal and dependable. The Air Force, as the youngest Service, boasted that its only tradition was a refusal to have any traditions. It saw itself as technologically oriented and therefore progressive.[19]

Granted, these characterizations are too facile, but the Services are different. Their histories and traditions have induced mindsets that shape the way they view strategy and war. As noted, the Army tends to follow a Clausewitzian bent, and its focus is on reaching close combat with the enemy. The Navy has traditionally followed a more economic form of war that emphasizes control of sealanes and the gradual disruption of an enemy's trade.[20]

Airmen also question the focus on an enemy's land forces. In 1930, Billy Mitchell wrote, "The advent of air power, which can go straight to the vital centers and either neutralize or destroy them, has put a completely new complexion on the old system of making war. It is now realized that the hostile main army in the field is a false objective, and the real objectives are the vital centers."[21] The point is that differing Service cultures shape the way Soldiers, Sailors, and Airmen view war—its purpose, its strategies, and its tactics. For decades, these diverse views generated confusion. After Vietnam, missteps in the Iran hostage rescue attempt of 1980, and the invasion of Grenada in 1983, the Services

if wars were total and the subjugation of the enemy was necessary, it followed that the aftermath of war should be the spread of the American spirit of democracy



National Archives

made concerted efforts to adopt a more joint approach to warfighting. This move toward increased jointness accelerated with the end of the Cold War. To minimize mistakes and confusion, military operations became more centralized and joint. At the same time, a technological breakthrough in the area of precision guided munitions was taking place.

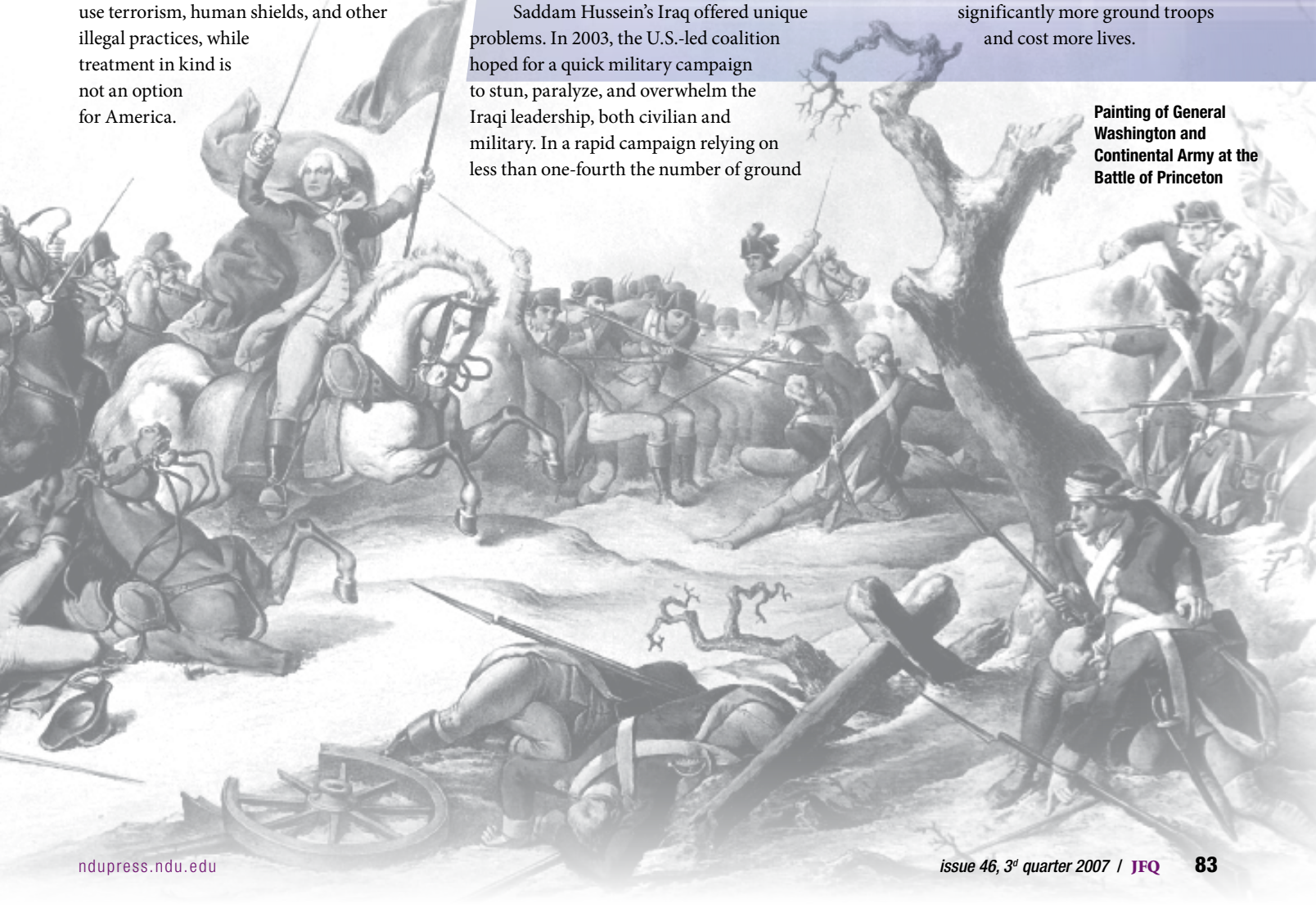
The emergence of these new weapons produced an increasing demand for discrete and less blunt applications of force. Annihilation—the goal of U.S. combat in the past—became inappropriate. Instead, military operations were planned to minimize casualties to enemy forces: the objectives became to dissuade them from fighting at all or to paralyze them so that they were unable to fight effectively and quickly surrendered.[22] More importantly, eliminating collateral damage to civilians became essential. Any bomb that went astray or any civilian killed by an edgy Soldier on patrol would be reported worldwide, thereby harming American foreign policy. Significantly, the United States is held to far higher standards than the adversaries they face. It is now expected that enemies will use terrorism, human shields, and other illegal practices, while treatment in kind is not an option for America.

Other technological advances emerged to continue the transformation of American military culture. Besides precision weapons, stealth, networked operations, and near-instantaneous global communications and intelligence have revolutionized the way America fights, beginning with Operation *Desert Storm* in 1991. Besides suffering remarkably few casualties, the Armed Forces achieved their objectives with unusual speed: *Desert Storm* lasted 6 weeks, and the 1999 air war over Kosovo took less than 3 months.

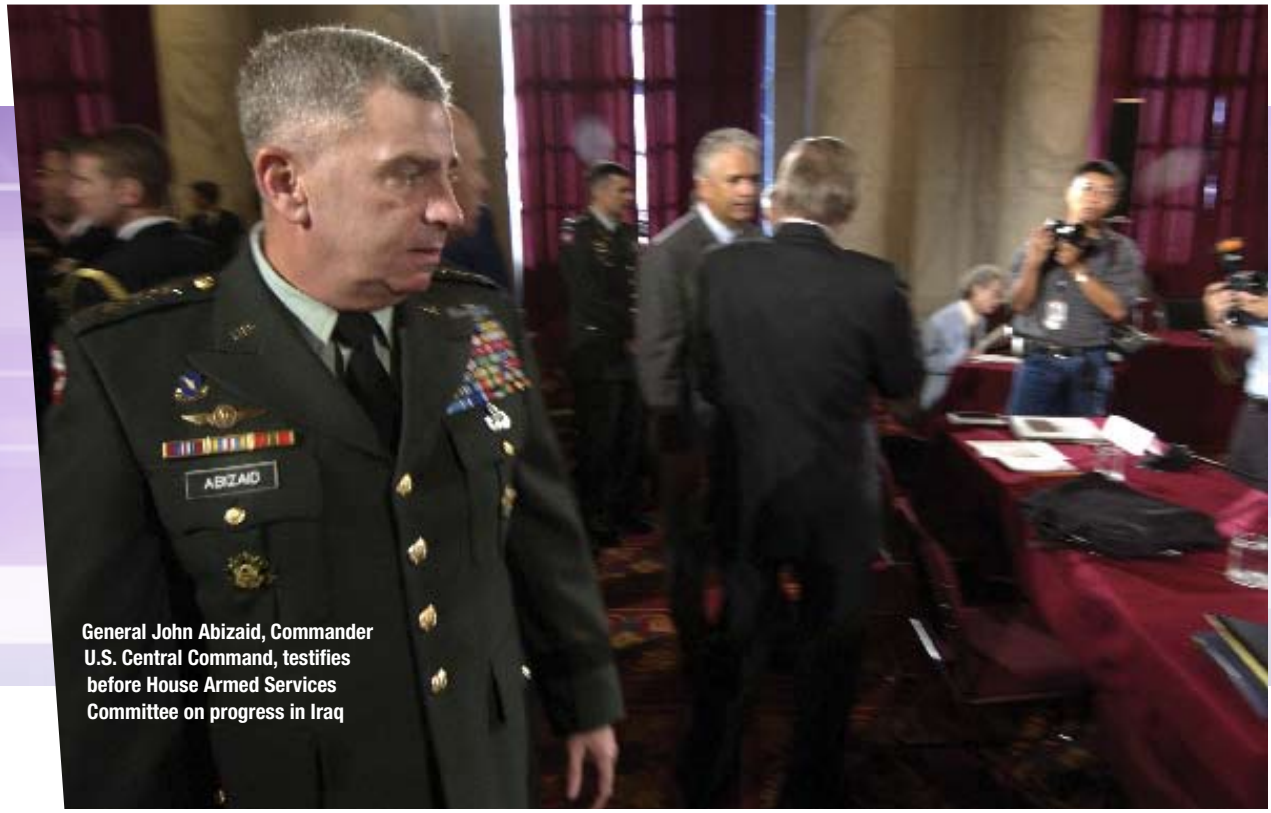
America's overwhelming military might generated a predictable response: enemies did not disappear; they morphed into a new form. Taking on the United States in a conventional fight was out of the question, so adversaries were left with asymmetrical strategies and weapons. This meant that the military began to worry seriously about weapons of mass destruction, cruise and ballistic missiles, information warfare, and terrorism. The catastrophe of 9/11 forced changes in American military culture by accelerating the move toward greater technological development and more joint command and control.

Saddam Hussein's Iraq offered unique problems. In 2003, the U.S.-led coalition hoped for a quick military campaign to stun, paralyze, and overwhelm the Iraqi leadership, both civilian and military. In a rapid campaign relying on less than one-fourth the number of ground troops used in 1991, the coalition struck with land, sea, air, and special operations units. Iraqi leaders were unable to organize a serious defense or even coordinate and control their forces. The coalition encountered only sporadic resistance from regular and Republican Guard forces, and within 2 weeks, Baghdad had begun to totter. A week later it was over—at least the United States thought it was. And that last comment echoes the concern advanced by Tocqueville nearly 2 centuries ago: Americans have difficulty getting out of wars.

It is useful to ask a related question regarding the strategy employed in Iraq: to what extent did the way in which the coalition fought contribute to the problems that have occurred afterward? In other words, did the coalition win too easily and bloodlessly, thereby leaving the Iraqi populace with the impression that they had not been defeated? In this argument, a slower, more deliberate, and more brutal campaign to destroy the Iraqi army and occupy all of the major population centers would have been more desirable—even though it would have required significantly more ground troops and cost more lives.



Painting of General Washington and Continental Army at the Battle of Princeton



General John Abizaid, Commander U.S. Central Command, testifies before House Armed Services Committee on progress in Iraq

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

The contrary argument maintains that it is not serendipitous that things had gone better in Bosnia, Kosovo, and Afghanistan after major hostilities ended; it was precisely because American ground presence was so slight. From this perspective, the wisest strategy is to place as few of our troops in harm's way as possible.

Military Service culture will to a great extent determine where one falls on the complex (and oversimplified) issue outlined above. Clearly, however, the clash of Service cultures is apparent and harbors serious implications for how America fights. In sum, it appears that the peculiarities of American culture have shaped a distinctive American way of fighting. But culture changes as a result of new directions in society's circumstances, attitudes, and beliefs. American military culture has thus changed too, especially following World War II and again after the Cold War. Clearly, one cultural paradigm has been irrevocably shattered—the days of U.S. isolationism are gone.

Other cultural artifacts have not disappeared. The long-standing belief in the efficacy of the citizen-soldier is deeply ingrained. American youngsters know of the famed Minutemen, those rugged colonials who grabbed the long rifle hanging over the fireplace and went off to fight when the situation demanded. This legend has endured in American culture for over 2 centuries and for good reason. The armies that have fought U.S. wars have been populated largely by draftees, short-term volunteers, and Guard and Reserve forces, reinforced by a small cadre of professionals.[23]

to wait several years to come forward and state "I knew it all along" is "dereliction of duty"

This has now changed. The demise of the draft after the Vietnam War means that, for the first time in American history, a professional military is dominant.[24] Even so, this issue is not clear-cut because the Guard and Reserve play a greater role than they did previously, due to increased overseas commitments. For example, over 50 percent of airlift and air refueling missions are now flown by Air Guard and Reserve crews. During the Iraqi campaign, the Army mobilized over 150,000 Reservists and Guardsmen, the Marine Corps activated over 20,000 Reservists, and the Navy called up nearly 10,000.[25] Clearly, both a professional military and one made up of citizen-Soldiers, Sailors, Airmen, and Marines are essential.

Still, questions regarding the role of the military continue to echo in American society. What is the appropriate role of senior military leaders in political decision-making? The combatant commanders, those four-star officers assigned to geographic commands around the world, have great political influence, dealing routinely with foreign civilian leaders, as well as their military counterparts, regarding issues as diverse as status of forces agreements, contingency plans, and local terrorist threats. The war on terror, with its necessary emphasis on all aspects of terrorism—political, economic, religious, ethnic, cultural, and military—means that these combatant commanders are destined to play a greater, not lesser, role in future crises. Are they trained for such roles? Are they given sufficient guidance from Washington to help them navigate the shoals?

Civil-Military Relations

This leads to the broad yet critical issue of civil-military relations—more specifically, civilian control of the military. This is a huge topic, but the essence of this matter was perhaps best expressed by Peter Feaver: "The civil-military challenge is to reconcile a military strong enough to do anything the civilians ask them to with a military

subordinate enough to do only what civilians authorize them to do."[26]

This is an emotional subject that has generated much ink. Some today speak passionately about a crisis in American civil-military affairs, seeing danger at every turn.[27] The Clinton years were seen as particularly troubling because it appeared the military did not like their Commander in Chief. Recent studies indicate that the American military is becoming increasingly conservative, and two-thirds of military personnel surveyed thought that the military had higher moral standards than did society at large.[28] It was feared that an ideological gulf was developing between society and the military chartered to protect it, and this spelled danger. Others have argued just as strenuously that there is no crisis at all.[29] This is a vital subject that strikes at the core of American military culture. Civilian control of the military is fundamental to our political and cultural system.

Our military leaders must recognize that they have a crucial role in American military policy and strategy. Because senior commanders will generally be on the scene where crises develop, they will undoubtedly have valuable insights to share with political leaders. At the same time, and this is the heart of the matter, the military will often be directed to implement the actions that civilian leaders decide on. It is therefore essential that the military advice given—and any reservations—regarding a strategic course of action be well thought out, practical, and practicable.

Therein lies the rub. Too often in recent memory, our military leaders have fallen short in providing this necessary advice—especially when it conflicted with the views of civilian leaders. In the Vietnam War, for example, it is notable that no senior officers from any Services forcefully pressed their reservations on the strategy and the conduct of the war to the point where they tendered their resignations. Yet a number complained bitterly in their memoirs regarding that strategy.[30] By then it was too late.

Similarly, in spring 2006, several recently retired generals publicly denounced the strategy being followed in Iraq and called for the resignation of Defense Secretary Donald Rumsfeld.[31] Again, however, none of these men so forcefully expressed these complaints while in uniform. This is simply not good enough when the lives of America's sons and daughters are at stake. If senior commanders sincerely believe that the military strategies directed by our civilian leaders are fatally flawed—as apparently did many officers in Vietnam and in Iraq—then they have a responsibility to the country and to those under their command to express those reservations forcefully and unambiguously. To wait several years to come forward and state "I knew it all along" is, to use the evocative phrase of H.R. McMaster, "dereliction of duty."[32]

Related to this, and putting even greater pressure on our senior commanders, is the fact that fewer American politicians have military experience than previously. Today, only 29 percent of Senators and 23 percent of Congress have served in the military—compared to 77 percent and 71 percent respectively in 1977.[33] This is not to say they are uninformed or incapable of making wise decisions regarding military issues, but it does mean that such knowledge must be gained in other ways.[34] Once again, this could indicate the need for a close relationship between politicians and the military leadership.

The Endstate

Other distinctive traits of American military culture remain. The military continues to conduct itself in a rigidly legal fashion. If anything, the growth of global news media has made this requirement even more compelling. Americans also continue to view war as an aberration that should be undertaken only with reluctance and ended quickly. Regrettably, as Iraq demonstrates, a war's aftermath is still given scant consideration by Soldiers or politicians until it is too late.[35] Our combatant commanders must therefore plan for what will happen after major combat operations are over. Our State Department must play a far greater role in advising commanders during this critical phase. Our Presidents must ensure that the desired endstate is clearly understood by all participants and that plans are developed to reach that endstate. Once again, however, it appears certain that senior military commanders must be part of this crucial process for the simple reason that they—and, more specifically, the men and women working for them—will be the ones who may have to pay the ultimate price for failure.

wars now took place far off and, for the United States at least, for limited ends

Of great importance, the tendency to regard battle as an end in itself, to see annihilation of the enemy as a desirable goal, and for military commanders to be blind, or at least naïve, to anything on a plane higher than the tactical level of war, is no longer viable. Instead, the U.S. military today is far more attuned to the political, social, and cultural implications of its activities than ever before. It also relies ever more heavily on technology as a way to achieve its objectives quickly and efficiently, with the least possible loss of life—to both sides. The campaigns since *Desert Storm* in 1991 show this new trend clearly. Although specific weapons and tactics will most certainly change in the decades ahead, the basic cultural trends noted above probably will not. This is good; the American Armed Forces, the most powerful in the world, must continue to be guided by the legalistic and democratic ideals of our forebears. Moreover, the military must recognize its own cultural imperatives before it can effectively cooperate with allies and confront its enemies. **JFQ**

NOTES

[1] Alexis de Tocqueville, *Democracy in America*, Everyman's Library ed., 2 vols. (New York: Alfred Knopf, 1994), I, 244.

[2] Ibid., II, 268.

[3] Alfred Vagts, *A History of Militarism, Civilian and Military*, rev. ed. (London: Hollis & Carter, 1959), 13.

[4] Ibid., 103.

[5] Samuel P. Huntington, *The Soldier and the State: The Theory and Politics of Civil-Military Relations* (Cambridge: Harvard University Press, 1957), 169–179.

[6] See, for example, Walter Millis, *Arms and Men: A Study of American Military History* (New York: Putnam's, 1956); Graham A. Cosmas, *An Army for Empire: The United States Army in the Spanish-American War* (Columbia: University of Missouri Press, 1971); Jerry M. Cooper, *The Army and Civil Disorder: Federal Military Intervention in Labor Disputes, 1877–1950* (Westport, CT: Greenwood Press, 1980); Stephen E. Ambrose, *Upton and the Army* (Baton Rouge: Louisiana State University Press, 1964); William B. Skelton, *An American Profession of Arms: The Army Officer Corps, 1784–1861* (Lawrence: University Press of Kansas, 1992); Edward Coffman, *The Old Army: A Portrait of the American Army in Peacetime, 1784–1898* (New York: Oxford University Press, 1986); and Arthur A. Ekirch, *The Civilian and the Military* (New York: Oxford University Press, 1956).

[7] John Shy's *A People Numerous and Armed* (New York: Oxford University Press, 1976) is an excellent book on the subject of colonial military affairs.

[8] Russell F. Weigley, *History of the United States Army* (New York: Macmillan, 1967), 64.

[9] Richard S. Hartigan, *Lieber's Code and the Law of War* (Chicago: Precedent, 1983).

[10] Actually, Grant's given names were Hiram Ulysses; he later changed them to Ulysses Simpson. Most folks called him Sam.

[11] World War II was a sea change in this regard: in both Germany and Japan, the United States left behind occupation troops, for years, to ensure that democracy took root.

[12] Russell F. Weigley, *The American Way of War: A History of United States Military Strategy and Policy* (New York: Macmillan, 1973), xviii.

[13] Carl von Clausewitz, *On War*, ed. and trans. Michael Howard and Peter Paret (Princeton: Princeton University Press, 1976). There are over 20 passages in *On War* that stress the necessity and primacy of finding and destroying the enemy army.

[14] For critiques of Eisenhower's decision, see John Toland, *The Last 100 Days* (New York: Random House, 1966), and Cornelius Ryan, *The Last Battle* (New York: Simon and Schuster, 1966). For more balanced treatments, see Stephen E. Ambrose, *Eisenhower and Berlin, 1945* (New York: W.W. Norton, 1967), and Forrest C. Pogue, "The Decision to Halt at the Elbe," in *Command Decisions*, ed. Kent R. Greenfield (Washington, DC: Office of the Chief of Military History, 1960), 479–492.

[15] According to some, Army leaders continued to press Johnson for an invasion option throughout the war, but the President would have none of it. Andrew F. Krepinevich, Jr., *The Army and Vietnam* (Baltimore: The Johns Hopkins University Press, 1986), 60, 164–165, 179, 261–262. For the argument that a move with conventional U.S. forces into Laos and Cambodia was a war-winning option, see Harry Summers, *On Strategy: A Critical Analysis of the Vietnam War* (Novato, CA: Presidio, 1982), 104, 119, 123–124.

[16] Quoted in Dennis M. Drew, *Rolling Thunder, 1965: Anatomy of a Failure*, CADRE Paper (Maxwell Air Force Base: Air University Press, 1986), 31.

[17] Wayne Thompson, *To Hanoi and Back: The USAF and North Vietnam, 1966–1973* (Washington, DC: Air Force History and Museums Program, 2000), 5–6.

[18] Besides career officers such as Andrew Jackson, Zachary Taylor, U.S. Grant, and Dwight Eisenhower, there were many others who had served as senior Army officers and had run for the Presidency, some successfully: George Washington, William Henry Harrison, Franklin Pierce, Winfield Scott, John Fremont, and George McClellan. Indeed, the six Presidents after the Civil War had all been Union generals. In contrast, it was not until 1960 that a former naval officer—and John F. Kennedy had only served as a Reserve lieutenant—became President. An admiral has never run for the Presidency, although James Stockdale was Ross Perot's Vice-Presidential running mate in 1992.

[19] Carl H. Builder, *The Masks of War: American Military Styles in Strategy and Analysis* (Baltimore: The Johns Hopkins University Press, 1989), passim.

[20] U.S. Navy, Naval Doctrine Publication 1, *Naval Warfare* (Washington, DC: Department of the Navy, March 1994), 35.

[21] William L. Mitchell, *Skyways* (Philadelphia: J.B. Lippincott, 1930), 155.

[22] In decrying those who complained that too many Iraqi soldiers died in *Desert Storm*, Harry Summers wrote a trenchant editorial with the heavily sarcastic title, "Bambifying War: A Virus from the Ideological Swamp," *The Washington Times*, September 19, 1991, G1.

[23] For spirited accounts from the late 19th century, see Emory Upton, *The Military Policy of the United States* (Washington, DC: U.S. Government Printing Office, 1912), who argues the need for a professional military, and John A. Logan, *The Volunteer Soldier of America* (Chicago: R.S. Peale, 1887), who extols the virtues of the citizen-soldier. Upton and Logan had been Union generals during the Civil War. Upton was a West Point graduate and career Soldier. Logan had been an Illinois congressman before the war who resigned from office and took up arms, rising to the rank of major general and temporary command of a corps. After the war, he returned to politics.

[24] Paradoxically, an all-volunteer force is viewed by some as undemocratic because it removes an important check on government's power. In this view, it is a good thing for political leaders to have to worry about disgruntled draftees—and their families. Thus, it would be a step for democracy if men and women were *forced* into the armed services. See, for example, Diane H. Mazur, "Draft May be Needed to Rein in All-Powerful Military," *The Chicago Tribune*, December 28, 2003.

[25] See Department of Defense, News Release, March 26, 2003, available at <www.defenselink.mil/releases/2003/b03262003_bt156-03.html>; Air Force Office of Public Affairs, "U.S. Air Force Snapshot," April–June 2004. The Army and Air Force have both National Guard and Reserve Components; the Navy and Marines have only Reserve forces.

[26] Peter D. Feaver, "The Civil-Military Problematique: Huntington, Janowitz, and the Question of Civilian Control," *Armed Forces and Society*, no. 23 (Winter 1996), 149.

[27] Richard H. Kohn, "Out of Control: The Crisis in Civil Military Relations," *The National Interest*, no. 35 (Spring 1994), 3–17.

[28] Gordon Trowbridge, "Today's Military: Right, Republican and Principled," *Army Times*, January 5, 2004, 15.

[29] For a response to Kohn, see "An Exchange on Civil-Military Relations," *The National Interest*, no. 36 (Summer 1994), 23–31. The four respondents were Colin Powell, John Lehman, William Odom, and Samuel Huntington.

[30] See, for example, U.S. Grant Sharp, *Strategy for Defeat* (San Rafael, CA: Presidio, 1978); William W. Momyer, *Air Power in Three Wars* (Washington, DC: U.S. Government Printing Office, 1978); and William C. Westmoreland, *A Soldier Reports* (Garden City, NY: Doubleday, 1976).

[31] Evan Thomas and John Barry, "Anatomy of a Revolt," *Newsweek*, April 24, 2006, 28–32; Michael Duffy, "The Revolt of the Generals," *Time*, April 24, 2006, 41–42. Anthony Zinni was an exception; he had retired before the Bush administration decision to invade Iraq.

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

[33] "Vets Aren't Taking Hill: Military experience in Congress is at a 60-year low," *Military Officer*, January 2007, 32.

[34] Some politicians are, however, very aware of the effects military operations have on their political fortunes. Wesley Clark stated that he was under pressure to end the war in Kosovo before July because Vice President Al Gore wanted it over before he began his Presidential campaign that month. R. Jeffrey Smith, "Clark Papers Talk Politics and War," *The Washington Post*, February 7, 2004, A1, A5. In December 1972, Richard Nixon was anxious to end the war before the new, and heavily Democratic, Congress took office in January. He therefore gave his military commanders great latitude in prosecuting the *Linebacker II* air campaign. Henry Kissinger, *White House Years* (Boston: Little, Brown, 1979), 1,458.

[35] For a discussion of this issue, see Thomas E. Ricks, *Fiasco: The American Military Adventure in Iraq* (New York: Penguin, 2006), passim.

ON THE NATURE OF Strategic COMMUNICATIONS

By CARNES LORD

Strategic communications, as now generally understood within the Department of Defense (DOD), encompass (to use the bureaucratic terms of art) public affairs, "defense support for public diplomacy," and military psychological operations (PSYOP). That there has been something less than smooth cooperation among these various components is hardly a secret.

In the fall of 2001, for instance, the Pentagon established an Office of Strategic Influence (OSI) with significant funding of its own to plan and coordinate a joint and coalition campaign to shape the communications battlefield in the war on terror. This promising initiative promptly blew up. In early 2002, Secretary Donald Rumsfeld felt compelled to disestablish OSI when press accounts alleged that the office was placing so-called disinformation in the American media (later investigation showed the charges to be false or grossly misleading). Evidently, these attacks were inspired from within the Pentagon itself by elements of the DOD public affairs community. Continuing tension between the PSYOP and public affairs communities over the fundamental nature of strategic communications remains perhaps the most serious impediment to more effective action by the Defense Department in this critical arena.[1]

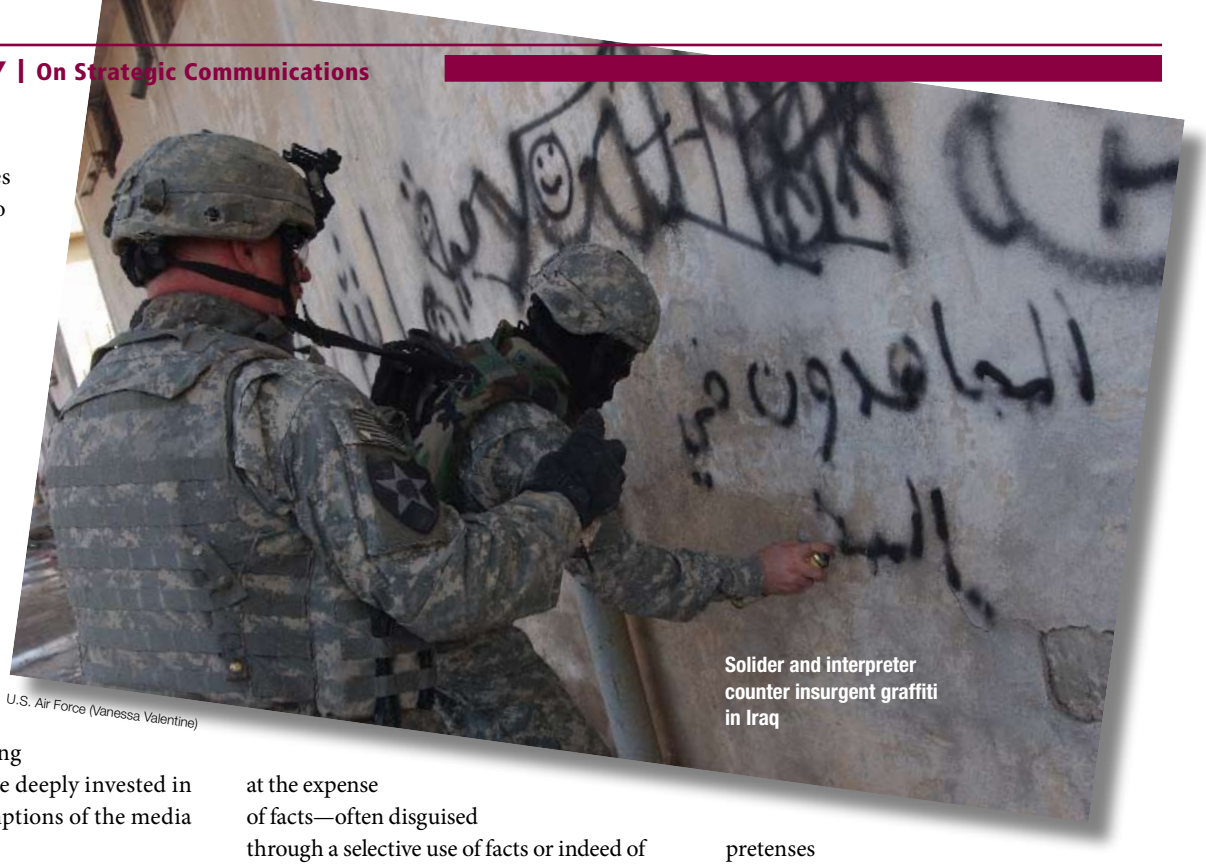
Afghan National Police officer reads free newspaper

55th Combat Camera Company (Bertha Flores)

Truth Versus Journalism

The OSI incident highlights the powerful constraints imposed on the U.S. Government in the strategic communications arena by American political culture—more specifically, the culture of the so-called mainstream media. These constraints operate in several ways. Most obviously, the media directly shape the strategic communications agenda by defining what is newsworthy, setting the standards by which news is reported, and framing news items in what might be called a narrative of their own. Anyone familiar with the operating environment of the

Carnes Lord is Professor of Military and Naval Strategy in the Strategic Research Department of the Center for Naval Warfare Studies at the U.S. Naval War College. He is the author of *Losing Hearts and Minds? Public Diplomacy and Strategic Influence in the Age of Terror* (Praeger, 2006).



U.S. Air Force (Vanessa Valentine)

Solider and interpreter counter insurgent graffiti in Iraq

media understands the power of such narratives and how difficult it is to correct the impression they initially make on an audience. Second, and not so obviously, the media form the strategic communications agenda by shaping the outlook of those laboring in the strategic communications vineyards. In fact, many of these people were trained as journalists, worked in commercial journalism before joining the government, and are deeply invested in the fundamental assumptions of the media world.

Among these fundamental assumptions is a set of beliefs about what I shall simply call "truth"—about what constitutes truth in the context of journalism as well as the value of truth so understood. A careful analysis of these beliefs can help us understand the limitations of contemporary journalism and thereby provide some necessary perspective on the proper tasks and challenges facing strategic communications by governments.

the media form the strategic communications agenda by shaping the outlook of those laboring in the strategic communications vineyard

Perhaps the overriding characteristic of journalistic truth is empiricism. By this I mean that journalists anchor their stories by reference to observed facts or to facts or opinions derived from contact with living individuals. The problem, of course, is that facts do not simply speak for themselves and also that recitals of facts by themselves are unappealing as a practical matter to the mass audiences for whom journalists write. So these facts are embedded in a story that links them and tries to make sense of them (the "narratives" I mentioned earlier). Good journalism is defined by skill in melding facts with narratives. Bad journalism has two extremes; the more dangerous is the extreme that purveys narratives at the expense of facts—often disguised through a selective use of facts or indeed of invented facts or pseudo-facts. Spectacular cases of bad journalism of this sort are not especially rare these days even in American media of the highest prestige (*The New York Times* being a recent case in point). It is also worth noting that such journalism is more the norm than the exception in many other parts of the world, and particularly in the Middle East. Indeed, in many regions of the globe, truth in any sense has at best a tenuous relationship to the profession of journalism.

A rarely questioned belief of contemporary journalism is that truth in the sense just discussed is valuable to its audiences. A bedrock conviction as to the utility of truth is at the heart of American journalism's self-understanding, linked to its conviction of the absolute sanctity of the free speech provision of the first amendment to the U.S. Constitution. It does not take a great deal of philosophical analysis to see that this belief is totally untenable. There is little visible utility, for example, in extended media coverage of mining disasters, triple murders, or interstate pile-ups; at the end of the day, this is journalism as entertainment, not public service. The widely noted tendency of the American media today to cover war in the spirit of a spectator sport is equally problematic from this perspective. The point of all this is not to trash the media but simply to question the pretenses of the media to the moral high ground in their ongoing if undeclared war against the strategic communications programs of the U.S. Government.

Let me return to the issue of truth. To see clearly the limitations of journalistic truth, we might distinguish two other sorts of truth. One kind I will call "granular truth," the other "higher truth." By granular truth, I mean a level of truth that reflects a greater degree of analysis than is generally performed by journalists. Such analysis provides essential context for understanding the meaning of the empirical facts that journalists present; it can be historical, comparative, or quantitative in character. Generally, this sort of analysis is what historians or social scientists do. There is nothing preventing journalists from doing it themselves, and the best sometimes do, but generally they lack the time and the appropriate skills. One might think that academic analysis can be directly appropriated by journalists to shape their narratives. The reality is that such studies are cited by journalists more than they are actually read, and often serve decorative as much as substantive purposes. In bad journalism, the use of such material often borders on the fraudulent or serves a barely disguised ideological agenda.

By higher truth, I have in mind something such as the Platonic notion of a level of reality that is in a sense more real than the merely empirical. This is the realm of

grand ideas, of fundamental truths about man, nature, the right form of government, the best life, and, not least, war. At the end of the day, the empirical facts of journalistic truth are meaningless unless they can be located in relation to truth in this sense. Journalists are particularly ill equipped to perform such a function, though again, there are exceptions (for example, consider someone such as Timothy Garten Ash, or from an older era, the great Walter Lippmann). Examples of higher truths in this sense are Clausewitz's "fog of war," or his thought that intelligence in war is unreliable.

military psychological operators regularly claim that American PSYOP deals only in truth

Implications for Strategic Communications

Let us return to the OSI incident. Much confusion has arisen over the question of whether OSI activities involved "lying" to the media. While there was apparently a small covert component to the OSI kitbag involving press placements with foreign—not domestic—media, there is no evidence that these placements were anything other than truthful in the ordinary journalistic sense. Military psychological operators in fact regularly claim that American PSYOP deals only in truth. If or to the extent that this is correct, however, it becomes difficult to distinguish PSYOP from public diplomacy—or, for that matter, from public affairs, the strategic communications interface with the domestic media. But the psychological operators seem unable to convince others that this is really the case.

A major study published recently by the National Defense University of lessons learned from our recent operational experience reveals considerable unhappiness on the part of field commanders with the performance of PSYOP forces in Iraq and Afghanistan and argues that there is a pressing need to reconceptualize the PSYOP discipline.[2] In particular, it holds that the notion that psychological operations only deal in truth is self-defeating and unsustainable and that much more attention needs to be given to increasing the persuasiveness of PSYOP messages through appealing to human emotions. It suggests that psychological operations need to be reoriented to support combat commanders at the tactical and operational level, rather than producing public diplomacy, such as materials for theater-wide consumption. Such a reorientation could go a long way to clarify the respective missions of PSYOP and public affairs and reduce the tensions between them.

Whether DOD has a distinct public diplomacy function apart from supporting State Department requirements in this area is a murky question, but I believe the answer has to be *yes*.[3] There is a wide range of public diplomacy issues that can only be effectively handled by people with intimate and current knowledge of defense and security matters (consider the enormous role that intelligence issues have had in the public debate in this country and abroad over the war in Iraq). The core of the defense public diplomacy function is counterpropaganda, counterdisinformation, and the care and feeding of the foreign press. The core of the defense public affairs function is the care and feeding of the domestic press. As such, it is fair enough to say that both of these disciplines deal in "truth."

To differentiate them properly, however, let us return to the different senses of truth discussed earlier. A case can be made that public diplomacy needs to operate not only at the journalistic level of truth but also at the granular and the higher truth levels. Public diplomacy and public affairs alike need to keep journalism honest by countering factual lies or mistakes and—perhaps more importantly—challenging its narratives when they become overly detached from empirical truth. At the same time, public diplomacy should operate in more sophisticated modes. It should be able to bring to bear, if only in limited ways, the granular contextual analyses of historians and social scientists, and it should be able to tap into the higher truth—if you like, "bigger picture"—interpretations of metajournalists, intellectuals, or philosophers. To state the matter in this way is to make it obvious that not only the Defense Department but also the State Department itself—the lone official guardians of public diplomacy today—are a long way from having such capabilities. **JFQ**

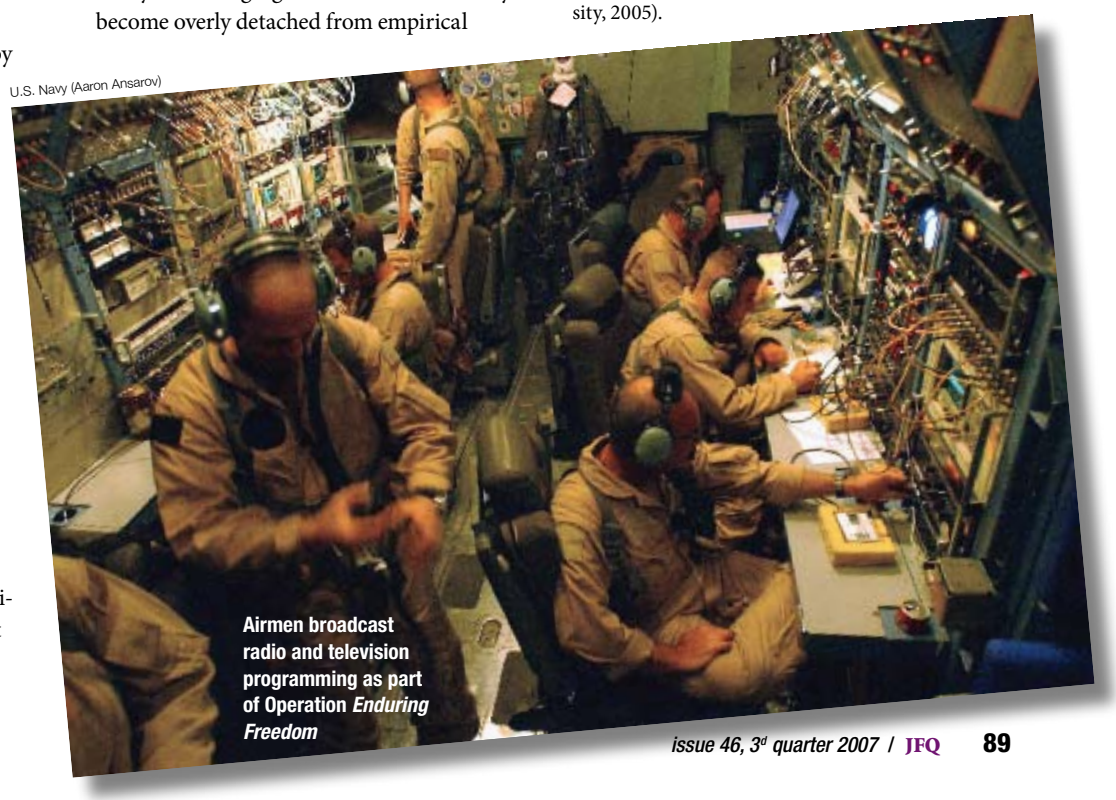
NOTES

[1] See Brigadier General Simon P. Worden, USAF, Lieutenant Colonel Martin E.B. France, USAF, and Major Randall R. Correll, USAF (Ret.), "Information War: Strategic Influence and the Global War on Terror," unpublished paper, October 2002. General Worden (since retired) was Director of the Office of Strategic Influence.

[2] See Christopher J. Lamb, "Review of Psychological Operations Lessons Learned from Recent Operational Experience" (Washington, DC: National Defense University Press, 2005), available at <www.ndu.edu/inss/Occassional_Papers/Lamb_OP_092005_Psyops.pdf>.

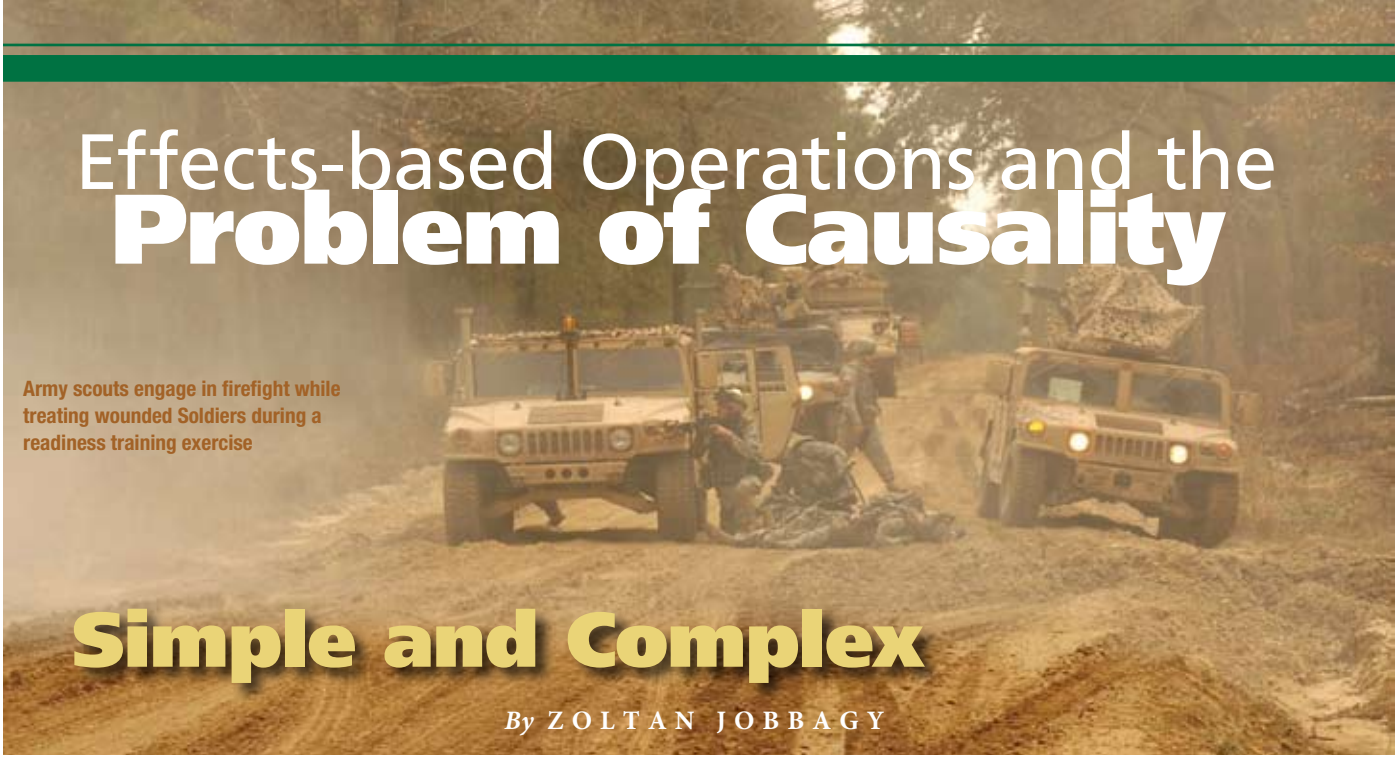
[3] See Robin A. Campbell, Lieutenant Colonel Annette N. Foster, ANG, and Lieutenant Colonel Steven J. Smith, USA, *Harnessing the Military's Voice: An Argument for a Greater Role in Public Diplomacy by the U.S. Military,* National Security Program Discussion Paper Series (Boston: John F. Kennedy School of Government, Harvard University, 2005).

U.S. Navy (Aaron Ansarov)



Airmen broadcast radio and television programming as part of Operation *Enduring Freedom*

Effects-based Operations and the Problem of Causality



Army scouts engage in firefight while treating wounded Soldiers during a readiness training exercise

U.S. Army (Shawn Cassatt)

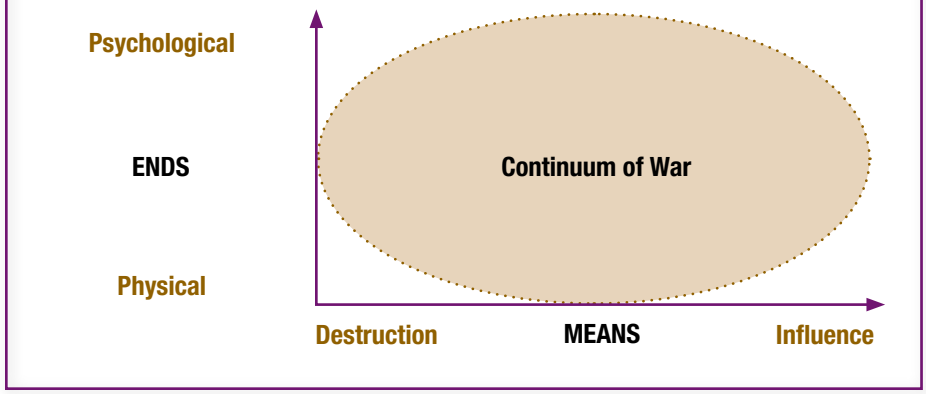
Simple and Complex

By ZOLTAN JOBBAGY

It has become fashionable in most armed forces worldwide to go "effects-based." The *2006 Quadrennial Defense Review Report* emphasizes explicitly the need to make the shift "from massing forces—to massing effects" and "from focusing on inputs (effort) to tracking outputs (results)."[1] In a similar fashion, the North Atlantic Treaty Organization (NATO) is adopting the effects-based approach in order to drive force employment and transformation. The Alliance claims that its interest in effects in military operations represents "a fundamental way of thinking that focuses on the efficient and effective achievement of desired effects in the operational environment, vice a primary focus on the completion of assigned tasks."[2] Armed forces outside NATO are moving in an effects-based direction, too; for example, the Israel Defense Force chief of staff emphasized that force transformation issues must focus less on force and power but more on effect.[3]

It appears that nothing can stand against the power that comes from a causal focus aimed at achieving various sorts of effects on the enemy. However, there are many reasons to be doubtful regarding the practical utility of *effects-based operations* and the *effects-based approach* in general. Thus, the aim of this article is to address some basic assumptions upon which the two neologisms are built and analyze whether those assumptions are valid.

Figure 1. The Continuum of War in Terms of Ends/Means Relationships



Lieutenant Colonel Zoltan Jobbagy is a member of the Hungarian Defense Forces. He is assigned to the Planning and Coordination Department, Human Strategy Division, at the Ministry of Defense in Budapest.

Setting the Scene

To understand war in terms of causality better, we suggest depicting it as a continuum characterized by an ends/means relationship as seen in figure 1. Whereas ends can be placed on the vertical axis, characterized by the combination of physical and psychological effects, the means can be located along the horizontal axis, ranging from destruction to influence.

Thus, effects can occur on a spectrum characterized both by tangible and intangible attributes. In a similar way, Carl von Clausewitz indicated the existence of a material and a nonmaterial domain in war. As he emphasized, war is "a trial of moral and physical forces through the medium of the latter" in which "psychological forces exert a decisive influence on the elements involved."[4] Based on figure 1, the following is proposed in terms of effects:

- The material domain represents categories such as physical strengths and stamina. They describe the space that the military tries to influence through combat and maneuver. In the material domain, we deal with tangible items such as physical platforms and communications networks that the enemy usually needs to wage war. This is the traditional basis for measuring combat power that has to be rendered useless. The material domain can be defined as reality proper or ground truth. Attempts to achieve effects in this domain aim at physical ability and serve the purpose of changing functions.

■ The nonmaterial domain is characterized by psychological factors such as moral strength and stamina. It represents the mind and attributes that generally influence the will in the form of perception, awareness, understanding, belief, and values. Effects in this domain stand for influencing intangibles that the enemy needs to wage war. Consequently, effects in the nonmaterial domain aim at changing behavior.[5]

Despite the difference regarding the two domains, we assume a strong correlation between them as physical and psychological factors form an organic whole. As Clausewitz emphasized, the physical domain is the "wooden hilt," whereas the psychological domain is "the real weapon, the finely honed blade."[6]

F–16C Falcon flies over Nellis Air Force Base

U.S. Air Force (Aaron Allamon)

effects can occur on a spectrum characterized both by tangible and intangible attributes

Semantic Issues

Before we proceed with our inquiry, it is equally important to understand what the term *effect* stands for. In normal English usage, an effect indicates a result or outcome, something that is produced by an agent or cause. Thus, an effect immediately follows the antecedent as a resultant condition and implies something that necessarily and directly follows a cause. Terms such as *result*, *consequence*, *upshot*, *after-effect*, *aftermath*, *sequel*, *issue*, *outcome*, and *event* are all regarded as synonymous with *effect* and generally signify a condition that is ascribable to a cause or a combination of causes.

A further skim of the dictionary makes clear that *effect* refers to so many meanings that it might not obviously promote precision and clarity of military language. As one observer ironically remarked, if the proponents of the effects-based approach "were aware of the many different meanings and usages of the term *effect* it is doubtful that they would have made it the first choice among the words they wanted to use."[7] The second and probably bigger problem arises from the fact that although an effect follows an antecedent directly, both effects-based operations and the effects-based approach focus on achieving higher order, follow-on effects mostly in the psychological domain. Unfortunately, semantically, any reference to indirect or higher order effects becomes questionable at best and empty at worst. The more we move toward higher order effects, the more we depart from an effects-based approach and arrive at something that would better be named *consequence-based*, *outcome-based*, or *event-based*. Thus, the more we move toward psychological effects aimed at influencing enemy behavior, the more meaningless the two neologisms become. Clausewitz pointed out in *On War* that whatever we do, "consequences of some kind always follow."[8] He indicated that regardless of what we do, we achieve effects anyway. This, however, means that both neologisms might essentially be vacuous, and it can turn out that we refer to something that is scarcely more than a military truism or commonplace.

Dissecting the Mechanism

Even proponents claim that a successful implementation of an effects-based approach is extraordinarily difficult and requires hard thinking. Some acknowledge that any single action can produce more than one effect, which requires that we consider all potential consequences of the actions taken. It is also stated that effects have a "dual nature" as they ripple and cascade through the enemy system. Thus, the effect of a given action may induce further changes with the result that it becomes increasingly difficult to predict higher order effects.[9] This difficulty in both predicting and achieving desired effects, especially in the psychological domain, indicates that the mechanism linking causes with effects can also be regarded as the Achilles' heel and resembles gambling.

As a rule of thumb, the more we move toward higher order psychological effects, the more difficult it becomes to identify causal linkages. Effects appear to be complex phenomena, as cause-and-effect relationships are of intricate nature. To understand the mechanism of causality better, we suggest examining it along two dimensions, such as couplings and interactions. Although these dimensions were originally introduced to study the way accidents happen, they can also explain, in a slightly modified form, the way causal relationships develop. They indicate four rough areas representing different sorts of causality since interactions can be linear or complex, and couplings tight or loose.[10]

The first dimension is interactions. Due to their simplicity and comprehensibility, linear interactions allow for visible and simple relationships between causes and effects. Linearity can be anticipated since the underlying sequence of causality is directly comprehensible. Complex interactions indicate branching paths, feedback loops, and jumps from one sequence to another. Connections can multiply in unexpected ways, often revealing unintended and unfamiliar effects. Causal relationships are outside the normal and assumed sequence of events, as they are either invisible or not immediately comprehensible.[11] Linear interactions can also display invisible cause-and-effect strains, but they occur mostly in a well-defined segment and sequence. Complex interactions do not stand for a well-defined segment or sequence, as causes and effects can be linked differently and may interact in unexpected ways. Causal processes are more indirect and inferential (in the case of complex interactions, for instance, not even the top of an iceberg is visible). We have to expect a wide array of misunderstood

or missed signals and faulty information regarding causes and their likely effects. Whereas linear interactions have minimal feedback loops and are generally clear and concise, complex interactions are more likely to display unanticipated or unintended relationships.[12]

The second dimension is couplings, which refer to slack or buffers in cause-and-effect relationships. Tight couplings do not contain slack or buffers; these refer to direct causality in which an effect is coupled to a cause. Loose couplings can best be characterized by ambiguity and flexibility, since connections can remain unobserved. Whereas loose couplings make it possible to display logic in terms of causality, tight couplings restrict such attitudes. Loose couplings are also more stable since they can accommodate shocks without destabilization. In contrast, tight couplings generally respond in a quicker and more disastrous fashion to perturbations.[13] To sum up the preceding structural analysis, we can state the following:

- Linear interactions indicate spatial segregation and dedicated connections. They refer to attributes such as easy substitution with only a few feedback loops. They also allow for single-purposed and segregated control, as the emphasis is on direct information that makes an extensive understanding possible.
- Complex interactions are based on proximity and common mode connections. They display interconnectedness, which means limited substitution and many feedback loops. They require multiple and interacting control, which stands for indirect information and limited understanding.
- Tight couplings do not make delays possible. Due to the underlying invariance of sequences, there is only a small amount of slack. Should buffers and redundancies exist, they are mostly built-in features that allow only for limited substitution. In tight couplings, there is hardly any spatial and temporal separation between a cause and effect.
- Loose couplings allow for delays due to the changeable order of sequences. The result is extended and often unanticipated sets of alternative methods, slack, and buffers in which substitutions are fortuitously available.

the more we move toward higher order psychological effects, the more difficult it becomes to identify causal linkages

Projecting the Mechanisms

It became clear that linear interactions refer to highly structured, logical, sequential, and predictable cause-and-effect relationships. In contrast, complex interactions offer less predictability due to the presence of unplanned and unforeseen relationships. Tight couplings can be described by high centralization and rigidity, which allow for a close monitoring and a certain tolerance. Loose couplings mean decentralized operations and allow for a wide variety of outcomes in terms of effects.[14]

Based on the four combinations of interactions and couplings, we suggest subdividing the continuum of war, as depicted in figure 2, into four different but interrelated areas such as simple, complicated, complex, and chaotic.[15] The more we move from the first area to the last, from tightly linear to tightly complex, the more the level of causality decreases, and in the case of the latter, it disappears entirely. The figure also shows that even if it is possible to discern causality in terms of physical effects due to the underlying mechanism, it is mostly impossible to see which way a particular effect relates to subsequent and desired psychological consequences.

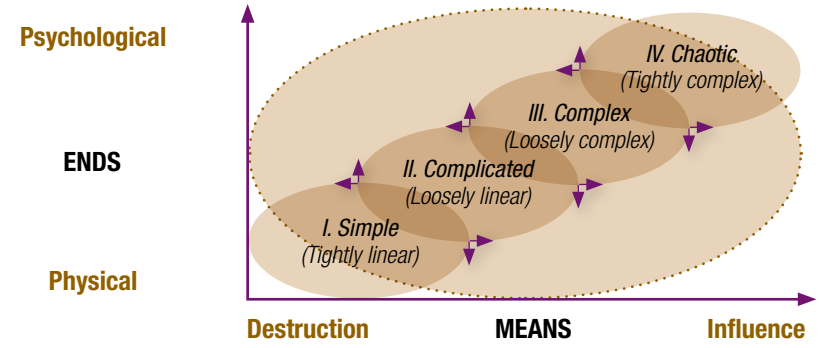
The growing instability of couplings and interactions points toward an increasing difficulty in decoding causal relationships. Nevertheless, the following listing explains some characteristics of the combinations found in figure 2:

- *Simple*. Area I can be described as tightly linear and stands for linear causality, indicating known causes and effects. We can discern clear and visible cause-and-effect relationships that allow for prediction. Due to their empirical nature, causal relationships are not open to dispute and planning. Consequently, this area can be characterized by the predominance of centralized causes and effects.
- *Complicated*. Area II can be described as loosely linear and refers to knowable causes and effects. Although causal relationships exist, due to spatial and temporal separations, they might not become fully known. The relationship between causes and effects is generally difficult to comprehend, which indicates limitations in terms of prediction. Planning for effects still makes sense, but we must take into

Officer walks through rubble after firefight with insurgents in Salah Ad Din, Iraq

U.S. Army (Russell Klika)

Figure 2. The Flattened Quadrant Projected on the Continuum of War



account that centralized causes increasingly yield decentralized and unexpected effects.

- *Complex*. Area III can be described as loosely complex. Cause-and-effect relationships still exist, but they defy most attempts at categorization or other analytical techniques. Effects can be perceived but not predicted since their relationship is not open to any inspection. Both interactions and couplings indicate that causes and effects are mostly decentralized and appear coherent only retrospectively, but even then, causality is subject to debate.
- *Chaotic*. Area IV can be described as tightly complex. Here, no visible cause-and-effect relationships exist, which indicates that causality is not perceivable. The number of factors together with spatial and temporal separations makes prediction either impossible or confined to very general terms. In this area, it is not possible to plan for effects or to discern causal relationships in a meaningful way.[16]

The two dimensions made it possible to dissect war into four interrelated areas with different characteristics. In colloquial terms, we can say that in tightly linear systems, everyone can detect causality. In loosely linear systems, only experts might detect causality, and in loosely complex systems, causality often becomes clear only retrospectively. In tightly complex systems, there is no discernible causality that can guide our actions.[17] Thus, the more we move toward tightly complex attributes, the more unpredictability takes hold.

Unfortunately, the "high ambition" of the effects-based approach indicates a focus on an area where it is very difficult, if not impossible, to detect and exploit causality. A further problem is that even the area in which we *can* discern clear causality interacts with areas that are rather unpredictable. Consequently, we must expect novelty everywhere and every time in war. In other words, the Clausewitzian assumption that in war, everything is simple but even the simplest thing can become difficult generally takes hold. The four areas also remind us that if we have no firm basis for comprehending the initial state with all the factors that must be considered, we have equally no basis to judge which of the possibilities should be regarded as desired effects. Thus, we claim that even if effects-based operations or the effects-based approach worked, they would offer considerable promise only for physical effects—but in the case of psychological effects, they appear hopeless. In the case of systemic effects, the concept touches the borderline that separates prediction from pure guesswork. So an effects-based approach is generally good for creating desired physical effects and might occasionally be good for generating desired systemic effects. However, in the case of psychological effects, the best we can say is that the concept does not work well.[18]

Continuum as Complexity

Analyzing the continuum of war along the two dimensions makes it possible to see the way structures are produced and dissolved in causal terms. The four areas make clear that war stands for a general unpredictability that has serious consequences for effects-based operations and the effects-based approach. Moving toward the pole characterized by "physical/destruction" indicates direct causality and prediction, but the value of the effects achieved is normally seen as low. Although effects achieved around the "psychological/influence" pole have high values, they increasingly prohibit predictions in causal terms. It is a truism to state that in war all activities take place in an environment in which chaos meets order constantly in a disorderly way. However, the four areas indicate war to be a phenomenon in which pre-order meets order in disorder as occurrences move continuously back and forth in the continuum. This is also in accordance with Clausewitz's observation regarding the nature of war. His Dynamic Law depicts war as a phenomenon in which "periods of active warfare [are] always . . . interspersed with greater or smaller periods of rest." According to him, every "action in war is not continuous but spasmodic. Violent clashes are interrupted by periods of observation, during which both sides are on the defensive." As he emphasized, the "state of crisis is the real war; the equilibrium is nothing but its reflex."[19]

Due to such attributes, war can best be described by the term *complexity* since it denies the primacy of order and causality and the drive for efficiency and constant affirmation. In general we can say that complexity stands for freedom and openness, which puts an emphasis on action and possibility.[20] It demands that we take the various interdependences better into account. Links between

Tomahawk cruise missile fired from nuclear-powered submarine USS *Florida* during Exercise Giant Shadow

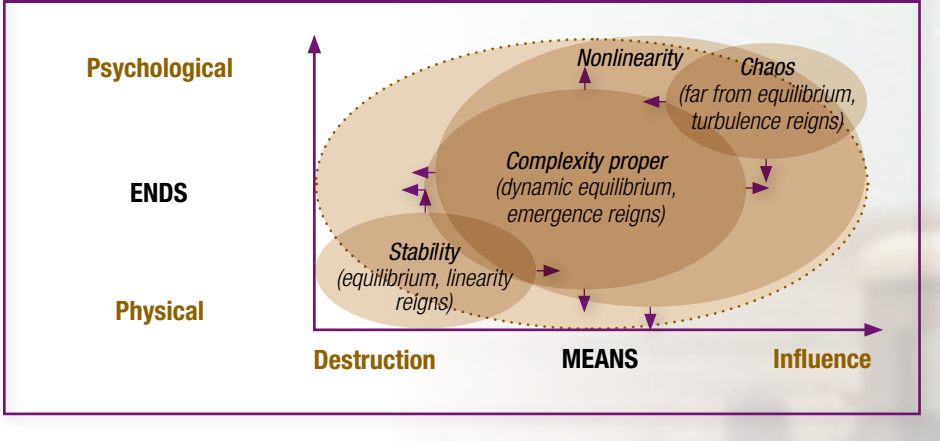
U.S. Navy

causes and effects can become distant in time and space, and in the case we proceed as if "simple linear links exist, even if we do not know what they are, then we are likely to undertake actions that yield unintended and surprising results."[21] Complexity displays a bewildering array of causal relationships that spans several scales in which we have to deal with emergent properties that come from the constant interplay of chaotic and non-chaotic forces. The result is a broad network of various alternatives that cannot be represented based on reasoning and causality.

We made clear that the combination of interactions and couplings can often produce unforeseeable results. However, the four areas also make discernible an explanatory framework that helps us to understand better the consequences of our actions and the spatial and temporal effects generated.[22] The four combinations allow for establishing generalized areas in the continuum of war as depicted in figure 3. In these areas, different characteristics overlap and constantly influence each other, making cause-and-effect relationships difficult to identify. As we can see in war, linearity goes together with nonlinearity and stability always coexists with complexity and chaos. Whereas stability stands for simplicity and linearity reflecting a tight and linear relationship between causes and effects, nonlinearity points toward chaos that can be described by extreme sensitivity to initial conditions.

The biggest area within the continuum of war is complexity proper, which stands for nonlinearity, far-from-equilibrium conditions, and emergence. The figure clearly shows that although war contains linear properties, its mechanisms are mostly defined by nonlinear attributes. Consequently, we must rethink the basic mechanism that drives effects-based operations and the effects-based approach and shift our reasoning away from prediction aimed at identifying desired effects.[23] The generalization also indicates that the continuum of war can reveal both deterministic outcomes and random fluctuations. This constant shuffling between stability and instability explains why war can display "growth and decay, capture and domination, periods of opportunity for alternative developments followed by solidification of the existing domination structures."[24] Put simply, war displays emergent and interactive attributes that come as a result of structured but nonadditive interactions. It is more than the sum of its constituents, and we always face a general unpredictability in relation to the input.

Figure 3. Overlapping Characteristics of War



The belligerents continuously adjust and adapt, providing them with multiple and often unexpected paths, making causal explanations very difficult.[25] Instead of a causal focus, war requires an everything-affects-everything-else model in order to grasp the entire web of various connections. War is a messy phenomenon that cannot be examined through conceptual elegance reflecting rational thinking, deductive logic, and analytical categorization. It contains novelty that often comes from simple properties producing emergent and unpredictable effects. Depending on the level chosen, we always confront structures for which different laws, concepts, and generalizations apply. In contrast to most assumptions that drive effects-based operations and the effects-based approach, war stands for an infinite variety of possibilities and a general unpredictability regarding causes and their likely effects.[26]

complexity stands for freedom and openness, which puts an emphasis on action and possibility

Conclusion

The effects-based approach emphasizes deductive reductionism and causal laws in order to predict desired effects. The supporting assumption is that war displays order and equilibrium, the possibility for rational choice, and the ability to steer and control events. Unfortunately, war stands for variety and novelty in which certain properties remain inherently unknowable to the human mind. This short analysis reveals that although war can be described in general terms using causal relationships, effects that go beyond the immediate spatial and temporal horizon cannot be predicted with any accuracy. Complexity indicates something very different than the fundamental assumption of the two neologisms—namely, that it is possible to comprehend only some things, especially those that are local to us both in space and time.

Everything in war is interrelated, and we can attain nothing more than a temporary and partial interpretation. Complexity also reminds us that we tend to confuse causation with correlation and simulation with prediction. Whereas the former refers to our preference for creating retrospective validation to identify best practices, the latter points to the fact that even if we can simulate something, it does *not* mean that we can equally predict its future.[27] War is a phenomenon full of discontinuities and uncertainty, which indicates a general unpredictability that makes both individuals and organizations disoriented. This uncomfortable feeling explains why focusing on effects appears attractive for so many. The international arena has been a messy place since the demise of the bipolar world order. During turbulent times in which orientation becomes difficult, humans increasingly turn to panaceas for advice. If we do not understand or cannot cope with challenges, we often look for simple or simplistic solutions that promise quick help.[28] The unpredictability of war stands for several possible futures in which there is not always time for mechanical, deductive systemic analyses aimed at detecting causality. The most important message

war is full of discontinuities and uncertainty, which indicates a general unpredictability that makes both individuals and organizations disoriented

of complexity is that instead of focusing on certain desired effects, we should rely on the ability to respond consistently to war's unpredictable nature. War cannot be waged based on single and prescriptive models but requires that we evolve rapidly to handle dynamic and changing situations.[29]

The serious contradiction between the basic assumptions behind the two neologisms and the complex nature of war naturally raises the demand for a better conceptualization. Unpredictability of war indicates that we must be satisfied with understanding certain general features in terms of correlation rather than attempting to discover a mechanism that links causes with effects directly. Consequently, the unpredictable nature of war should be regarded as an opportunity that can explain qualitative behavior instead of inaccurately predicting futures in terms of desired effects.[30] This, however, indicates a low practical ceiling both for effects-based operations and the effects-based approach. **JFQ**

NOTES

[1] Military Operations Research Society (MORS), "Analyzing Effects-Based Operations Workshop Report" (Alexandria, VA: MORS, January 2, 2003), available at <www.mors.org/publications/reports/2002-Analyzing_Effects_Based_Operations.pdf>; Department of Defense (DOD), *2006 Quadrennial Defense Review Report* (Washington, DC: DOD, February 6, 2006), 5; Tony Skinner, "NATO endorses effects-based approach," *Jane's Defence Weekly*, April 26, 2006, 5.

[2] Marvin Barnes, "Effects-based concepts face test in Turkey," ACT Operational Experimentation, February 14, 2006, accessed at <www.act.nato.int/multimedia/articles/2006/060214mne4.html>.

[3] Robin Hughes, "Interview: Lieutenant General Moshe Ya'alon, Israel Defence Force Chief of Staff," *Jane's Defence Weekly*, November 17, 2004, 34.

[4] Carl von Clausewitz, *On War* (New York: Everyman's Library, 1993), 145.

[5] David S. Alberts et al., *Understanding Information Age Warfare* (Washington, DC: DOD C4ISR Cooperative Research Program, 2001), 12–14; Jon Huss, "Exploiting the Psychological Effects of Air Power: A Guide for the Operational Commander," *Aerospace Power Journal*, no. 4 (Winter 1999), 23; Iain McNicoll, "Effects-Based Operations: Air Command and Control and the Nature of the Emerging Battlespace," *RUSI Journal* 148, no. 3 (June 2003), 39.

[6] Clausewitz, 217.

[7] Paul K. Van Riper, personal communication to author, September 5, 2006.

[8] Clausewitz, 212.

[9] Dennis J. Gleeson et al., "New Perspectives on Effects-Based Operations: Annotated Briefing," Institute for Defense Analyses, Joint Advanced Warfighting Program (June 2001), 13–15; U.S. Joint Forces Command J9, "A Concept Framework for Effects-Based Operations," White Paper Version 1.0, October 18, 2001, 8–15; Edward Mann et al., *Thinking Effects: Effects-Based Methodology for Joint Operations*, CADRE Papers No. 15 (Maxwell AFB, AL: Air University Press, October 2002), 25–34, available at <www.au.af.mil/au/awc/awcgate/cadre/mann.pdf>.

[10] Charles Perrow, *Normal Accidents: Living with High-Risk Technologies* (New York: Basic Books, 1984), 63.

[11] Ibid., 75–78.

[12] Ibid., 79–85.

[13] Ibid., 86–92.

[14] Tom Czerwinski, *Coping with the Bounds: Speculations on Nonlinearity in Military Affairs* (Washington, DC: DOD C4ISR Cooperative Research Program, 1998), 89–92, 96–98; Perrow, 332.

[15] Zoltan Jobbagy, "Wars, Waves and the West: Putting Effects-Based Operations into Context," TNO Defence, Security and Safety, TNO–DV1 2004 B077, May 2005, 47–57, available at <www.ccss.nl/publications/2005/20050500_ccss_report_zobbagy.pdf>.

[16] Cynthia F. Kurtz and David J. Snowden, "The new dynamics of strategy: Sense-making in a complex and complicated world," *IBM Systems Journal* 42, no. 3 (2003), 468–469; David J. Snowden and Peter Stanbridge, "The Landscape of Management: Creating the context for understanding social complexity," ECO Special Double Issue, 6, no. 1–2 (Fall 2004), 144–145.

[17] Kurtz and Snowden, 472.

[18] Edward N. Lorenz, *The Essence of Chaos* (London: University College London Press, 1993), 102–110.

[19] Carl von Clausewitz, *On War* (Chicago: NTC/Contemporary Publishing Company, 1997), 257, 260, 262.

[20] Eric Lefebvre and Hugo Letiche, "Managing Complexity from Chaos: Uncertainty, Knowledge and Skills," *Emergence* 1, no. 3 (1999), 7–15; Robert Axelrod and Michael D. Cohen, *Harnessing Complexity, Organizational Implications of a Scientific Frontier* (New York: The Free Press, 1999), 28–31; Michael R. Lissack, "Complexity: The Science, Its Vocabulary, and Its Relation to Organizations," *Emergence* 1, no. 1 (1999), 110–125.

[21] Ralph D. Stacey, *Strategic Management & Organisational Dynamics* (London: Pitman Publishing, 1996), 275; Hiroshi Tasaka, "Twenty-first-century Management and the Complexity Paradigm," *Emergence* 1, no. 4 (1999), 115–123.

[22] Simon A. Levin, "Complex Adaptive Systems: Exploring the Known, the Unknown and the Unknowable," *Bulletin of the American Mathematical Society* 40, no. 1 (2003), 163–168; Michel Baranger, "Chaos, Complexity, and Entropy: A physics talk for non-physicists," (Cambridge, MA: Massachusetts Institute of Technology, n.d.), 9–11, available at <http://necsi.org/projects/baranger/cce.pdf>; Paul Cilliers, *Complexity and postmodernism: Understanding Complex Systems* (London: Routledge, 1998), 2–5; Grégoire Nicolis and Iliya Prigogine, *Exploring Complexity: An Introduction* (New York: W.H. Freeman and Company, 1989), 5–8, 31–32; Ilya Prigogine and Isabella Stengers, *Order out of Chaos: Man's New Dialogue with Nature* (Portsmouth, NH: Heinemann, 1984), 131–137.

[23] Czerwinski, 39–60; John Briggs and David F. Peat, *Turbulent Mirror: An Illustrated Guide to Chaos Theory and the Science of Wholeness* (New York: Harper and Row, 1989), 174–180.

[24] Stacey, 324.

[25] Marion Russ and Josh Bacon, "Organizational Extinction and Complex Systems," *Emergence* 1, no. 4 (1999), 75–79; Douglas Griffin, Patricia Shaw, and Ralph Stacey, "Knowing and Acting in Conditions of Uncertainty: A Complexity Perspective," *Systemic Practice and Action Research* 16, no. 2 (April 2003), 302–304.

[26] Mitchel M. Waldrop, *Complexity: The Emerging Science at the Edge of Order and Chaos* (New York: Viking Press, 1992), 38–39, 60–63, 81–83.

[27] Robert L. Flood, "Knowing the Unknowable," *Systemic Practice and Action Research* 12, no. 3 (1999), 247–252; Kurtz and Snowden, 462–463; Snowden and Stanbridge, 146; Stacey, 346–347.

[28] Russel T. Ackoff, "Fundamentalism and Panaceas," *Systemic Practice and Action Research* 14, no. 1 (2001), 3–10; Clayton M. Christensen and Michael E. Raynor, "Why Hard-Nosed Executives Should Care about Management Theory," *Harvard Business Review* (September 2003), 67–74; James N. Rosenau, "Many Damn Things Simultaneously: Complexity Theory and World Affairs," in *Complexity, Global Politics, and National Security*, ed. Thomas J. Czerwinski and David S. Alberts (Washington, DC: National Defense University Press, 1997); and Steven R. Mann, "The Reaction to Chaos," in *Complexity, Global Politics, and National Security*.

[29] David Snowden, "The Paradox of Story," *Scenario and Strategy Planning* 1, no. 5 (November 1999), 16–20.

[30] Claus Emmeche, Simo Køppe, and Frederik Stjernfelt, "Explaining emergence: Towards an ontology of levels," *Journal for General Philosophy of Science*, no. 28 (1997), 116, available at <www.nbi.dk/~emmeche/coPubl/97e.EKS/emerg.html>.

Officer remotely operates Predator MQ–1 in

U.S. Air Force (Chad Kellum)

Military Officer Attitudes Toward UAV Adoption
Exploring Institutional Impediments to Innovation

By JAMES R. FITZSIMONDS *and* THOMAS G. MAHNKEN

The prospective introduction of large numbers of unmanned aerial vehicles (UAVs) arguably represents the most significant ongoing development in U.S. military aviation in decades.[1] The inventory of large UAVs across all Services is projected to increase from 250 in late 2005 to over 1,400 by 2015. Moreover, more than 1,000 mini-UAVs and an undetermined number of even smaller micro-UAVs are projected to enter service during the same period.[2] Until recently, it could be argued that immature technology and relatively poor operational performance made UAVs inferior to manned aircraft, even for the so-called dull, dirty, and dangerous missions.[3] However, ongoing developments in computer control and long-range data links show great near-term promise for many types of UAVs to match, or even exceed, the effectiveness of manned aircraft in a number of roles. If so, the growing arsenals of UAVs will have the potential to take increasing numbers of aviators out of the cockpit.

In his well-known case studies of naval innovation, historian Elting Morison characterized a military service as a self-contained society in which members tend to "find the definition of their whole being."[4] It is generally accepted that the military profession possesses a distinct set of traditions and values that defines this society and distinguishes it from the civilian world. As Morison and others have pointed out, transitions from one type of military approach or system to very different operational concepts or technologies have a major impact on the individuals within these societies. Innovations require new types of skills and different professional knowledge, which in turn render the old skills and knowledge less important. Innovative systems generally demand different tactical employment schemes and operational concepts, which in turn affect command authority, hierarchical relationships, and institutional control of both people and resources. Increasing numbers of officers pursuing the new area of professional specialization actively seek different career

James R. FitzSimonds is Research Professor in the Center for Naval Warfare Studies at the U.S. Naval War College. Thomas G. Mahnken is Professor of Strategy at the U.S. Naval War College.

paths for promotion and command, putting them in competition with "traditionalists." This was certainly true for the introduction of the steamship, aircraft, tank, aircraft carrier, and other major innovations over the past century and a half—all of which generated internal conflicts.

It is likely that such organizational "disorder," to use Morison's term, could accompany the large-scale introduction of unmanned aircraft as well. Indeed, a key conclusion of Stephen Rosen's case studies of military innovation is that because cultural change within the military is so difficult, any major peacetime innovation requires a full generation to complete—enough time for a new cadre of junior officers practicing the new techniques to rise to positions of leadership.[5]

It is the mass of officer practitioners—those below flag level—who must actually adopt and supervise the operation of new systems. They will be the combat users of the new systems, and some will become the future senior leaders of their Services. The common wisdom is that military aviators identify themselves so strongly with manned aviation that they are unlikely to embrace this technological trend. Indeed, some believe that officer pilots today, just like cavalry officers on the eve of ground force mechanization, could actually impede an objective evaluation of the UAV and introduce unwarranted delays into its operational employment. Despite the potential importance of the broad officer corps to major innovation, there has been exceedingly little empirical information regarding attitudes and actions of these individuals in promoting or impeding major change.

In early 2006, to shed some light on the issue of cultural or social impediments to military-technical innovation, we surveyed nearly 400 officers with aviation specialties who were attending intermediate and senior professional military education institutions.[6] These schools provided not only a readily accessible survey population but also a body of officers identified by their own Services as having the best prospects for advancement and leadership within the Armed Forces. These are the officers who are most likely to have control over the future acquisition and operational employment of new technologies, such as unmanned systems.

This survey was intended to probe personal issues associated with the career and culture of aviation—such as career choice, professional risk, personal danger, and various aspects of the flying ethos. The goal was to enrich our collective knowledge of what motivates individual officers in order to determine their receptivity to major institutional change within their own professional specialties during the course of their careers. There was no attempt to evaluate the wisdom of the transition from manned aircraft to UAVs (although an underlying assumption was that these systems appear to have increasing utility). Rather, the intent was to discern how the current practitioners and future leaders of the U.S. military assess the impact of that transition on both themselves and their chosen profession. The immediate intent was to provide useful insights to those seeking to promote the introduction of UAVs and other innovative technologies. Although the survey might accurately reflect current thinking within the officer corps with respect to UAVs, the extent to which these attitudes might manifest themselves in active opposition to change—either through the creation of impediments to the adoption of new systems or simply through neglect to pursue them—might be known with certainty only from a future, retrospective analysis of how these systems fared within the various Services and Service branches. In that respect, this data will ideally serve to inform analysts of innovation some 10 or 20 years in the future.

Our survey showed aviators had attitudes that diverged markedly from popular stereotypes. Contrary to the common wisdom, we found that most aviation officers had little or no expectation of detrimental career impact from the increasing use of unmanned systems. Most aviators appeared to be motivated primarily by professional advancement rather than flying, supporting the notion that a secure career path for promotion and command would be an inducement to attract officers into emerging fields such as unmanned system control. Also contrary to the conventional wisdom, senior officer responses reflected more positive views of both the expectation of the introduction of unmanned systems and the overall impact of unmanned systems on military operations and the military

it is the mass of officer practitioners who will be the combat users of the new systems, and some will become the senior leaders of their Services

Navy RQ–8A vertical takeoff and landing UAV is demonstrated

U.S. Navy (Daniel McLain)

Hunter Joint Tactical UAV is used in training exercise

U.S. Air Force (Reynaldo Ramon)

Services than did junior officers. If there was an identifiable "seam of rejection" of autonomous operations, it was in the area of preprogrammed computer "decisionmaking" in determining how and where to employ lethal force.

Expectation of Change

One of the most fundamental questions has to do with aviators' expectations of future change. Do they expect manned aircraft to be as useful in future years as they are today, or do they believe that UAVs will be increasingly useful? Past survey results have been mixed. In an earlier survey in 2000, for example, we found that 58 percent of all officers canvassed held that manned aircraft would be as important in 2020 as they were at the time. Conversely, 46 percent responded that within the next 20 years, uninhabited combat aerial vehicles would become the predominant means of conducting strike warfare.[7]

Our 2006 survey revealed that most officers believed that although UAVs will play an increasing role, they are unlikely to displace manned aircraft completely in any but limited specialties. Not surprisingly, two-thirds of all officers surveyed believed that during their military careers, UAVs would be operationally fielded in such a way that they would perform at least some of the functions that their aircraft currently perform. Senior officers (the term applied to officers O–5 and above in this survey) were in slightly more agreement than junior officers (O–4 and below), with 69 percent of senior and 66 percent of junior officers in agreement. However, only 24 percent of officers who believed that UAVs would perform at least some of the functions that their aircraft performed held that UAVs would outnumber manned aircraft in their specialties. As might be expected, given the increasing prevalence of UAVs for surveillance missions, aviators from intelligence, surveillance, and reconnaissance aircraft (E–3, RC–135, EP–3, and U–2) were more inclined to believe that UAVs would outnumber manned aircraft in their specialties.

Importance of Officer Support

As both Eliot Cohen and Adam Grissom have noted, the existing literature on innovation focuses on the top-down direction of senior civilians and military officers; the phenomenon of bottom-up innovation by mid-grade officers has received less study.[8] Although there is anecdotal evidence from historical case studies that officer-practitioners can be important to the introduction of new innovations, the question of whether broad officer support is critical to success is far from clear. What is clear from our survey is that most officers believed major innovation was unlikely to succeed without the active support of mid-grade officers in the field.[9] Two-thirds of all respondents felt that mid-grade officers are critical to the success of major innovations. It should also be noted that nearly one in four did not believe that mid-grade officer support was critical to innovation. Whereas only 50 percent of Army officers believed that mid-grade officer support was important, 66 percent of Navy, 66 percent of Marine Corps, and 69 percent of Air Force officers believed it was.

Flying as a Career Choice

Officer support for the widespread introduction of UAVs is presumably related to the value that the officer attaches to flying. To the extent that aviators value flying, they may resist the introduction of UAVs. As a result, we attempted to explore the personal importance of flying relative to other career choices. Somewhat surprisingly, only 35 percent of aviators responded that they would not have joined the military had they not been able to fly. This suggests that most current aviators were attracted to military service by things other than flying. More predictably, given the centrality of manned flight to the identity of the Air Force, 41 percent of Air Force junior officers responded that they would not have

joined the military if they had not been able to fly. By contrast, only 30 percent of Navy, 19 percent of Marine Corps, and 13 percent of Army aviators gave the same response.

We similarly found that very large percentages of both junior and senior officers would likely complete a full military career even if they could no longer fly. As might be expected, senior officers, who are much closer to retirement and beyond their prime flying days, expressed a stronger likelihood of staying in the military in a nonflying role. Only 10 percent of senior officers responded that they would leave the military before mandatory retirement if they could no longer fly an aircraft. More surprising is the fact that only 19 percent of junior officers (including zero percent for the Army) indicated that they would leave the military if they could no longer fly.

Thirty percent of all officers, and 34 percent of junior officers, indicated that they would choose to transition to flying UAVs rather than leave the military. As might be expected, more than 8 in 10 senior officers indicated that they would fly UAVs rather than leave the military.

most officers believed that although UAVs will play an increasing role, they are unlikely to displace manned aircraft completely in any but limited specialties

One of the frequently used arguments for UAVs is that they will free aviators from performing missions that are "dirty, dull, or dangerous." As a result, we sought to determine how willing aviators would be to hand over "dull" or tedious missions to UAVs.[10] We found that declining tolerance for dull flying missions was somewhat predictably pegged to seniority—with 60 percent of senior officers but only 43 percent of junior officers responding that they would prefer to have a UAV fly a mission that they deemed tedious. This suggests a diminishing allure of flight as pilots accumulate more hours in the air—and likely a greater receptivity to handing those missions over to UAVs.

We also sought to determine the importance of flying relative to command and promotion. Senior officers, whose primary flying days are behind them, opted

Soldiers assemble Raven UAV for short-range reconnaissance

1st Combat Camera Squadron (Russell Cooley)

for command or promotion over flying: 85 percent of senior officers chose command over flying, and 80 percent chose promotion over flying. But more than half of all junior officers in the Army, Navy, and Marine Corps—and nearly half in the Air Force—also opted for command and promotion over flying. This result is quite revealing and indicates that most officers are motivated by incentives that can be accommodated even with the transition to unmanned vehicles. It also supports Rosen's conclusion that a secure career path—that is, an institutionalized opportunity for promotion and command—is a key incentive for drawing junior officers into new operational specialties. This might be especially important if the new technologies or systems do not offer a significant personal thrill or other allure like flying.

Professional Risk from UAVs

The widespread introduction of UAVs poses several potential professional risks for aviators. A reduction in the number of pilots could lead to diminished opportunities for promotion and command among currently serving officers as well as a loss in organizational influence by aviators—including the power to select the Service's future leaders. We nonetheless found that more than 70 percent of all respondents did not expect the increasing introduction of UAVs in their specialties to reduce their personal prospects for promotion. Senior officers (presumably with flying-related promotion criteria behind them) saw less impact than junior officers. It is also noteworthy that Air Force junior officers had the highest expectation of reduction in promotion opportunity from UAVs compared with other junior officer aviators, but still, only 18 percent reflected much concern.

Similarly large majorities did not expect their personal prospects for command to decline with the increasing introduction of UAVs in their specialties. Again, senior officers predicted less impact than junior officers (presumably because most command opportunities were behind them). Air Force junior officers had the highest expectation of reduction in command opportunity, but only 21 percent were concerned.

a reduction in the number of pilots could lead to diminished opportunities for promotion and command among serving officers

The Flying Ethos

The large-scale introduction of UAVs will change not only the career prospects of aviators but also the ethos of flying. There are undoubtedly many reasons why individuals join and make a career out of an innately risky profession such as military aviation. Many are likely attracted by the physical and mental challenges of controlling a high performance aircraft in combat—including the social exclusivity of being a highly trained aircraft commander. Many aviators likely identify with the organizational "ethos," or set of peculiar cultural values, inherent in military aviation squadrons. It is possible that unmanned systems might introduce unacceptable changes to some of the more esoteric aspects of the ethos that personnel find most appealing. The increasing use of unmanned systems will likely alter traditional features of combat—including some aspects of combat leadership. Greater use of autonomous systems for weapons employment could alter the traditional sense of authority and responsibility for assessing risk and applying lethal force—with all of the implications arising from the possibility of fratricide and collateral civilian casualties. UAVs will likely also reduce the experience of personal risk or danger, with diminished opportunities for battlefield valor. Recruiting and retention could be affected by those who fear, as did an early crew member of the USS *Monitor*, that "there isn't enough danger to give us glory."[11] For Air Force pilots, there

U.S. Air Force (Suzanne Jenkins)

Officer and Airman jointly operate Predator RQ–1 at Tallil Air Base, Iraq

is the added issue of maintaining control of their own Service.

Personal Risk. There would have been no military aircraft, tanks, or submarines if large numbers of officers had not been willing to take on the inherent personal risk of actually climbing into and operating those early crude machines of often dubious safety. Our survey sought to determine the willingness of officers to hand over to UAVs missions that they personally deemed dangerous.[12] Specifically, we asked whether officers would rather have a UAV fly a mission that they deemed "high risk" than to fly that mission themselves. Fifty-six percent of officers overall expressed a preference to fly even high-risk missions, suggesting an inherent attraction of risk in manned flight. The issue of willingness to accept risk also showed a marked, and somewhat predictable, difference between junior and senior officers, with 44 percent of senior officers but only 28 percent of junior officers amenable to handing over high-risk missions to unmanned aircraft. There was also a significant difference among the Services—and especially between the ground forces—with 50 percent of the Army aviators willing to cede dangerous missions to UAVs, but only 17 percent of Marines showing a preference to do so. Such a result perhaps reflects the close tie that exists between Marine aviators and ground forces.

Control of UAVs by "Pilots." It is debatable whether UAVs can be operated successfully in the future without control by rated "pilots" having extensive flight experience in manned aircraft. The issue of "stick" handling might be irrelevant if future UAVs are essentially autonomous—responding to preprogrammed algorithms and simple keyboard inputs—and do not require direct flight control. Interestingly, 40 percent of all respondents believed that UAVs should be controlled only by individuals qualified to pilot an aircraft. Moreover, there were significant Service differences on this matter: 11 percent of Marine officers, 15 percent of Army officers, and 33 percent of Navy officers—but 51 percent of Air Force officers—expressed the belief that only pilots should control UAVs. At least part of the explanation is likely that Air Force UAVs tend to be much larger than those in use by the other Services, with support and control requirements relating more closely to manned aircraft. Current practice in the Air Force, but not in the other Services, is that UAV operators be rated aviators. There might also be an ingrained cultural proclivity within the Air Force to identify the pilot with the aircraft, or simply widespread belief that trained pilots are likely critical to the success of any type of major aviation program.

Control of UAVs by "Officers." Enlisted military pilots were not uncommon through World War II, primarily due to a need for rapid expansion of the pilot ranks. Since then, aircraft pilots in the U.S. military have been almost exclusively commissioned or warrant officers. Whether this is primarily a cultural issue ("pilot" and "officer" being seen as synonymous) or a question of command authority and individual responsibility is unknown. In looking to the future, we sought to determine whether officers felt that UAVs should be flown or controlled only by commissioned or warrant officers. What we found was a significant split. Whereas 36 percent of senior officers felt that only officers should control UAVs, 49 percent of junior officers did. The reason for the senior-junior split is not known, but junior officers might fear reduced opportunities for promotion and command if control of UAVs were widely opened to enlisted personnel. The Air Force divergence from the other Services is also noteworthy. Whereas 55 percent of Air Force officers believed that only officers should control UAVs, 49 percent of Navy, 10 percent of Army, and 9 percent of Marine aviators felt the same way. As noted above, current Air Force UAVs are much larger than those in use by the other Services, and they are operated by commissioned officers. But the responses also beg the question of whether most Air Force aviators culturally equate the pilot to an officer, or whether there are issues of command authority and responsibility that drove this response.

UAV Operators as Warfighters. We also sought to determine whether aviators considered UAV operators to be "warfighters." We found that 74 percent of officers overall agreed with the statement "UAV operators are warfighters." Perhaps counterintuitively, more seniors (83 percent) than juniors (71 percent) agreed with this statement, suggesting a different notion of "warfighter" between the age groups.

UAVs and Individual Valor. The Distinguished Flying Cross (DFC) is awarded to an individual who "distinguishes himself by heroism or extraordinary achievement while participating in an aerial flight." The award is generally assumed to involve both risk to and achievement by an individual while airborne. We sought to determine whether officers believed that a UAV operator could someday be recognized with the DFC for an extraordinary combat achievement while, presumably, not being airborne and under no personal risk. Very large majorities—and notably, a far higher percentage of seniors than juniors— rejected this notion. There was also little uncertainty on this issue, suggesting the deeply held opinion that at least for some level of personal awards, human risk should always be a distinguishing criterion. Nevertheless, 15 percent of respondents overall, and 22 percent of Air Force respondents in particular, expressed some measure of agreement with the statement. It must be emphasized that responses do not necessarily signify agreement with the idea of awarding a DFC to a UAV operator, but simply the expectation that it will happen. This particular statement elicited a number of written comments—all critical—and reflected something of the visceral emotion of combat valor. One respondent termed the question itself "incredibly disturbing." Another suggested the creation of a new type of award to recognize the combat achievements of UAV operators.

it is current practice in the Air Force, but not the other Services, that UAV operators are rated aviators

Autonomous Control of Lethal Force. A major argument for more autonomy in UAV systems is to reduce the vulnerability of UAV data links to interdiction by enemy action. As one survey respondent commented, "The moment an adversary learns to jam the command/control link of UAVs, we're in trouble." Yet 59 percent of all respondents rejected the prospect of autonomous application of lethal force, agreeing that enemy targets should be engaged with lethal force only by systems that allow direct human intervention or control. This is an interesting result. Although U.S. doctrine has been migrating away from indirect area fires—including harassment and interdiction artillery fire and aerial bombardment—launching

lethal ordnance at a distant geographic position where enemy forces are expected to be located has become common practice. Presumably, most officers accept the use of global positioning system–guided ordnance such as cruise missiles and the Joint Direct Attack Munition, suggesting that there is some level of autonomous control they do not find unsettling. One can speculate that this relates to autonomous target identification by the system on the scene as opposed to human input of target data. Interestingly, the concept of lethal force without direct human intervention or control was rejected by a higher percentage of junior than senior officers. The Service breakout is also noteworthy, with only slightly more than one-third of Army respondents agreeing with this statement.

most officers see a continuing need for individual humans to monitor, evaluate, and approve all lethal force "decisions" by autonomous platforms

Confidence in Assessments

We sought to understand officers' knowledge of their Service branch plans for the introduction of UAVs. Senior officers expressed far more confidence in their knowledge than junior officers, with 65 percent of senior officers and 59 percent of junior officers assessing that they were adequately informed to make substantive decisions with respect to the introduction or use of UAVs in their specialties. This might be expected since senior officers generally have held positions that are closer to such program details and decisions. This also might explain why seniors appear to be more open to UAVs, and the impact of UAVs, in many of the earlier statements.

We also asked officers to assess the adequacy of their superiors' knowledge to make substantive decisions with respect to the introduction of UAVs. Fifty-five percent of all officers expressed confidence in their superiors. The Service breakout is interesting, with majorities of Army, Air Force, and Marine Corps aviators, but fewer than half of Navy respondents, expressing such confidence in their superiors. In contrast to the other Services, most Army respondents expressed more confidence in their superiors' judgment than their own.

Finally, very large percentages of officers believed that the pace at which UAVs were being introduced was "about right" (see table). Interestingly, a much higher percentage of seniors than juniors believed that the pace was "not fast enough"—and a higher percentage of junior officers felt that the pace was "too fast." One interpretation could be that junior officers are not as "forward thinking" as senior officers, or not as knowledgeable of UAVs. Another interpretation could be that junior officers have more legitimate concerns about the pace of UAV introduction at the tactical level given the current state of technology.

Summary

One survey respondent reflected the popular view of aviators toward UAVs when he commented, "God willing, there will never be a time when UAVs take over the job of a qualified and competent fighter pilot." Yet in his exhaustive study of the history of UAVs in the U.S. military through the late 1990s, Thomas Ehrhard found "no parochial, pilot resistance standing in the way of UAV development in the Air Force, only a general enthusiasm for UAVs that in retrospect was not supported by the technology of the time."[13]

Our survey corroborates Ehrhard's conclusion, revealing no widespread or deep-seated opposition to UAVs beyond technological uncertainty. We found that, in general, aviators did not believe that they would see the large-scale displacement of manned aircraft by UAVs in their own specialties during the remainder of their careers. Thus, most saw no detrimental career impact from the ongoing introduction of UAVs. Most aviators also expressed a willingness to pursue their military careers even if displaced by UAVs. For the majority of officers, military service itself, rather than flying, appeared to be the primary career motivator. Most aviators indicated that they would select promotion or command if forced to choose either of those over flying. This tends to support the theory that the establishment of a secure career path will motivate a large percentage of officers to enter new career fields with different types of systems and skills.

We also found that in most areas, senior officers showed more receptivity to UAVs and changes wrought by UAVs than did junior officers—even in those cases where future career impact did not appear to be a factor. In particular, senior officers were more open to what might be considered cultural change to the "institution" of flying, including UAV control by nonpilots, UAV control by enlisted personnel, and consideration of UAV operators as warfighters. More senior officers than junior officers also believed that UAVs were not being introduced fast enough. These responses tend to refute the stereotypical notion of conservative senior officers squelching the innovative ferment within the junior officer ranks.

In general, Air Force aviators showed more traditionalism than did officers in the other Services with respect to UAVs, with substantial percentages opposing UAV control by individuals other than officer pilots. However, it is not evident from the survey data that this opposition is rooted in culture rather than issues arising from command authority and responsibility. Moreover, this would reflect a more informed view if Ehrhard is right in his observation that a pilot-centric "aviation

The Pace at Which UAVs Are Being Introduced into My Specialty Is . . .

	Not Fast Enough (percent)	About Right (percent)	Too Fast (percent)
All Officers	18	71	11
O–4 and Below	15	72	13
O–5 and Above	26	68	6
Army	20	70	10
Navy	22	73	5
Air Force	17	68	15
Marine Corps	15	83	2

discipline" might be critical to successful UAV operations.

If there is a seam of rejection, it would appear to lie in the degree of autonomy afforded to UAVs. With the notable exception of the Army, large majorities of aviators hold to the view that enemy targets should not be engaged with lethal force by systems without direct human intervention or control, thus seeming to reject fully autonomous systems that search for, identify, track, target, and destroy enemy targets.[14] The implication is that officers will likely insist on direct communications with unmanned systems for the application of lethal force at least against mobile or relocatable targets—with the resulting provision for secure communications pathways between the system and the human controller regardless of distance or enemy actions. Most officers see a continuing need for individual humans to monitor, evaluate, and approve all lethal force "decisions" by perhaps large numbers of autonomous platforms. Future developments will determine whether the pace of high-intensity combat operations, and possible enemy use of autonomous systems without a human in the loop, will force U.S. military officers to accommodate more autonomy in the application of lethal force.

The lack of evidence of outright rejection of UAVs may stem, as Ehrhard suggests, from the creeping automation that has occurred in manned flight over the past decade or so—both in precision-guided munitions and flight controls.[15] The average Navy strike-fighter pilot now accepts the fact that he must have his hand off the stick controls of his F/A–18 in order for it to launch from a carrier deck. Thus, the distinction between the manned aircraft and UAV is gradually diminishing even for the pilot in the cockpit. Another factor in UAV acceptance might be that the most significant large UAV program, Predator, has been flown and managed by rated pilots in the Air Force who cycle between manned and unmanned platforms. Aviators with higher career aspirations (as most seem to have), therefore, might be just as likely to seek excellence in UAV operations as manned aircraft operations. Manned aviation also has significant "ownership"—and likely pride in that ownership—of the growing Predator fleet. As the Air Force transitions to a dedicated UAV training and operational career path, it will be interesting to see whether segregating the officer corps into manned and unmanned operators will kindle career and cultural competition that impedes UAV development and integration.

Whether or not the preferences expressed in this survey will accurately reflect officer actions in response to the growing numbers of increasingly autonomous systems remains to be seen. Perhaps institutionally based opposition will emerge when major organizational and professional changes wrought by growing numbers of unmanned systems actually begin to ripple through the Services. A retrospective analysis of the transition from manned to unmanned flight will be needed over the coming decades to determine whether institutional factors actually played any role in impeding technological innovation. **JFQ**

NOTES

[1] Joint Publication 1–02, *Department of Defense Dictionary of Military and Associated Terms* (Washington, DC: The Joint Staff, April 12, 2001), defines UAV as "A powered, aerial vehicle that does not carry a human operator, uses aerodynamic forces to provide vehicle lift, can fly autonomously or be piloted remotely, can be expendable or recoverable, and can carry a lethal or non-lethal payload. Ballistic or semi-ballistic vehicles, cruise missiles, and artillery projectiles are not considered unmanned aerial vehicles." The term *unmanned aircraft system* (UAS) is now used by the Defense Department in place of UAV to emphasize that the aircraft vehicle is only one component of the system, and due to the fact that the Federal Aviation Administration uses the term *UAV* to designate specific types of UAS falling under regulatory control.

[2] Office of the Secretary of Defense, *Unmanned Aircraft Systems Roadmap 2005–2030* (Washington, DC: Office of the Secretary of Defense, August 4, 2005), 26–37.

[3] See Thomas Paul Ehrhard, "Unmanned Aerial Vehicles in the United States Armed Services: A Comparative Study of Weapon System Innovation" (Ph.D. diss., The Johns Hopkins University, June 2000).

[4] Elting E. Morison, *Men, Machines, and Modern Times* (Cambridge: The Massachusetts Institute of Technology Press, 1966), 34.

[5] Stephen P. Rosen, *Winning the Next War: Innovation and the Modern Military* (Ithaca: Cornell University Press, 1991).

[6] The professional military education institutions surveyed comprised the U.S. Naval War College, U.S. Army War College, Air War College, Air Command and Staff College, National War College, Industrial College of the Armed Forces, Marine Corps War College, Army Command and General Staff College, Air Command and Staff College, Marine Corps Command and Staff College, School of Advanced Air Power Studies, School of Advanced Warfighting, Air Force Squadron Officers School, and Expeditionary Warfare School. Respondents had the following officer specialty codes: Army (15X/Aviation), Navy (131X/Pilot and 132X/Naval Flight Officer), Air Force (11XX/Pilot and 12XX/Navigator), and Marine Corps (75/Pilot/Naval Flight Officer).

[7] Thomas G. Mahnken and James R. FitzSimonds, *The Limits of Transformation: Officer Attitudes toward the Revolution in Military Affairs*, Newport Paper 17 (Newport, RI: Naval War College Press, 2003), 30–33. See also Thomas G. Mahnken and James R. FitzSimonds, "Revolutionary Ambivalence: Understanding Officer Attitudes toward Transformation," *International Security* 28, no. 2 (Fall 2003).

[8] See Eliot A. Cohen, "Change and Transformation in Military Affairs," *Journal of Strategic Studies* 27, no. 3 (September 2004), 395–407; and Adam Grissom, "The Future of Military Innovation Studies," *Journal of Strategic Studies* 29, no. 5 (October 2006).

[9] The term *mid-grade* was not further defined in the survey.

[10] The term *tedious* was not further defined and is likely to be highly individual. For the purposes of this statement, it was deemed sufficient for the respondent to consider his or her own definition of a tedious mission. Officers were asked to provide percentages of overall flight hours that they deemed tedious. Most felt that the majority of their flight hours were not tedious. As might be expected, senior officers tended to assess a higher percentage of their own flight hours as tedious than did junior officers.

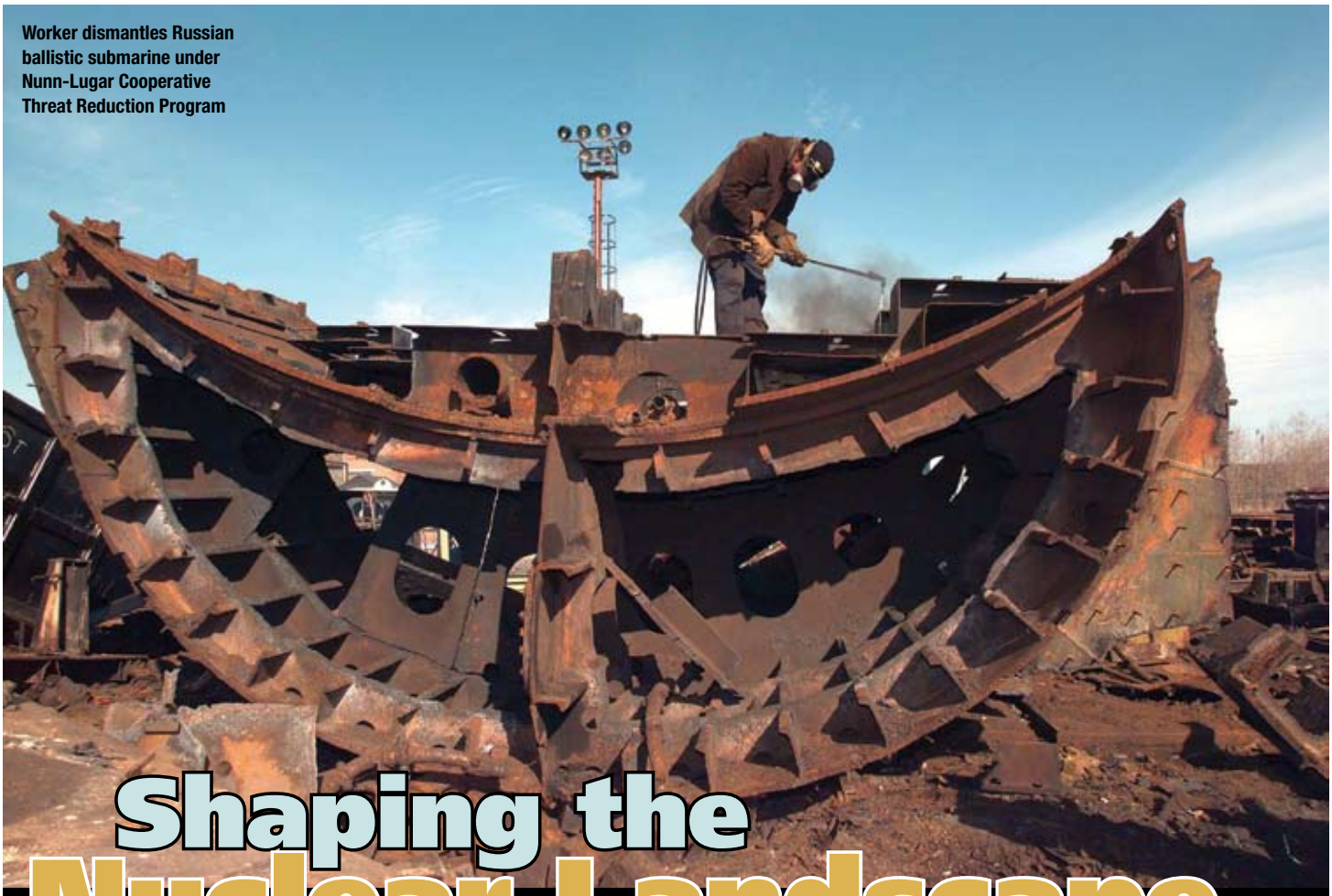
[11] This was the question posed by William Frederick Keeler when assigned as the first paymaster of the USS *Monitor*. Subsequent action confirmed that there was still abundant danger—and opportunity for glory—even in an armored ship. See David A. Mindell, *War, Technology, and Experience aboard the USS* Monitor (Baltimore: The Johns Hopkins University Press, 2000), 2.

[12] The term *high risk* was not further defined and is likely to be highly individual. For the purposes of this statement, it was deemed sufficient for the respondent to consider his or her own definition of a high-risk mission.

[13] Ehrhard, 493.

[14] The Low Cost Autonomous Attack System (LOCAAS) developed and tested by Lockheed-Martin was just such a system. It was rejected by the Air Force due, among other things, to the lack of a man-in-the-loop to control the attack. The basic LOCAAS technology has since been resurrected in other strike systems that provide for human intervention in the attack process.

[15] Ehrhard, 625.



Worker dismantles Russian ballistic submarine under Nunn-Lugar Cooperative Threat Reduction Program

U.S. Navy

Shaping the Nuclear Landscape

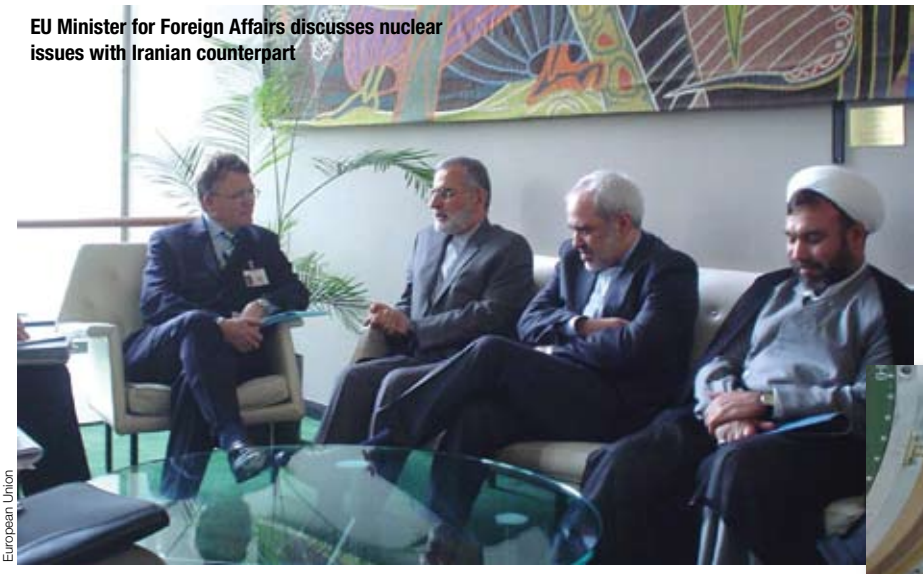
By PAUL I. BERNSTEIN, JOHN P. CAVES, JR., *and* JOHN F. REICHART

In important ways, the world is at a nuclear crossroads. The complex and dynamic nuclear landscape presents us with challenges along at least four axes: regional nuclear proliferation, nuclear terrorism, great power nuclear relations, and the security implications of increased interest in nuclear energy. These problems are interrelated in ways that the national security community does not fully understand. Strategy and policy frameworks do not address them in sufficiently integrated fashion. New conceptual thinking is required to develop a more unified understanding of and approach to managing the risks and opportunities posed by these 21st-century nuclear challenges.

Today, more than at any other time in the nuclear era, nuclear capacity and potential (knowledge, technology, and materials) are accessible to a growing number of actors with more ambitious goals. The result is a high degree of nuclear latency that challenges traditional thinking about nuclear threats. Whereas 30 or 40 years ago, only a handful of countries were assumed to know how to acquire nuclear weapons, as many as 35 or 40 nations currently are believed to be in the know, and many more could become so based on their participation in civilian nuclear energy programs.[1]

In a world characterized by high nuclear latency, a number of risks stand out. One is simply that there may be multiple ways for states to be considered nuclear-capable. While robust nuclear weapons programs remain the most serious proliferation danger, a range of possibilities below this threshold or level of capability must be of concern as well. So must be models of weapons development enabled by technologies and processes that might be easier to conceal and harder to detect (for example, laser enrichment). A nuclear-latent world also challenges our thinking about warning, suggesting the possibility of a significant mismatch between lead times and reaction times. Finally, careful attention must be paid to the catalytic or transformative events that could push a latent nuclear actor toward a more active or accelerated posture. Japan often is cited as a possibility in this regard, but also of concern are so-called rollback states that could, with varying degrees of ease,

Paul I. Bernstein is a Vice President with Science Applications International Corporation. John P. Caves, Jr., is a Senior Research Fellow in the Center for the Study of Weapons of Mass Destruction (WMD Center) at the National Defense University (NDU). John F. Reichart is Director of the WMD Center at NDU. This article is adapted from *The Future Nuclear Landscape* (NDU Press, 2007).



EU Minister for Foreign Affairs discusses nuclear issues with Iranian counterpart

European Union

attention needs to be paid to the events that could push a latent nuclear actor toward a more active posture

SS–18 ICBM slated for elimination under Nunn-Lugar Cooperative Threat Reduction Program

Office of Senator Richard Lugar

reconstitute their nuclear weapons programs in response to changed conditions.

These considerations have significant implications for political and technical intelligence, not least of which is the need for a sharper focus on intentions. More broadly, there needs to be a way to measure latency that is meaningful to decisionmakers and planners. Metrics may be qualitative and/or quantitative and should strive to enable policies that can influence both intentions (through incentives) and capabilities (through barriers).

Pressures Against Cooperation

The latency challenge will grow as more states gain access to either basic or more advanced levels of nuclear technology. Consider the countries that recently have expressed interest in or intent to initiate or expand nuclear energy activities, including in some cases developing an indigenous capability to enrich uranium: Algeria, Argentina, Australia, Brazil, Bulgaria, Canada, Egypt, the Gulf Cooperation Council states, Indonesia, Jordan, Kazakhstan, Morocco, South Africa, Tunisia, Turkey, Ukraine, Venezuela, and Yemen. Driving these decisions is a dynamic mix of motivations shaped by security, energy, and science. Anxiety about North Korea and Iran likely is fueling proliferation pressures in East Asia and the Middle East as threat perceptions evolve and concerns grow about the fraying of the international nonproliferation regime. Others may look at these cases and conclude that possessing or seeking nuclear weapons results in enhanced leverage and influence. Energy security is an increasingly salient factor in the appeal of nuclear technology, given the economics of oil and what may become growing pressures to find alternatives to fossil fuels in light of global warming. Additionally, many countries associate *nuclear* not just with security or energy, but with modernity as well. That is, access to nuclear science and technology is seen by those who consider themselves behind as a powerful means to join the community of advanced nations.

The problem is not limited to states. Small groups or individuals operating outside traditional political boundaries may be capable of assisting states or terror groups in developing or acquiring nuclear capability. In this sense, the A.Q. Khan clandestine nuclear procurement network—to cite only the most prominent nuclear black market activity—is a concrete manifestation of globalization in the security arena. In the future, we may look back at the Khan phenomenon not as an anomaly but as the harbinger of a period in which literally anything could be bought or sold. Certainly, this is a problem that the framers of the Nuclear Non-Proliferation Treaty (NPT), 40 years ago, could not have anticipated.

It is no surprise, then, that the nuclear nonproliferation regime is under great stress. The regime overall has been effective in containing the spread of nuclear weapons, not least by giving governments confidence that restraint is in their self-interest. But the progress of determined, hostile proliferators poses a major threat to the integrity of the regime and the norms that it embodies. Failure to resolve these challenges and delegitimize various models of creeping proliferation could lead to a broad-based loss of faith in the regime and its effectiveness as a security alternative to possessing nuclear weapons. Increasing global energy demand is a complicating factor not only because nuclear energy is becoming more appealing but also because of the geopolitics of oil. In a time of higher oil prices, it will be difficult to impose the type of hard sanctions that may be necessary to induce states such as Iran—a major oil exporter that also has the capability to interfere with other exporters' oil shipments—to limit their nuclear ambitions. China's rapidly growing need for imported energy is of particular concern here, as Beijing seeks to establish strategic relationships with major oil exporters such as Iran.

Indeed, it is not possible to separate regional nuclear proliferation challenges fully from the dynamics of great power strategic relations. While the United States has been highly proactive in developing innovative approaches to the weapons of mass destruction (WMD) problem, it needs the help of Russia and China to work the hardest cases, such as North Korea and Iran. Washington, Moscow, and Beijing clearly have some common interest in managing these problems, but there are also pressures working against cooperation, including differing assessments of the importance and urgency of these regional proliferation challenges and uncertainty in each capital about where the others are headed in terms of nuclear and other strategic force capabilities. Strategic dialogue to address these uncertainties and forge a more common perspective on the nuclear

future may make it easier to bridge some of the differences evident in addressing the WMD challenge. Exploring linkages across these dimensions of security may yield new opportunities for great power cooperation.

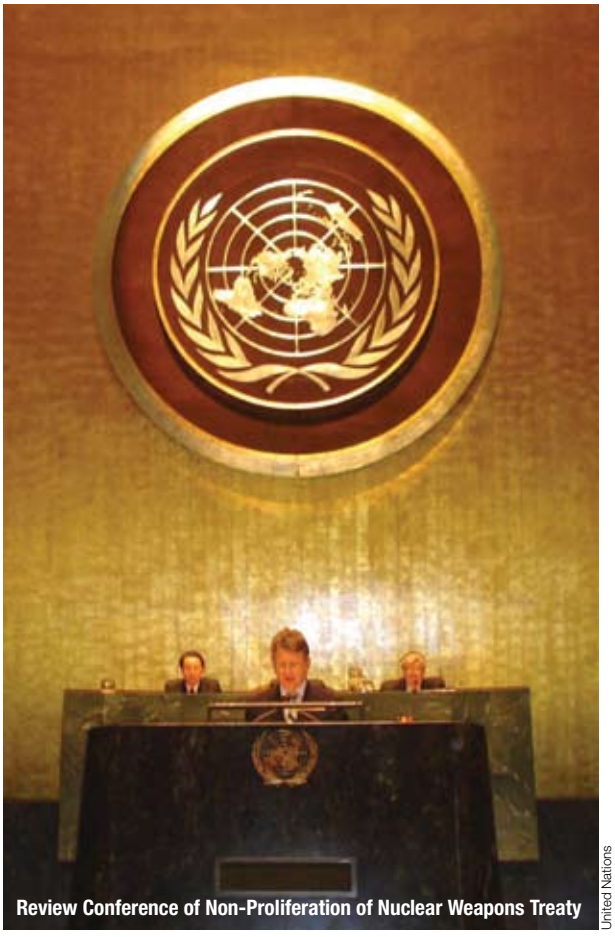
The Major Challenges

Impact of the Iraq War on U.S. Nonproliferation Efforts. Many governments feel alienated from Washington because the public rationale for the Iraq war is widely viewed as either illegitimate or based on a massive intelligence failure. The damage to American credibility has been serious, making it more difficult to marshal others to confront new proliferation threats vigorously (or support U.S. objectives more broadly).

Forging a common approach to Iran within a coalition that divided bitterly over Iraq has compelled the United States to make significant adjustments to its strategy. The war also has deepened political divisions at home, making the search for bipartisan approaches more difficult. These domestic political constraints and the strain on U.S. forces resulting from the war are recognized by Iran and North Korea, whose leaderships may now see the United States as less willing or able to pursue coercive strategies that implicitly or explicitly threaten military action in response to their proliferation activities. As a result, these countries may be emboldened to resist international pressure to dismantle their nuclear programs or capabilities.

Moscow and Beijing care about containing the spread of nuclear weapons, just not as intensely as does Washington

Limited Help from Russia and China. Moscow and Beijing care about containing the spread of nuclear weapons, just not as deeply or intensely as does Washington. While Russia and China do not wish to see unchecked proliferation, neither are they prepared to make major political or economic sacrifices to support a nonproliferation agenda that is viewed at least by some officials as preserving American advantage. Strategic economic considerations increasingly reinforce this: nuclear technology is one of the few technologies that Russia can market competitively, and China's aggressive effort to secure energy sources colors its posture toward proliferation problems, such as that of Iran. Whereas in the past it may have been possible to treat the proliferation problem as a more or less stand-alone issue in great power relations, it is no longer possible to separate it from broader economic, energy, and regional security considerations. Any effort by the United States to forge a more common or cooperative great power approach to managing WMD challenges will require recognizing and addressing Russian and Chinese equities.



Review Conference of Non-Proliferation of Nuclear Weapons Treaty

United Nations

Chinese officials and commentators increasingly suggest that U.S. nonproliferation policy is self-serving and based on double standards. Whereas China is pressed on cases such as Pakistan, Iran, and North Korea, the United States expects others to support preserving the special status of Israel, rewarding India despite its refusal to join the NPT, and accepting the "creeping nuclearization" of Japan. Russia, for its part, has recently issued an official document on nonproliferation policy that accuses the United States of politicizing nonproliferation and opposes key elements of U.S. strategy (although without mentioning the United States).[2] On the other hand, neither country likely would allow differences over proliferation to cause a fundamental breach in their relationships with Washington, and there are cooperative activities that are potentially significant. The ongoing strategic dialogue with China provides an opportunity to seek stronger common ground on countering WMD. Presidents Bush and Vladimir Putin recently launched the Global Initiative to Combat Nuclear Terrorism, designed to expand and accelerate efforts and capacity among like-minded nations to control nuclear materials, stop illicit trafficking, respond to acts of nuclear terror, deny safe haven, and strengthen national legal frameworks.[3]

Gaps in Knowledge and Understanding of Suspect Programs and Activities. Limitations in WMD intelligence are by now a well-studied problem. Even before the serious questions raised by the Iraq war, there were efforts to assess the capabilities of the Intelligence Community with respect to WMD and identify required reforms.[4] The WMD intelligence track record is mixed. There have been major successes (not always publicly acknowledged), and there are recognized oases of excellence in the community with respect to WMD intelligence collection and analysis. There have also been significant failures and chronic dysfunctions stemming from a broad range of organizational, operational, and analytical shortfalls.[5] In the aftermath of Iraq and in the face of continuing uncertainties vis-à-vis the nuclear intentions and capabilities of North Korea, Iran, al Qaeda, and others, it is not surprising to hear the question: Are our intelligence capabilities good enough to understand this threat properly and anticipate the range of challenges that may emerge?

While there is significant room for improvement, it is essential to have realistic expectations. Determined, adaptive proliferators skilled at deception and denial will find ways to conceal at least some of their activities from even a greatly improved WMD intel-

ligence enterprise. To some degree, therefore, uncertainty will always outweigh certainty, and policymakers must accept that there are inherent limits to WMD intelligence. But much can be done to reduce uncertainty and the ambiguity associated with clandestine WMD programs. Emphasis should be placed on minimizing the prospects for significant strategic surprise and providing decisionmakers with more robust and timely actionable intelligence. Reforms to enable this must encompass organization, methodology, and technology. Compensating for inevitable intelligence gaps also requires the military to emphasize a capabilities-based approach to planning and investing.

Organizationally, a fundamental problem has been the lack of aggressive Intelligence Community ownership of all aspects of the combating WMD intelligence mission. Creating the Office of the Director for National Intelligence (ODNI) and a supporting National Counterproliferation Center (NCPC) is intended to remedy this problem. Among the greatest challenges facing the ODNI and NCPC are improving horizontal integration across the WMD Intelligence Community and coordinating collection and analysis efforts around specific high-priority targets.[6] With respect to methodology and technology, new sources and approaches are required that are less well known to adversaries and more tailored to discovering concealed WMD activities. These methods overall must focus more on the earliest stages of the proliferation process, and they require a sharper focus on intentions, people, transactions, and critical nodes, enabled by improved human intelligence, information processing, and exploitation of persistent intrusive sensing technologies.

Cultural and Organizational Obstacles to Effective Responses. Strategy and policy analysts often do not understand science and technology well. Nuclear functionalists tend to lack in-depth regional expertise, while regional or country specialists are not always well versed in strategic force issues (China is a good example). There also is a gap between nuclear analysts and those working on other military issues. These cultural problems both reflect and perpetuate divergent vocabularies and frames of reference, and contribute to stovepipes, turf battles, and weak integration of activities. In the combating WMD arena, stovepiped organizations and processes have been a persistent problem dating back many years. There are signs, however, that the community is moving toward greater unity of effort.

In the last 2 years, the Department of Defense (DOD) has established an organizational and planning framework to define and execute the combating WMD mission. The National Military Strategy to Combat WMD provides an "ends-ways-means" approach to planning, executing, and resourcing to guide the activities of combatant commanders, Services, and support agencies. It defines core military strategic objectives, guiding principles for developing concepts of operations and plans, and eight critical missions for the Armed Forces.[7] The designation of U.S. Strategic Command (USSTRATCOM) as lead command for combating WMD has laid the foundation for a more integrated, synchronized effort across the combatant commands and DOD as a whole to implement this strategy. For the first time, there is a single focal point for the Armed Forces, an important step toward further institutionalizing combating WMD in DOD.

there is a gap between nuclear analysts and those working on other military issues

To execute on a day-to-day basis, the commander, USSTRATCOM, has established the USSTRATCOM Center for Combating WMD, a component-like organization closely linked to the Defense Threat Reduction Agency. The test of these new command and organizational arrangements will be the degree to which they can help regional commands to define, plan and resource for, and execute rigorously all aspects of the combating WMD mission. One key focus today is the development of Concept Plan 8099, the global concept for the combating WMD mission that will provide the planning template for all regional commands. Another is the set of joint concepts and capabilities-based assessments that are being conducted to support the definition of warfighter requirements and enable the USSTRATCOM commander to be an effective advocate in the requirements process.

In the Department of State, the Office of the Under Secretary for Arms Control and International Security has reorganized to align its activities with national combating WMD priorities, to include nuclear detection activities, nuclear information-sharing, consequence management, and the development of country- and region-specific plans that can be synchronized with DOD plans. In the Intelligence Community, the aforementioned National Counterproliferation Center will integrate intelligence, coordinate planning, and conduct strategic operational planning at the national level.

Indicators of greater intra- and interagency cooperation are encouraging, as are signs that the WMD terror threat has brought the counterproliferation and counterterrorism communities closer together. But a strong push is needed to ensure that interagency structures and processes are capable of effectively managing complex contingencies involving WMD from start to finish—from policy formulation to coordination and execution of operations. Policymakers a decade ago recognized that WMD could be a complicating factor in managing complex contingencies.[8] This is no less true today, and indeed has been brought into even sharper relief by intervening events. So the question remains: How can the Government institutionalize a collaborative process to plan, execute, and assess combating WMD activities and operations, utilizing all the tools of statecraft? Especially as the combating WMD playing field becomes more crowded, as the toolkit becomes more diverse and sophisticated, and as multiple national and international efforts become more interdependent, the requirement for timely and effective interagency coordination will only grow. This will require more than refining national strategy and preparing decisions for the President; it must include putting in place mechanisms to create and sustain long-term plans for combating WMD that develop integrated courses of action and enable their execution across multiple agencies, including DOD. This capability, if it can be achieved, will create new opportunities for defeating the threat, in some cases reducing pressures for military action.

Practical steps toward strengthening interagency capabilities for combating WMD include developing an overarching interagency concept of operations; clarifying DOD's relationship to other agencies for both war plan execution and response to domestic events, and the associated requirements for interagency support; creating the capacity for

rapid interagency crisis action planning and mission execution; and increasing capacity in civilian agencies to better support operations.

Progress in Addressing Nuclear Threats

A range of programs is now in place to enhance capabilities to deny terrorists access to WMD materials, technologies, and expertise. These include initiatives that target the spectrum of chemical, biological, radiological, and nuclear threats, such as the Proliferation Security Initiative, and efforts managed by the Department of the Treasury to disrupt terrorist financing. In the nuclear area specifically, additional effort has been focused on a number of important challenges, such as the security of nuclear facilities in Russia, detecting the movement of nuclear or radiological materials, attributing nuclear attacks in the United States, and meeting the consequence management information needs of first responders.

Security of Russian Nuclear Facilities. Terrorists may acquire nuclear capability in a number of ways, including an outright purchase or gift from a nuclear weapons state, or through the theft of materials that could be used to construct a nuclear or radiological weapon. Theft, in fact, is our greatest concern with respect to the security of nuclear facilities in Russia. Efforts to date to improve nuclear security there have been effective: today, 80 percent of the sites where materials are stored have been secured, and current programs are on a pace to complete this process by 2008. There has been some progress as well in instilling a security culture, a best practices approach, and an emphasis on emergency management capabilities.

But there are troubling trends as well. The growing influence of the security services has created obstacles to accessing some sensitive sites, though Russian authorities have said that they will upgrade security at these sites on their own. It is also clear that Russian standards for physical security are less robust than our own. Moreover, a culture of corruption persists in Russia, underscoring the risks associated with the insider threat. Many small-scale incidents demonstrate this, and while it is a problem the Russian military seems to appreciate, it is less clear that officials of the Federal Agency on Atomic Energy have a similar appreciation. Of equal or greater concern are questions about whether the Russian leadership is willing to commit the resources needed to sustain security improvements over time. If they are not, much of the progress that has been made under bilateral threat reduction programs could be at risk.

Nuclear Detection. The U.S. organizational focal point for this mission is the Domestic Nuclear Detection Office (DNDO), which is a jointly staffed national office established to improve capabilities to detect and report unauthorized attempts to import, possess, store, develop, or transport nuclear or radiological material for use against the United States. Managed by the Department of Homeland Security (DHS), the DNDO has formulated a global nuclear detection architecture with multiple geographic layers and multiple opportunities for detection, including materials protection, control, and accountability, overseas border security, port of departure screening, overseas interdiction, Coast Guard inspections, and U.S. border protection. A systematic assessment has been performed of these layers and associated capabilities to encounter, detect, identify, and interdict the threat. Plans to close capability gaps have been put in place.

theft is our greatest concern with respect to the security of nuclear facilities in Russia

Currently, two programs provide the majority of detection assets to foreign ports of departure: the DOE Megaports Initiative and the DHS Container Security Initiative (CSI), which operates at 50 ports worldwide. In 2005, CSI ports processed 73 percent of all containers destined for the United States prior to lading.[9] Secondary screening measures are executed on containers that trigger existing detectors. Future emphasis will be placed on increasing the volume of U.S.-bound cargo scanned for nuclear and radiological material, using both passive detection and automated radiography, and transmitting all collected data to appropriate government authorities. An important R&D thrust is to develop

U.S. Air Force (Isaac Freeman)

Personnel don protective gear for exercise

Department of Homeland Security

Customs and Border Protection agent deploys nuclear detection technology

next-generation passive sensors to enable 100 percent passive coverage of all official ports of entry, with relocatable assets for other locations. There is also substantial investment in handheld and portable systems to support the Border Patrol and Coast Guard, commercial vehicle inspection, expanded surveillance for high-risk cities, and Federal surge capacity.

Nuclear Attribution. Developing a robust forensics and attribution capability for covert nuclear attacks presents major technical, organizational, and policy challenges. The national-level effort in this area, known as the National Technical Nuclear Forensics program, is an interagency activity managed by the Domestic Nuclear Detection Office in the U.S. Department of Homeland Security. Within this national effort, the DOD Defense Threat Reduction Agency has the lead for post-detonation technical nuclear forensics. Such forensics can support a determination of attribution that would also be informed by intelligence and law enforcement findings. An initial operational capability for post-detonation forensics has been achieved for improvised nuclear devices, and government authorities have expressed a high degree of confidence that this mission can be accomplished in a timely way.[10] Attention has now turned to radiological dispersal devices, for which many more potential sources exist.

From a technical standpoint, the forensic requirement is to determine materials and design, and from there identify the source. For the former, capabilities such as robotic technologies and deployable field laboratories are being developed. For the latter, there must be a known source against which to compare debris, and our database of sources needs to be as comprehensive as possible. Whether the goal is to support legal prosecution or to respond politically and militarily to an attack (or both), it is essential to maintain a chain of evidence and to exercise the decision process with decisionmakers. Ultimately, attribution is a political process that will require senior leaders to determine how much and what kind of information to make available to allies, adversaries, the international community, and the public. An effective attribution capability contributes importantly to deterrence.

Nuclear Consequence Management. With the increased concern today about the likelihood of nuclear use, especially by terrorists, greater attention is being paid to the Nation's preparedness to respond to the effects of one or more low-yield nuclear detonations in a major urban area. In a series of workshops, the Center for the Study of Weapons of Mass Destruction (WMD Center) undertook to identify the key questions about such effects that responders would need answered in the immediate aftermath of an event and to determine whether the answers would be available to them in a timely way.

In identifying the key questions that would need to be answered, the WMD Center found that one or more low-yield nuclear detonations in a major U.S. urban area would directly engage to varying degrees almost all U.S. Federal agencies as well as those of affected states, localities, and private sector entities. These entities would turn to U.S. nuclear experts, particularly at the Federal level, to provide fast, accurate, and actionable responses to a large and diverse set of questions about nuclear effects and response. The most important questions that U.S. nuclear experts would be looked upon to field in the immediate aftermath of the detonations would concern:

- impacts on key infrastructure, especially communications, transportation, and power
- government capacity for response, especially the availability of response personnel and medical resources
- who is in charge of the response
- timely guidance on how to respond, especially evacuation versus shelter-in-place, triage, and movement from the hot zone to a clean zone
- rapid delineation of radiation hazard zones, especially their perimeter and variability, and whether responders can safely enter.

In examining the Nation's preparedness to answer those questions in a timely way, it becomes evident that important, actionable gaps exist. Most gaps arise from a failure to communicate existing knowledge effectively about nuclear effects and the most appropriate responses thereto from national sources of expertise to responders at state and local levels. Responders need greater education about nuclear weapons effects and response, especially regarding radiation. National standards for nuclear response need to be established and/or harmonized across all levels of government. Nuclear response standards and guidance need to be made available to responders in readily accessible, field-useable form. Closing some gaps may require new knowledge, which may be obtainable through modeling/simulation, technological research and development, surveys/inventories, and other research.[11]

Improving U.S. preparedness to respond to low-yield nuclear detonations in a major urban area does not necessarily require a new, high-profile government initiative; it should be possible to accomplish via existing Federal interagency and Federal/state/local government information-sharing and cooperation mechanisms. However, it will require sustained, active leadership and oversight by a national entity with the requisite mission and authorities, such as the U.S. Homeland Security Council or Department of Homeland Security.

Adapting Declaratory Policy

Despite significant, even dramatic, changes in U.S. strategy and security policies in response to new concerns about weapons of mass destruction and terrorism, there has been little debate about or innovation in declaratory policy in recent years. Some senior policymakers have suggested that declaratory policy is an underutilized tool in the fight against proliferation and WMD terrorism and requires more systematic thought—and not simply in terms of managing crises or the run-up to conflict, but as an integral element of ongoing efforts to dissuade and deter new kinds of adversaries and reassure allies.

The longstanding U.S. policy of calculated ambiguity has eschewed explicit statements concerning how the United States would respond to WMD attacks in order to avoid both limiting the President's freedom of action and placing too high a value on nuclear weapons as an instrument of policy. The benefits and risks of this declaratory posture are well understood; less clear is whether new security concerns argue for adaptations or changes to declaratory policy. Alternative policies would either make the threat of nuclear response more explicit, or eliminate it entirely through some type of no-first-use pledge.

New concerns about the spread of nuclear capabilities raise new challenges for

greater attention is being paid to the Nation's preparedness to respond to the effects of one or more low-yield detonations in a major urban area

declaratory policy. To what degree, and how, should U.S. declaratory policy address the possible transfer by a state of nuclear capabilities to hostile third parties (states or terror groups)? One could argue that developments in this arena, including documented terrorist interest in nuclear weapons and the extensive covert nuclear procurement network operated by A.Q. Khan, point to gaps in declaratory policy that should be filled as part of a comprehensive combating WMD strategy that also emphasizes prevention and interdiction. Declaratory policy can help reinforce the risks associated with nuclear transfers, in part by indicating some of the specific consequences that would follow exposure of such activities. This is an area where nonnuclear responses are likely to figure prominently and where focused concept development should be undertaken.

As the technical means to attribute nuclear attacks improve, policymakers will need to decide how to communicate this capability to potential adversaries in order to maximize its deterrent value. In doing so, it will be essential to strike a balance between conveying a credible capability to identify the source of an attack and protecting intelligence and scientific techniques which, if known to adversaries, could provide the means to complicate the process of forensic investigation and possibly escape attribution.

Finally, it is worth asking whether the anticipated maturation of nonnuclear capabilities as part of the New Triad raises issues or new requirements with respect to declaratory policy. In particular, as missile defenses and conventional strike systems (both kinetic and nonkinetic) become more advanced and assume a more prominent role as strategic-level force assets, there may be value in crafting some specific messages regarding these capabilities (including their relationship to nuclear forces) for the consumption of both allies and adversaries. **JFQ**

NOTES

[1] Mohamed ElBaradei, "Towards a Safer World," *The Economist*, October 16, 2003.

[2] See Nikolai Sokov and Leonard S. Spector, "Russian Government White Paper on WMD Nonproliferation Reveals Both Differences and Similarities with U.S. Approach," *WMD Insights*, issue 8 (September 2006), available at <www.wmdinsights.com/PDF/FP_SeptIssue.pdf>. On the positive side, the white paper endorses the Proliferation Security Initiative and acknowledges the contribution of the United States (among others) in enhancing WMD security in Russia.

[3] "The Global Initiative to Combat Nuclear Terrorism," Fact Sheet, Office of the Press Secretary, The White House, July 15, 2006; and "U.S.-Russia Joint Fact Sheet on the Global Initiative To Combat Nuclear Terrorism," Office of the Spokesman, Department of State, July 15, 2006.

[4] These include the Commission to Assess the Organization of the Federal Government to Combat the Proliferation of Weapons of Mass Destruction (the Deutch-Specter Commission) of 1999 as well as multiple internal Intelligence Community reviews.

[5] These are discussed in the report of the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction (Silberman-Robb Commission), March 31, 2005.

[6] Ibid., 317–319.

[7] The six guiding principles are active, layered defense; situational awareness and integrated command and control; global force management; capabilities-based planning; effects-based operations; and assurance. The military missions are offensive operations, elimination operations, interdiction operations, active defense, passive defense, WMD consequence management, security cooperation and partner activities, and threat reduction cooperation.

[8] See Presidential Decision Directive 56, "Managing Complex Contingency Operations," May 1997, which states: "We must also be prepared to manage the humanitarian, economic, and political consequences of a technological crisis where chemical, biological, and/or radiological hazards may be present. The occurrence of any one of these dimensions could significantly increase the sensitivity and complexity of a U.S. response to a technological crisis."

[9] U.S. Customs and Border Protection, *Container Security Initiative 2006–2011 Strategic Plan*, August 2006, 34, available at <www.cbp.gov/linkhandler/cgov/border_security/international_activities/csi/csi_strategic_plan.ctt/csi_strategic_plan.pdf>.

[10] The final analytic or technical judgment on the findings of a forensic investigation would be made by the Joint Atomic Energy Intelligence Committee.

[11] There is a wealth of information on nuclear effects based on atmospheric testing that occurred until 1963, and a good deal of data on responding to nuclear attacks as well. But many first responders are unaware of this information. Additionally, available data are not adequately adapted to the needs of contemporary first responders. Some efforts are under way to address this, such as the Department of Homeland Security Protective Action Guides for Radiological Dispersal Devices and Improvised Nuclear Devices.

A JTF Training Dilemma

Component Rigor versus Joint Realism

U.S. Army (Jon Soucy)

Navy officer and Soldiers hook Humvee to helicopter during Exercise Granite Triangle

By THOMAS E. WARD II

As we in the land component commands increasingly recognize the value of thinking jointly and prepare to be better partners with our fellow components, we find ourselves facing a training dilemma: ground combat training rigor versus the situational realism of the joint fight. Stated another way, good joint training rigor tends to limit the level of intensity for ground combat. If we fight the "joint fight" well, we shape the environment so that ground combat is minimized or even precluded, friendly ground forces are free to maneuver extensively, and these forces are not seriously threatened with penetration or annihilation by opposing ground forces.

This is not simply a Service-centric problem. Ultimately, this training dilemma derives from the way our nation has chosen to wage its conflicts. Because we value the lives of our citizens so highly, we are loath to put them in jeopardy. This is particularly true in cases where our national interests may be at stake, but our national survival is not. In economic terms, we have chosen to employ a capital-intensive rather than a labor-intensive approach to conflict. We have been willing to make huge investments in extraordinarily capable ships and aircraft in order to minimize or preclude what Carl von Clausewitz referred to as the "cash payment" of the decision by combat—especially ground combat.[1]

While our ground combat forces possess enormous strength and significant standoff advantages through the use of technology, their use places a large number of troops at risk. We have deliberately chosen to place more of our technology-enabled capital at risk, and less of our human capital; we are much more willing to spend money and expend machines than to expend lives.

Put into a campaign perspective, this means that we have a fairly standardized sequence of priorities that we want to accomplish during a crisis leading to a conflict and then during the conflict itself. First, we want to ensure that we have freedom of action in order to project forces and ensure the continuity of their logistical support. This means establishing air and maritime superiority in the area of operations and along the lines of communication (LOC) that extend from our power projection bases to the area of operations. Such freedom of navigation is essential for projecting and deploying any type of combat power, including ground combat power. Establishing local air superiority is a

Dr. Thomas E. Ward II is Battle Geometry Analyst in the Operations Group Delta at the Battle Command Training Program, Fort Leavenworth, Kansas.

critical precursor to employing ground forces, and we certainly strive to achieve air supremacy. We are unwilling to risk having precious ground forces destroyed by enemy aircraft or tactical ballistic missiles.

Lessons from U.S. History

We need look only as far as our own history to see how true the above assertions are and why. The turning point in the joint campaign to capture Guadalcanal, for instance, occurred when the Navy interdicted the Tokyo Express in November 1942, as it was attempting to deliver the bulk of the Japanese 38th Infantry Division to the island. Of the 10,000 Japanese troops destined for Guadalcanal, only 4,000 arrived, and the Japanese never again attempted a similar reinforcement operation.

we have deliberately chosen to place more of our technology-enabled capital at risk, and less of our human capital

How much difference did this maritime interdiction make to the beleaguered U.S. ground forces? It is hard to say, but this engagement occurred almost exactly halfway through the extended series of ground battles to secure Guadalcanal. Japanese troop strength had steadily increased until the destruction of the Tokyo Express, peaking at 30,000 in November. In December, it dropped to 25,000. Without fresh troops and effective resupply, Japanese capability to mount a counterattack dwindled, and the tactical initiative shifted to the Americans, enabling a string of hard-fought but successful ground battles, gaining momentum until the island was declared secure in late February 1943.[2]

We have been uncontested during real conflict at sea since World War II. Just the same, because the Soviet Union was perceived as such a serious threat during the Cold War, we invested enormous talent and treasure to ensure that we could prevail in any conflict, especially that we could maintain freedom of navigation across the North Atlantic through the Greenland–Iceland–United Kingdom gap in the event of a conflict in Europe. Local threats to freedom of movement, through the Straits of Hormuz or in the Gulf of Sidra, for example, have been taken seriously and dealt with successfully without major sea battles. Consequently, during major conflicts, our maritime forces have been employed primarily to augment and support domination of the air and ground battles. This was true during the Korean War, Vietnam, Operations *Desert Shield* and *Desert Storm*, the Balkan conflicts, and Operations *Enduring Freedom* and *Iraqi Freedom*.

The same is true, although perhaps less so, when we consider airpower. Superiority in the air is a prerequisite for freedom of navigation, security of LOC, and the deployment or employment of ground forces. We need air superiority not only to protect our freedom of movement but also to conduct offensive air operations that shape the battle environment and protect our ground forces—close air support, air interdiction, and a strategic air campaign. One of the differences between the maritime and air environments is that we are more likely to find a challenging air environment than a challenging maritime environment. Since the United States has no peer in the maritime environment, an adversary would be unable to challenge U.S. forces there, except in a relatively small locale, and then only for a short time.

The situation is not quite as rosy in the air environment. Many nations, among them potential adversaries, have chosen to invest heavily in their air components and air defense forces. With these forces, they are able to establish at least parity over their sovereign territory and may have the capability to extend an umbrella of superiority in the region beyond their borders, including maritime areas. Consequently, to maintain freedom of movement, reduction or elimination of the air threat is a high priority, even with secure strategic LOC from power projection bases. We secure the sea and air first and then launch ground operations.

This style of warfare has allowed us to prevail, using our technological advantage to enable maneuver of forces and massing of fires without necessarily massing our most prized resource—personnel. Our ability to establish superiority, even supremacy, over enemy air and maritime forces means that we are able to interdict those forces not only as they deploy through the air and maritime environments, but also, almost at will, as they attempt to move or maneuver on the ground. We use these advantages to shape the ground environment in our favor, attempting to ensure that our ground forces do not have to cope with an enemy force that could overwhelm them through sheer mass.

We also enable our forces to maneuver effectively, avoiding enemy strengths and focusing on enemy weaknesses. *Desert Storm* was a superb example of this type of campaign at work. A relatively well-equipped enemy was first blinded through destruction of its air component, and then completely deceived by operational maneuver on an unprecedented scale. With air supremacy, we were able to maneuver ground forces without fear of air interdiction, or even of detection by means of aerial reconnaissance during the critical pre–ground offensive operational movement of the XVIII and VII Corps to the west, while inflicting overwhelming casualties on enemy ground forces through air interdiction.[3]

The Dilemma of Success

Phenomenal success has created a training dilemma. We still want our ground forces to experience the rigor of engaging a competent near-peer ground force in a high-intensity environment. We have done so in the past by creating training experiences largely devoid of the synergistic contributions of the other Services. The Combat Training Center (CTC) experience and the Battle Command Training Program (BCTP) "Warfighter" experience have been superb for supplying rigorous, high-stress training for ground combat, but until recently, they have been relatively devoid of joint context. Even now, providing a joint context in the "dirt" CTC and "virtual" BCTP training environments is focused primarily on tasks supporting the tactical level, providing nonorganic intelligence, surveillance, and reconnaissance support, fire support, or logistics.[4]

Participants in CTC training perceive a joint environment, but the joint context is shaped to provide an awareness of other Services, not an appreciation for capabilities that can furnish operational level shaping of the battlespace. This is not a criticism of the tactical focus of CTC; it is merely an observation of a limitation imposed by that focus. Part of the Army's Title 10 responsibility is to provide trained, equipped, and ready forces to combatant commanders. Tactical proficiency is paramount, so we have learned how to develop and maintain superb tactical proficiency.

Excessive focus on the contributions of other Services at the tactical level of ground

combat causes us to overlook or ignore the operational level contributions they make through the prosecution of their own tactical level engagements in their respective environments. Maritime interdiction of a sea LOC and air interdiction of deploying ground forces, for example, are tactical missions for the respective Services, but they have operational level impact on the campaign.

As ground component forces, we have trained well to succeed at the tactical level of combat. We can congratulate ourselves for becoming the best in the world at what we do. But we must temper that pride with recognition of two significant facts: the contributions of our comrades in arms in the other Services have enabled success through their contributions to the campaign; and we need to be able to think operationally as well as tactically in order to get the most out of the capabilities of the other Services. Tactical level mastery at any level, from fire team to field army, is a perishable skill. We must retain our level of excellence in the ground combat environment by sustaining rigorous training. But we must not rest on our laurels, because we have learned the hard way that tactical level success can be extraordinarily expensive and that tactical success on the ground does not necessarily translate into operational or strategic level victory.

Training at the Operational Level

If the Army and Marine Corps are to fulfill roles at the operational level in the joint tactical/operational/strategic framework, we need to develop an ability to think and plan at the operational level. That includes an ability to shift focus from the ground tactical fight to the joint multicomponent fight. This ability seems a simple thing, but it has proven extraordinarily difficult, and that is not unique to the Army. Each Service has a tendency to see the universe from its own habitual perspective. For the ground components (and this is especially true of their staffs), there is a tendency to focus on the close fight, while ignoring the value or even the possibility of air or sea interdiction of deploying forces or lines of communication. Air and maritime component personnel show the same characteristic: a tendency to seek elimination of all risk from an enemy operating in their respective domains before they are inclined to provide resources to support other components' fights. This is not necessarily a matter of Service parochialism; it is a predictable consequence of the way we concentrate on our own tactical domains within each Service in our respective professional development processes of training, experience, and self-study.

A single exercise cannot adequately meet the desired training objectives of all the training stakeholders. Conflicting requirements from the various Services weigh against

we still want our ground forces to experience the rigor of engaging a competent near-peer ground force in a high-intensity environment

Soldiers participate in Exercise Omega at the Joint Multinational Readiness Training Center

U.S. Army (Gary Kieffer)

Training during Exercise Foal Eagle 2007

Fleet Combat Camera Group (Sandra Palumbo)

Multinational troops staff operations headquarters during Exercise Tradewinds

DOD (Joseph Bonet)

the design of an exercise that can be all things to all components. Meeting the needs of the land component is particularly difficult if the air and maritime components are exercised well and employed effectively. This becomes a strong argument against embedding a warfighter exercise (WFX) in a joint training exercise, which may appear to be cost efficient from a training dollar perspective but competes with training effectiveness.

For example, for an Army corps (or a Marine expeditionary force, for that matter) acting as a joint task force (JTF) headquarters, the first priority must be to fight the joint fight—that is, to take advantage of the synergy available from synchronized, coordinated employment of capabilities from all the Services. If they fight the joint fight well, they are unlikely to face the ground combat intensity that characterizes WFX rigor. Only if they fail to perform their JTF headquarters role well will they experience WFX-style rigor in the ground fight. To achieve that level of intensity in the ground fight would require restraining the success of the air and maritime components by constraining their actions to limit effectiveness or overwhelming them with a superior opposing force. Both of these options (constraining and overwhelming) require a highly contrived scenario—entirely possible, but not necessarily good training.

There are exceptions. Embedding a lower level exercise—a brigade or division WFX, for example—within a joint level exercise in which the WFX training audience is not a joint level headquarters allows deliberate shaping of the virtual battle environment in order to create what we have traditionally considered WFX rigor. This would require much less contrivance, as opposing ground forces could reasonably be expected to gain local tactical superiority from time to time.

Another approach would be to rationalize training objectives more rigorously for joint level exercises. This approach would prioritize the training value for the joint level headquarters and provide clear priorities for the training experiences of the secondary training audiences (the Services). A well-written scenario and effective exercise design could provide a rigorous training experience for any component, but such a design requires acknowledging that not every component can have the first priority. For example, in one year, in a given exercise, we would give the higher training priority to the land component as the supported command, with the air and maritime components as the supporting commands. The following year, or in another exercise, the training priority can be different. It is not an issue of which component is more important but rather of getting the best training experience for all the components and recognizing that we probably cannot accomplish all of that in a single exercise. From a systems perspective, it is merely recognizing that in order to optimize the entire system, we may have to accept suboptimization of a system component, at least from that component's perspective.

Yet another approach would exercise a joint force through all the phases of an entire campaign: deter/engage, seize the initiative, decisive operations, and transition.[5] This approach is seldom if ever seen because it takes so long to develop the campaign and its outcomes. However, by linking a series of exercises, such an approach would be possible. Service training experience priorities can be built into the different phases of the campaign that run through and link the series of exercise events. This would allow the JTF headquarters to experience the challenges of not only integrating the component capabilities but also allowing the headquarters to experience the challenge of planning and executing the transitions between phases and shifting supported and supporting command relationships. A natural byproduct of this design would be to allow each of the Services to experience supported and supporting command responsibilities and to experience the kind of training rigor each desires.

Joint training exercises create a Service training dilemma: good joint level training does not necessarily provide a good component training experience. This is not an unsolvable problem, but it will require a systems view of the joint and Service training experience. A single exercise cannot be all things to all components. Rather, to provide good joint and operational level training experience, individual components may find their experience suboptimized in any given exercise. With a long-term approach to exercise planning, however, everyone (the JTF headquarters and the individual Services) can experience the kind of training rigor they desire. They simply cannot all experience it at the same time or in every exercise. Overall systems optimization will most likely require suboptimization in order to put everyone through the desired level of rigor over time. **JFQ**

NOTES

[1] Carl von Clausewitz, *On War* (London: Penguin Books, 1982).

[2] Charles R. Anderson, *Guadalcanal—The U.S. Army Campaigns of World War II* (Washington, DC: Center for Military History, 1989), available at <www.army.mil/cmh-pg/brochures/72-8/72-8.htm>.

[3] Rick Atkinson, *Crusade: The Untold Story of the Persian Gulf War* (New York: Houghton-Mifflin, 1993).

[4] William S. Wallace, Timothy D. Livsey, and Richard A. Totleben, "A Joint Context for Training at the Combat Training Centers," *Military Review* 84, no. 5 (September/October 2004).

[5] Joint Publication 5–00.1, *Joint Doctrine for Campaign Planning* (Washington, DC: The Joint Staff, January 2002).

Log-centric Airbase-Opening Strategies in Korea

By STEVEN M. ANDERSON *and* DOUGLAS A. CUNNINGHAM

The airlift of supplies to the forward elements of the 8th Army, at a time when such an operation was our only means of supply, has permitted ground troops to continue their combat mission in the forward area. The keen application of the logistics situation, and the efficiency . . . demonstrate the close cooperation that exists between ground and air in the Korean War.

—Lieutenant General Walton H. Walker, Commander, 8th U.S. Army, Korea, 1950[1]

South Korean military participate with U.S. Soldiers, Marines, Airmen, and Sailors in the air operations center at Osan Air Base, Exercise Foal Eagle 2007

4th Combat Camera Squadron (Francisco V. Govea II)

Brigadier General Steven M. Anderson, USA, is Deputy Chief of Staff, Resources and Sustainment, Multi-National Force–Iraq. Major Douglas A. Cunningham, USAF, served as Chief of the Tactical Airlift Branch in the Transportation Division of Combined Forces Command between 2004 and 2006. He is currently pursuing a Ph.D. as part of the Air Force Institute of Technology's Civilian Institution program.

Operations *Enduring Freedom* and *Iraqi Freedom* have afforded the U.S. military unique opportunities to open airfields under wartime conditions—missions that have become increasingly important as more overseas bases close down. These opportunities have demonstrated the global reach capabilities of U.S. airbase-opening forces and the ways in which regional commanders employ these forces to achieve mission goals. The experiences have proven particularly valuable for specialized, task-organized airbase-opening units, such as the Air Force's Contingency Response Groups (CRGs), built as "first responders for opening airbases . . . [that] bridge the gap between the seizure forces and the follow-on combat/expeditionary combat support forces."[2]

As valuable as ongoing operations have been for exercising new airbase-opening structures and ideas, current theory remains focused specifically on opening airbases for fighter aircraft and other operations-centric missions already codified in doctrine.[3] In addition, present discourse centers almost exclusively on U.S. unilateral base-opening efforts, rather than exploring the ways multinational partners combine to accomplish airbase-opening missions. Alexander M. Wathen stresses this latter point: "Missing from the CRG concept of operations . . . and training plans is the construct of joining with our coalition partners throughout the globe. It is time to start thinking beyond 'jointness' and begin moving into the realm of 'coalition,' since recent history shows that unilateral U.S. action is becoming politically less viable."[4]

In the Korean theater of operations (KTO), Republic of Korea (ROK) and U.S. planners, from Combined Forces Command (CFC) and its components, are exploring ways to share the burden of airbase openings while, at the same time, focusing on how such airbases can serve as logistics (log)-centric distribution hubs for airlifted materiel. Both of these issues are important for further study and analyses; in the post-9/11 era, when American forces are spread

thin among various contingencies and conflicts across the globe, the military must increasingly plan and coordinate with its international partners to ensure the effectiveness of host-nation transportation infrastructures and supply distribution strategies. Without such coordination, commanders assume significant risk to the time-tested logistics promise of getting the right materiel to the right place at the right time.

it is time to start thinking beyond "jointness" and begin moving into the realm of "coalition"

As part of the effort to reach combined airbase-opening solutions and robust plans for aerial resupply of combat or other ground forces, CFC planners have adopted and adapted strategies employed in both Afghanistan and Iraq to develop a concept for forward-located distribution hubs in the KTO, known as air terminal supply points (ATSPs). This article examines the development of these combined airbase-opening concepts in the KTO and the lessons learned as a result of planning and executing a combined, proof-of-principle ATSP field training exercise and operational vignette during spring 2006.

Throughout the concept and exercise development processes, several key questions presented themselves. How would ROK and U.S. forces combine to open airfields on the Korean Peninsula? Which nation and which units would assume responsibilities for which tasks? What challenges might hinder progress toward combined goals? How would decisions be made regarding airfield selection and identification of the Senior Airfield Authority (SAA, the component charged with airfield operations) and Base-Operating Support Integrator (BOS–I, the component charged with life support and security for the airbase)? Who would make these decisions? Which agencies would own the ATSPs? While final answers to these questions are still under development, CFC and ATSP Working Group planners have nevertheless reached 10 interim conclusions that help light the way ahead for airbase-opening operations in the KTO and in other combined environments.

Background

The concept of opening austere airfields to support aerial resupply of regional forces or medical/equipment backhaul is certainly not new to the Korean Peninsula. United Nations forces, for instance, successfully employed the concept on several occasions during the Korean War. Recently, however, CFC planners, inspired by the successes of base openings in Operations *Enduring Freedom* and *Iraqi Freedom*, recognized the continuing viability of the concept within the KTO, dusted off the history books, and placed new emphasis on log-centric airbase openings.

To this end, in October 2004, the C[4] (Command, Control, Communications, and Computer) Transportation Division established the ATSP Working Group, a combined/joint team consisting of transporters, log planners, security forces, air mobility experts, operators, engineers, and various other functional areas. This working group operated with a mandate to plan combined, log-centric airbase openings and operations, and later to execute a field training exercise to validate these missions and to develop/maintain proficiency.

By March 2005, the working group had developed a white paper for distribution at the CFC Spring 2005 Senior Leaders Seminar that explicitly addressed a doctrinal gap in airbase terminology:

> ATSP *is a current term, specific to the KTO, that fills a doctrinal gap in both the terminology and operational concepts related to theater airlift operations. . . . [T]he term originated from the need to describe the location and purpose of a forward airfield specifically designated for air-landed re-supply operations in support of ground forces. Historically, the term* Forward Operating(-ions) Base (FOB) *was used in the attempt to describe what logistics planners intended; however, experience working with our ROK counterparts and exercise AARs* [after action reports] *indicated that this term was confusing, had different meanings to different users, and was not adequately descriptive. An initial survey of doctrinal terms listed* [in Joint Publication 1–02, Department of Defense Dictionary of Military and Associated Terms, and Field Manual 101–5–1, Operational Terms and Graphics] *shows that no one term is particularly suitable. The terms tend to speak of RSOI* [reception, staging, onward-movement, and integration] *processes, tactical air operations, ground operations, or special operations separately, and they do not adequately describe the air-ground, inter-modal, and combined nature of the concept.*[5]

The white paper went on to provide its exact definition of ATSP:

> *The term* Air Terminal Supply Point *marries the air concept of an air terminal to the ground concept of a supply point* [both of which are doctrinal terms]. *The term is simple, intuitive, and easily understood when translated literally as "a place to receive supply by air." Based on this construct, we currently define an ATSP as a designated air transportation hub that accommodates the loading and unloading of airlift aircraft and the in-transit processing of traffic [not to include cargo breakdown] in support of ground forces. The ATSP also serves as a designated location in an area of operations used as a base for supply and evacuation by air* [6] (see figure 1).

The term *ATSP* generates some controversy in the KTO (particularly among Air Force personnel with base-opening experience in Operations *Enduring Freedom* and *Iraqi Freedom*) because it is theater-specific and, for the time being, nondoctrinal. The irony, however, is that since the term was introduced to the theater in 2004, it has demonstrated its value and come into common use at all levels on both the ROK and U.S. staffs, from action officers up to the four-star commander of CFC.

the concept of opening austere airfields to support aerial resupply is not new to the Korean Peninsula

The term's usage persists because it addresses a specific mission performed at an equally specific airbase scale. Throughout 2005, however, planners continued to grapple with the term's nondoctrinal status, and for this reason, the ATSP Working Group designed an aerial port of debarkation (APOD) continuum (see figure 2) to represent where an ATSP (as an emerging doctrinal concept) might sit in relation to doctrinally accepted APOD sizes. This representation helped by acknowledging that an ATSP was not yet a doctrinal concept while, at the same time, providing planners with a doctrinal context for its local application

Figure 1. Air Terminal Supply Point Layout (Notional)

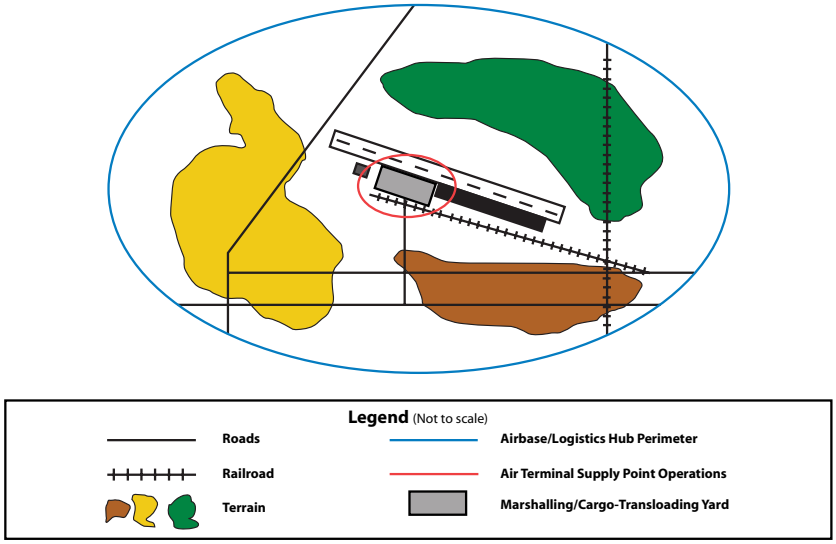
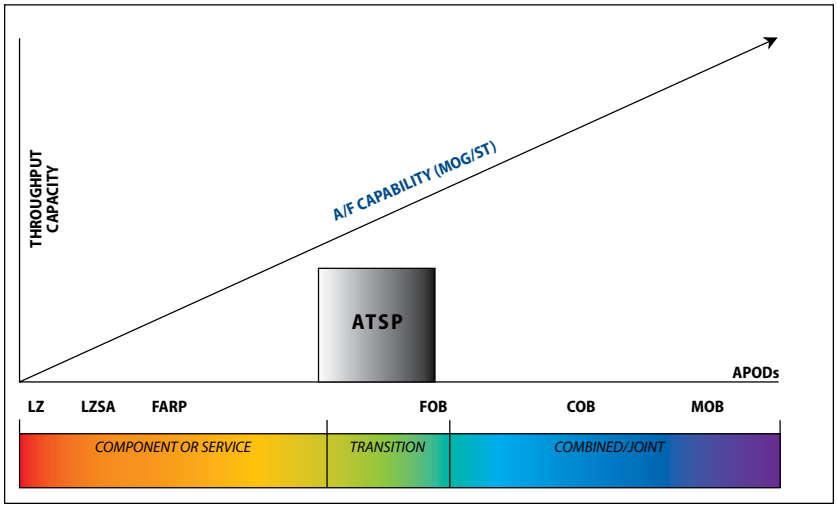


Figure 2. APOD Continuum



in the KTO. The chart also demonstrated that airfield sizes could be tailored to fit operational requirements, thereby eliminating the "one-size-fits-all" APOD versus ATSP thinking that had come to characterize thinking in the Korean theater of operations. Finally, the chart reflected the fact that an ATSP airfield has the potential to grow beyond its log-centric mission to become a larger-scale APOD, such as a collocated operating base or a main operating base, during which time its ownership would grow distinctly more joint and combined.

Between 2004 and 2006, planners in the KTO exercised the ATSP concept in a number of theater-level command post exercises (CPXs). Each of these CPX experiences helped to define the concept further while, concurrently, educating theater planners (particularly surface transportation planners) about the inherent strengths and limitations of ATSP operations.

More importantly, these CPXs made clear the need for a physical execution of the concept. Even at senior levels, leaders and planners often had misconceptions about the scale and realistic potential of ATSP operations. The ATSP Working Group planned to dispel these misconceptions with a combined field training exercise and operational vignette slated for the spring of 2006. After a year of planning, Working Group planners executed the field training exercise and operational vignette with great success. These events included practice and demonstrations of CRG airfield assessment and establishment of Air Force Red Horse Assault, Assessment, and Repair Operations; combined air-traffic control; combined airbase-ground defense; combined cargo-offloading and transloading (to both rotary-wing aircraft and ground transport); and combined SAA to BOS–I interaction (CFC's Air Component Command acted as SAA while Ground Component Command provided the BOS–I).

Ten Early Lessons Learned

Two years of exercise planning and execution by the ATSP Working Group have yielded some valuable and unique lessons regarding combined airbase openings in the KTO. These lessons will almost certainly prove useful in other theaters as planners evaluate options for reducing demand on U.S. forces to open log-centric, ATSP-like airbases in environments where forward basing has been dramatically reduced.

Crawl First, Run Later. C[4] Transportation, as the head of the ATSP Working Group, briefed the ATSP concept at every opportunity to permanent party military personnel in the KTO and to visitors from the continental United States. Although excited about the Working Group's efforts, many watching the briefings asked questions that were beyond the current level of planning. Many of these questions dealt with the specifics of execution at the component levels, which would necessarily be answered by the components themselves when writing the supporting plans for the CFC-level plan. During these early presentations, briefers always explained that the concept was in its "crawl stage" and that the "run stage" would come later (which it did). In almost every case, inquisitive audience members accepted this answer, and their well-intentioned questions contributed to

even at senior levels, leaders and planners often had misconceptions about the scale and potential of air terminal supply point operations

future thought and planning for the ATSP at both the theater and component levels.

Go Combined Early. The ATSP Working Group enjoyed the advantage of working in a well-greased combined environment in the KTO because the 56-year-old ROK–U.S. alliance provided long-tested channels through which to communicate. Language and cultural differences presented their share of challenges, but ATSP planning undoubtedly benefited from great ROK interest and participation. The combined nature of the planning, for example, quickly revealed many of the strengths and limitations that each nation would bring to actual ATSP execution, and it generated important discussion at the ROK component levels about the scale and supportability of the ATSP concept. Similarly, U.S. planners tempered their initial expectations based on ROK feedback, and the resulting planning products proved all the more realistic.

Stress Flexibility in Planning. As ATSP planning progressed, many combined logisticians, engineers, and even operators in the KTO became overly focused on the specifics of the planned ATSP locations, SAA, BOS–I, and so forth, and lost sight of the greater need to remain flexible enough to respond to operational needs. C[4] Transportation and the ATSP Working Group strived to correct this course of thought by stressing the need to think outside of the deliberately planned box. While purposeful planning remains the essential baseline for eventual execution, the mission, enemy, terrain and weather, troops available, time available, and civilians almost always dictate that the plan will have to change. The working group wants KTO planners prepared for these potential vector changes, and it has developed policies and procedures to ensure that all ATSP options get weighed in the struggle to meet operational requirements.

Empower Working Group Decisionmakers. As the ATSP concept began to mature and the planning for a field training exercise began, combined ATSP exercise planners soon encountered significant cultural differences in decisionmaking at the action-officer level. While the U.S. senior leadership empowered its action officers to discuss issues and make key decisions at planning conferences, the ROK senior leadership preferred to have action officers collect issues at planning conferences and then present those issues for decision at the O–6 or O–7 level. While neither method proved right nor wrong, the planning conferences nevertheless required the presence of empowered decisionmakers (this would have been especially true during fast-paced, real-world execution when the need to reduce the planning cycle time would be paramount). Eventually, the ROK planners appointed two capable and passionate ROK army colonels (with several action officers in tow) to represent its interests at major planning meetings. The U.S. planners kept their senior leadership informed and engaged, but they did not arrive on the ground at the field training exercise site until 2 weeks prior to execution. The key is to plan with cultural differences in mind while, at the same time, ensuring the presence of participants who can make decisions on behalf of their organizations.

Engage Operational Planners. Undoubtedly, operational planners have a lot on their plates. They realize the logistics fight is important, but sometimes their attention is necessarily focused elsewhere. When planning something as important as log-centric airbase openings, however, the input from operational planners is both invaluable and required. These individuals help to frame ATSP planning by providing requirements, schemes of maneuver, and operational timing/synchronization advice. Working Group planners succeeded in roping operational planners into ATSP concept planning through sheer persistence, demonstration of relevance, and a mutual understanding that operational planners will often have higher priorities on any given day. Because of the good working relationship established between the ATSP Working Group and the planners, both parties now comprehend the ways in which each can effectively respond to the needs of the other in deliberate, exercise, or crisis-action planning. These interactions have also educated the logistics community about the scope of operational requirements, and this education has enabled the ATSP Working Group to address those requirements more effectively.

Exploit Equivalent Capabilities. First during the ATSP concept planning and later during the ATSP field training exercise planning, the Working Group sought to identify and take advantage of similar capabilities between the United States and ROK. That helped the Working Group ensure that the airbase openings would truly be combined, with plenty of opportunities for the ROK side to act as full partner and contribute significantly in areas such as airlift, security, engineering, aerial-port operations, air-traffic control, and cargo loading, unloading, and transloading.

the key is to plan with cultural differences in mind while ensuring the presence of participants who can make decisions of behalf of their organizations

While the ROK military did not match American capabilities unit for unit, it did feature significant aerial port, engineering, security, and cargo-handling teams. For example, while the United States seeks to employ an ad hoc arrival/departure airfield control group as its primary cargo-handling and marshaling authority, the ATSP Working Group quickly learned that the Korean side has standing airlift service support point teams that perform the same mission. This discovery resulted in more planning and execution flexibility. Similarly, both the ROK and United States explored ways to utilize their equivalent engineering capabilities, expertise, and equipment essential to opening any airbase. Interestingly, the ROK side grew so enthusiastic about the Air Force CRG concept during discussions about the ATSP that they quickly researched ways to develop their own equivalent from preexisting ROK military units, and the ATSP field training exercise presented the ROK with its first opportunity to test this concept.

Share Costs, Facilities, and Equipment. As with the previous point, efforts to ensure truly combined airbase openings in the KTO would necessarily include shared costs, facilities, and equipment. While many of the details of these shared efforts will have to be identified and resolved at the component levels, primary areas for such sharing have surfaced during both ATSP concept planning and field training exercise planning (for example, life support, fuel, water, engineering, lodging, and materiel-handling equipment). As the concept matures in supporting plans, the ATSP Working Group will continue to look to precedents in *Enduring Freedom, Iraqi Freedom*, and even the Korean War to help materialize the mutually supportable solutions.

Secure Buy-in from Senior Leadership. The ATSP Working Group planners secured a great deal of buy-in by placing the ATSP concept before combined, four-star leadership at two key events: the Senior Leaders Seminar in spring 2005 and the ATSP field training exercise and operational vignette in

as a result of the field training exercise, the Working Group identified a lack of codified procedures for combined pallet buildup and cargo loading

Republic of Korea air force security advisor speaks with U.S. Army officer in Kirkuk, Iraq

U.S. Air Force (Suzanne Jenkins)

Supplies are loaded onto Korean C–130 at Hickam Air Base, Hawaii

U.S. Air Force (Ed Foster)

spring 2006. At each of these events, planners presented the CFC commander and dozens of other ROK and U.S. flag officers with briefings and prepared scenarios designed to demonstrate the viability of the ATSP concept. During the Senior Leaders Seminar, the deputy C4 explained the concept (then in its infancy) and described a tactical vignette scenario to which audience members contributed comments and questions. For the ATSP field training exercise and operational vignette 1 year later, the Air Component Command of CFC planned and executed a major ATSP orientation briefing and a real-world, scripted aerial port and cargo-transloading demonstration designed to communicate the scope of ATSP operations and capabilities. Both events were well received, generated a great deal of discussion among senior leaders, and contributed to a greater emphasis on ATSP operations in the KTO than the ATSP Working Group could possibly have envisioned in 2004.

Develop and Codify Procedures. The planning processes for both the ATSP concept and the ATSP field training exercise have provided unique opportunities to identify gaps in current policies and procedures. For example, as a result of the field training exercise, the Working Group identified a lack of codified procedures for combined pallet buildup and cargo loading. Resolution of this issue has now become a C4 Transportation priority. Similarly, ATSP play in various command post exercises uncovered a need for a more structured method of selecting ATSP locations and their respective SAAs and BOS–Is, which, in turn, could work in tandem with future command, control, and communications plans, processes, and time cycles. C4 Transportation, in concert with C4 Plans, devised a decision-tree process for this purpose for approval by the ATSP Working Group, and this process will soon find a home in the next edition of the C4 Logistics, Policies, and Procedures. As these procedural gaps arise, planners should convene the necessary working groups and operational planning teams to generate, codify, and secure approvals for proposed solutions.

Practice, Evaluate, Advertise Success. Certainly, any endeavor improves after practice under the watchful eyes of both internal and external observers. After practicing the ATSP concept during a major command post exercise in the spring of 2005, Working Group planners arranged for future planning oversight from CRG subject-matter experts during KTO planning conferences. The experience that these experts brought to further planning, both for the ATSP concept and the field training exercise, proved priceless. In addition, exercise planners arranged for observers from U.S. Joint Forces Command to provide feedback after watching the field training exercise and operational vignette. This feedback, too, proved invaluable to future planning efforts.

The U.S. military needs to look beyond its current paradigms for opening airbases by examining the ways in which multinational or host-nation partners can play a major role in relieving the American burden and contributing to current and future fights. The ATSP concept, developed for austere, log-centric airfields opened by the combined ROK–U.S. forces, offers a proven template for airbase openings, one that incorporates the latest lessons of operational requirements and logistical constraints.

While still under development as emerging doctrine, ATSP planning has demonstrated substantial promise as a key enabler to get the right materiel to the right place at the right time, through close coordination and participation of multinational and host-nation forces. And such cooperation with our allies is exactly what the United States needs to achieve success in its coalition efforts. **JFQ**

Contributors: Lieutenant Colonel Ken Stanfill, USAF, Major Lars Hubert, USAF, and Captain Jeffrey Jacques, USAF.

NOTES

[1] Quoted in William M. Leary, *Anything, Anywhere, Anytime: Combat Cargo in the Korean War* (Washington, DC: Air Force History and Museums Program, 2000), 10–11.

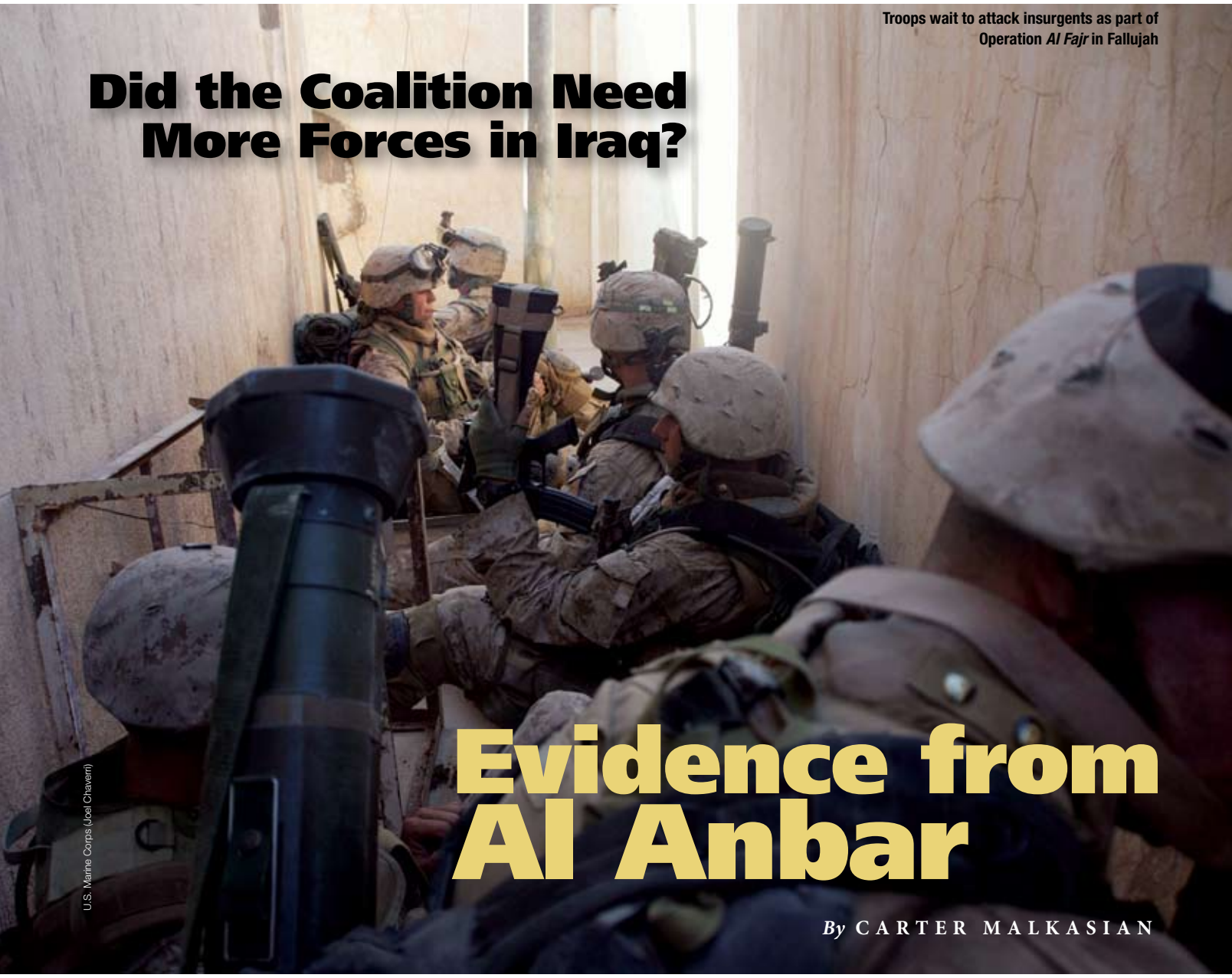
[2] Barbara Lee, "Air Force Contingency Response Group Operational Concept, Version 1.0" (Washington, DC: Headquarters U.S. Air Force, 2004), 2.

[3] Rodney L. Croslen and Marsha Kwolek, "Retooling Global Mobility and Forward Presence: Solving the Challenge of Opening Airbases," *Air Force Journal of Logistics* 29, no. 2 (Summer 2005), 18–31, available at <www.aflma.hq.af.mil/lgj/Vol_29%20No%202%20WWW.pdf>.

[4] Alexander M. Wathen, "Contingency Response Group: Time to Expand the Box and Think 'Coalition,'" *Air & Space Power Journal* 19, no. 2 (Summer 2005), available at <www.airpower.maxwell.af.mil/airchronicles/apj/apj05/sum05/sum05.html>.

[5] C4 Transportation, C4 Plans, and the ATSP Working Group, "Air Terminal Supply Points: A White Paper on a New Operational Concept," 2005.

[6] Ibid.



Troops wait to attack insurgents as part of Operation *Al Fajr* in Fallujah

U.S. Marine Corps (Joel Chaverri)

Did the Coalition Need More Forces in Iraq?

Evidence from Al Anbar

By CARTER MALKASIAN

Numerous scholars, military officers, and policymakers have argued that the United States deployed inadequate numbers of forces to secure Iraq.[1] They generally agree that by trying to secure the country with only 150,000 troops, the coalition allowed the insurgency to grow. The argument rests on an assessment that successful counterinsurgency is inherently labor-intensive. A standard back-of-the-envelope formula for the number of security personnel per civilian needed to suppress an insurgency is 20 per 1,000. The formula prescribes 500,000 troops for Iraq.[2] According to this camp, successful counterinsurgency requires securing the population through foot patrols, checkpoints, urban outposts, blockhouses, sniper operations, ambushes, curfews, and systematic management of population databases.[3] These techniques demand ample forces, particularly infantry. They are meant to prevent insurgents from controlling the population by impeding their freedom of movement. This method is known as the *clear-hold-build approach*, or presence.

The opposing argument is that the United States deployed adequate forces to Iraq. According to this camp, the presence of U.S. conventional forces only worsened the insurgency by presenting an image of occupation.[4] Congressman John Murtha (D–PA) is the most famous proponent of this argument. In his words, "Our troops have become the primary target of the insurgency. They are united against U.S. forces and we have become a catalyst for violence."[5] Many in this camp argue that a different approach to counterinsurgency could have enabled success with fewer forces. This alternative focuses on developing indigenous forces with a small number of advisors. Indigenous forces, not

Carter Malkasian is Director of the Center on Stability and Development at the CNA Corporation. Previously, Dr. Malkasian was assigned to the I Marine Expeditionary Force in Iraq as a field analyst.

American forces, protect the local population themselves, providing the numbers for successful counterinsurgency. A concept of embedding small cadres of advisors with indigenous forces has worked in previous counterinsurgency campaigns, such as Oman and El Salvador. Accordingly, the phrase "less is more" has been applied. This method has sometimes been called the *indirect approach*.

Empirical evidence collected in Al Anbar province suggests that the United States indeed dedicated inadequate forces to secure Iraq. The evidence was collected while the author worked as an advisor to I Marine Expeditionary Force (I MEF) from February 2004 to February 2005 and from February to August 2006. It compares the effectiveness of operations that used substantial U.S. forces to secure the population to those that did not. If operations involving relatively few forces experienced success, then the coalition might have been able to secure Iraq with fewer rather than more forces. This was not the case. Such operations generally could not suppress large-scale insurgent activity. When forces were meager, insurgent activity noticeably increased. Operations that saturated cities with coalition forces enjoyed a much stronger record of success.

The comparison implies that more forces, rather than fewer, would have improved the situation in Al Anbar and perhaps Iraq as a whole. Scarcity of forces was the major limitation on directly protecting the population. Until reinforcements arrived in late 2004 and mid-2005, the coalition lacked the forces to provide security in even the key cities. Progress in Iraq might have been accelerated if the population could have been protected in these cities in 2004. The comparison also offers insight into the likely effects of an American withdrawal from Iraq. If the surge fails, a reduction in U.S. forces in key cities and the implementation of an indirect approach may allow insurgent activity to increase and impede efforts to develop indigenous forces.

Case Studies of the Indirect Approach

Al Anbar province is overwhelmingly Sunni and an infamous center of insurgent activity. I MEF took responsibility for Al Anbar in March 2004. Three key cities—Ramadi, Fallujah, and Al Qa'im—needed to be held, along with eight other towns. With roughly 11 battalions in March 2004, I MEF could not hold every city with adequate forces, so it dispersed its strength near these cities, viewing them as key terrain. Iraqi forces under I MEF for most of 2004 consisted of seven locally recruited Iraqi National Guard (ING) battalions, plus police forces totaling perhaps 2,000.[6] Other than one ING battalion and one ING company, Sunnis manned all of these forces. With the exception of a single company, the ING battalions could not be moved from their home area. The Shi'a-dominant Iraqi army was still being trained and would not arrive until November 2004.

The ratio of 20 security personnel per 1,000 civilians far exceeds what the combined coalition and Iraqi indigenous forces could provide in Al Anbar. Thirty-one U.S. battalions would have been required to attain this ratio in just the 11 cities. A traditional operational method for mitigating scarcity of forces has been to concentrate troops over the key population centers and then expand outward, similar to an oil slick. As population centers are secured, indigenous forces are developed. Those forces eventually can take over security, freeing other forces to move on to secure a new area. Yet it is hard to see how the oil slick method could have succeeded in Al Anbar when the coalition deployed only 11 battalions and the ING forces were immobile.

comparison implies that more forces, rather than fewer, would have improved the situation in Al Anbar and perhaps Iraq as a whole

Fifteen battalions would have been required for Fallujah and Ramadi alone. This would have entailed abandoning key infrastructure, including the highways that served as supply lines. Neither the coalition headquarters in Baghdad, which had ordered the protection of key infrastructure, nor the Iraqi government would have accepted this cost.

I MEF and II MEF did not dictate how regimental and battalion commanders should employ their forces. Commanders were free to use the clear-hold-build approach, an indirect approach, or any other approach, although the clear-hold-build approach received the greatest emphasis. Three cases demonstrate the weakness of the indirect approach: Fallujah (May to October 2004), Hit (March 2004 to June 2005), and Al Qa'im (July 2004 to October 2005).

Fallujah. Following the ceasefire that halted I MEF's April 2004 offensive into the city, Fallujah, which contained roughly 250,000 people, grew as an insurgent safe haven, becoming the locus of command and control for the entire country. Forbidden from reentering the city, I MEF attempted an indirect approach that had two components. First, in May, I MEF organized the Fallujah brigade to enforce security. The brigade comprised approximately 2,000 local residents. I MEF paid them to keep terrorists and foreign fighters out of the city. The brigade had no advisors, and its leadership staunchly refused them. Its soldiers had no intention of working directly with the coalition and did not want to fight other Sunnis. Most of the brigade appeared sympathetic to the insurgency and too intimidated to take any firm

2d Marine Division Combat Camera Unit (Jason Beckstead)

Troops prepare for major assault during Operation *Steel Curtain* in Al Qa'im

action against foreign fighters. The initiative yielded little. Large insurgent units organized, trained, and staged within the city. Incident levels actually *increased* as insurgents gained control of the city and then clashed with coalition forces. Human intelligence collection became extremely difficult after the April ceasefire as sources became vulnerable.

Second, from late June until the second battle in November, the coalition conducted precision airstrikes against insurgent concentrations and command and control nodes within Fallujah. The goal was to take out key insurgent leaders and to kill as many fighters as possible while minimizing collateral damage. The strategy killed over 100 insurgents and may have temporarily disrupted their command and control. Intense fusion of airborne surveillance, signals intelligence, and imagery intelligence guided the strikes, which were particularly effective on the uncommon occasion when actionable human intelligence was available. They softened insurgent resistance in preparation for the offensive in November. Insurgent leadership had to conceal their movement, change methods of communication, and meet in smaller groups.

Precision airstrikes, however, were not effective in suppressing insurgent activity or permanently crippling insurgent command and control. In fact, insurgent strength continued to grow. From June to November, Marines often engaged groups of 30 to 100 insurgents on the outskirts of the city. Strikes impaired insurgent freedom of movement, but large units still could mass under urban cover and run checkpoints—and the population still could not conduct their normal lives. Problems in human intelligence collection persisted, limiting the number of available targets. Insurgents used Fallujah as a base to plan and organize attacks throughout Iraq. Before I MEF assaulted Fallujah in November, insurgent command and control proved sufficiently intact to relocate key leaders and numerous fighters elsewhere in Iraq.

Iraqi soldiers conduct security patrols in Fallujah

U.S. Marine Corps (Neil Sevelius)

Marine conducts rooftop security patrol

U.S. Marine Corps (Kenneth Lane)

I MEF did exactly what critics of presence prescribe—it all failed

The Fallujah brigade initiative remains one of the most prominent coalition attempts at a more sophisticated approach to counter-insurgency than clear-hold-build. I MEF did exactly what critics of presence prescribe: they used indigenous forces as a proxy for coalition ground troops, exploited technology, and lessened the sense of occupation by removing constant presence. It all failed.

Hit. The indirect approach met similar difficulties in Hit in 2004. Hit, with 110,000 residents, lies on the Euphrates between Ramadi and Al Qa'im. The 2d Battalion, 7th Marine Regiment (2/7) operated in Hit in early 2004.

After encountering minor resistance patrolling and receiving good cooperation from the city council, 2/7 made the progressive decision to focus on training the 503d ING Battalion. The Combined Action Program (CAP) platoon of 2/7 (42 Marines), augmented by 20 additional Marines, embedded with the 503d in late May 2004. Following in the footsteps of the highly effective CAP platoons of the Vietnam War, the Marines of 2/7's CAP platoon had a month of special training in Arabic, Arab culture, and Soviet weapons handling. It trained roughly 700 soldiers of the battalion and operated with them daily.[7] The CAP made a dramatic difference in ING performance. With the CAP, the battalion held and returned fire in 64 percent of engagements (May to October 2004), compared to 33 percent without the CAP (March to April 2004 and November 2004 to February

2005). Numerous Marine assessments in June and July found the 503d to be nearly ready for independent operations. Unfortunately, success was short-lived.

As hostilities escalated around Fallujah during the autumn, insurgents seized upon Hit as an alternative safe haven. Insurgents organized, massed, and fought a major battle with 1st Battalion, 23d Marine Regiment (1/23), 2/7's replacement, in October. Intimidated and bribed, the people looked the other way. Although temporarily defeated by the Marines, insurgents continued to flow into the city, and it became a major base of operations following the second battle of Fallujah. Marine officers described the insurgents as having free rein over the city.

The benefits of the CAP were not enough to enable the 503d to operate effectively amid large numbers of insurgents, who intimidated off-duty ING soldiers and overwhelmed isolated elements of the battalion. Soldiers increasingly quit because of threats, and they regularly abandoned posts attacked by car bombs and became ineffective on patrol. After September, no solid evidence existed that the battalion still stood and fought. During the October fighting in Hit, a subunit of the 503d working with 1/23 fled from positions defending the city bridge. The ING battalion commander could muster only 60 men to accompany the Marine counteroffensive into the city. Coalition airpower, which struck insurgent positions, supported the Marines and Iraqis in the battle, but this did not embolden the bulk of the ING battalion to fight. If the men fought, insurgents would kill them later. The situation worsened when the Marine battalion in Haditha moved to Fallujah in late October and 1/23 took responsibility for Haditha as well as Hit. Scarcity of forces restricted 1/23's ability to maintain a large number of advisors with the 503d. By the beginning of 2005, the 503d had essentially dissolved.

Hit provides another example of an indirect approach in Al Anbar. The 503d had coalition advisors, and coalition airpower was readily available. Nevertheless, the insurgent ability to mass superior numbers and intimidate crippled indigenous forces. The use of airpower did not alter the balance; the insurgents operated in a manner concealed from airstrikes.

Al Qa'im. Al Qa'im, which lies along the Euphrates River at the Syrian border, had a population of 110,000 in 2004. The Marines there initially adopted a clear-hold-build approach, flooding the urban areas with foot patrols, under the philosophy that presence would suppress insurgent activity and allow indigenous forces to develop. They abandoned this approach in the summer, however, because progress did not seem commensurate with steady casualties.

The lack of regular coalition presence allowed Abu Musab al-Zarqawi's organization, known as al Qaeda in Iraq (AQI), to concentrate in Al Qa'im and influence the area in late 2004. As AQI massed large numbers of foreign fighters arriving via Syria, Marines fought bigger and bigger firefights on the outskirts.

Concentration of AQI in Al Qa'im actually caused a local reaction. Tribes that had been fighting the coalition turned against AQI, most notably the Albu Mahal tribe. The Albu Mahal disliked AQI's treatment of civilians, importation of foreign fighters, and encroachment on their control of the black market. The tribe formed the "Hamza battalion," a tribal militia that actively defended Al Qa'im against AQI and initiated a unilateral ceasefire with coalition forces. The coalition apparently held an informal relationship with the Hamza battalion. According to a Marine spokesman, Iraqi informants helped find targets for coalition raids.[8] On one occasion, locals (presumed to be the Hamza battalion) fired on insurgents (presumed to be foreign fighters) attacking a Marine outpost.

Unfortunately, without being present in the city, the Marines could not ensure the survival of the Hamza battalion. AQI massed superior forces by turning to other local tribes and bringing in reinforcements, and they enforced strict Islamic law in areas outside Albu Mahal control and brutally intimidated anyone opposing them. Witnessing rising AQI strength, the other tribes cut a deal with Zarqawi and turned against the Albu Mahal.[9] The support of local tribes provided AQI with intelligence on the location of members of the Hamza battalion. In turn, the battalion lost intelligence on the location of AQI and its allies.

In early September, al Qaeda in Iraq defeated the Hamza battalion and seized Al Qa'im. With local support, AQI could move unseen to the Albu Mahal within the city and target relatively freely. It also enjoyed superior numbers and resources, having turned the other tribes against the Albu Mahal. The Hamza battalion had neither the men nor the arms to withstand persistent attacks. The Albu Mahal had become the minority opposition to AQI.

Coalition air support did not make a difference. The Marines conducted a series of airstrikes against AQI safe houses and in close support of the Hamza battalion. Those strikes reportedly killed over 50 insurgents, including at least 1 cell leader.[10] Airpower was probably ineffective due to the breadth and unconventional nature of the AQI attack. Ambushes, assassinations, and impromptu surprise attacks, rather than conventional tactics, characterized the AQI offensive. AQI mounted these attacks throughout the city, and it could not easily be targeted without having Marine squads and platoons present, especially in an urban environment in which AQI could move unseen among the population. Otherwise, the Marines would have needed to indiscriminately level sections of Al Qa'im with no regard for civilian casualties to stop the AQI advance. By September 5, AQI had taken over Al Qa'im, posting a sign that read, "Welcome to the Islamic Republic of Qa'im."[11]

The Hamza battalion is an example of the limitations of the indirect approach. An indigenous force had coalition air support and some degree of coordination with coalition ground forces yet could not defeat their opponents. Leaders in the Albu Mahal tribe believed that only direct coalition ground intervention could have turned the tide. After the battle, an Albu Mahal tribal leader expressed the need for a major clearing operation: "It would be insane to attack Zarqawi's people, even to shoot one bullet at them. . . . We hope the U.S. forces end this in the coming days."[12]

Why Did the Indirect Approach Fail?

The indirect approach experienced little success in reducing insurgent activity (particularly in terms of the size of attacks) and building human intelligence. Removing coalition forces from populated areas allowed insurgents to mass, control the population, and overwhelm local indigenous units. Insurgents would overwhelm indigenous units by either attacking subunits that had no advisors or intimidating off-duty personnel. Airstrikes could address neither. Advisors could not change the fact that local identity rendered soldiers and police highly vulnerable to intimidation. Indeed, soldiers in the 503d fled while operating alongside

Marines during the battle in Hit. Insurgents attacked, murdered, and kidnapped Iraqi soldiers and policemen, as well as their families. Intimidation is always a problem in counterinsurgency, but without coalition presence, insurgents enjoy total freedom to use it to coerce indigenous forces.

Popular support for the insurgency cannot be ruled out as a constraint on the indirect approach. General sympathy for the insurgency meant that certain local indigenous units, such as the Fallujah Brigade, had no intention of seriously fighting the insurgents. It also meant that groups who opposed the insurgency, such as the Albu Mahal, did not receive widespread support from other Sunnis. Advisors could not change Sunni sympathies.

The Clear-Hold-Build Approach

Despite numerous shortcomings, the clear-hold-build approach proved superior to the indirect approach. Two notable examples of the clear-hold-build approach were in Fallujah (November 2004 to August 2006) and Al Qa'im (November 2005 to August 2006). The clear-hold-build approach has also been applied in Hit (after June 2005), Haditha, Iskandariyah, Mahmudiyah, Karma, Khalidiyah, Nasser Wa Salaam, and Ramadi.

Fallujah. The saturation of Fallujah with coalition and Iraqi forces epitomizes the positive effects of the clear-hold-build approach. As noted above, the indirect approach failed in Fallujah following the first battle in April 2004. By November 2004, the coalition and Iraqi government agreed that Fallujah needed to be cleared. The strength of insurgent resistance and limited numbers of Iraqi forces left a direct approach as the only option. I MEF received two Iraqi brigades (five battalions) and one U.S. Army brigade (three battalions) to prosecute the offensive (Operation *Al Fajr*). The offensive could not have been conducted without these reinforcements. I MEF would have had to denude the rest of Al Anbar of forces to clear Fallujah. As it was, the 1st Marine Division sent two Marine battalions (plus Regional Combatant Team [RCT]–7 headquarters and other combat support elements) to join the three battalions of RCT–1 for the offensive. This left only a skeleton force covering the western desert and Ramadi. The overwhelming force combined with coalition firepower cleared Fallujah in pitched fighting in November and December, resulting in roughly 2,000 insurgent casualties and prisoners.[13]

After the battle, RCT–1 took responsibility for Fallujah with two Marine battalions and six Iraqi battalions. At that time, Iraqis were returning to the city. RCT–1 combined intensive patrolling with new population control measures. All residents returned via entry control points. Initially, vehicle traffic was restricted and a curfew was implemented. As the population grew from 5,000 to 100,000, RCT–1 enjoyed an overwhelming ratio of coalition/Iraqi forces per civilian. The population readily interacted with the Iraqi and coalition forces because they felt safe. Insurgents often fled the city, fearing that locals would inform on them. Throughout 2005, coalition and Iraqi army presence maintained security in Fallujah, allowing other essential elements of the counterinsurgency to move forward. Iraqi army units were able to develop their skills in a permissive environment and with the support of the Marine battalions. Every Marine battalion partnered with two to three Iraqi battalions, training and operating alongside them. The Marines slowly organized, trained, and deployed a local police force, which would prove competent in 2006. Presence mitigated the intimidation that had formerly sunk efforts to build a local indigenous force. Additionally, civil affairs officers and the State Department representative, Kael Weston, undertook an intensive engagement effort. They managed to get local leaders, most notably the imams, to endorse the Iraqi security force and elections. This effort resulted in high turnout for the January 2005 national election, October 2005 referendum, and December 2005 national election. In general, although they still opposed coalition occupation, a local city government and civil society developed that were averse to violence and preferred achieving their aims via political means.

ambushes, assassinations, and impromptu surprise attacks, rather than conventional tactics, characterized the al Qaeda in Iraq offensive

Al Qa'im. As noted above, coalition units had adopted an indirect approach in Al Qa'im in the summer of 2004. That approach persisted until November 2005, when coalition forces staged a major operation to clear Al Qa'im, known as Operation *Steel Curtain*. II MEF received substantial reinforcements to mount the operation because its own forces could not be shifted from the vital cities of Ramadi and Fallujah without unacceptable risk. Two Marine infantry battalions and one Iraqi brigade assaulted the city and then established a permanent presence. The assault cleared out AQI elements. With AQI defeated, the Albu Mahal tribe enjoyed a permissive environment to enforce security with the Marines.

The 3d Battalion, 6th Marine Regiment (3/6) adopted an aggressive plan for maintaining presence. Rather than minimizing contact with locals, they maximized it: Marines integrated thoroughly with the Iraqi army brigade and dispersed in small subunits throughout the city. Every platoon lived and worked with an Iraqi platoon in an outpost in the area. The battalion established a dozen outposts. The platoons conducted intensive satellite patrolling day and night. Living close to the population generated intelligence and forced the Marines to learn how to interact with the locals. The population accepted the Marine and Iraqi presence, probably because the Albu Mahal supported the Marines, not wanting foreign fighters to return. Marines could move about freely, even purchasing food from local markets.

With sustained presence and the support of the Albu Mahal tribe, the coalition recruited large numbers of police and soldiers. AQI could no longer effectively intimidate locals. Within 3 months of the completion of Operation *Steel Curtain*, 400 locals had become police. By the summer of 2006, a working police force existed of roughly 850 men, largely from the Albu Mahal tribe. Additionally, locals readily joined the Iraqi brigade, which boasted more Sunnis than any other brigade in the Iraqi army. Partnership with the Marine battalion and the benign operating environment allowed the brigade's skills to be developed slowly.

Effectiveness

These cases demonstrate the effectiveness of the clear-hold-build approach over the indirect approach in Al Anbar. Similar trends pertain to other cases, with only Ramadi varying from the pattern. The clear-hold-build approach reduced large-scale insurgent activity because patrols, ambushes, and outposts inhibited insurgent freedom of movement. Coalition and, more importantly, Iraqi forces enjoyed a more permissive

operating environment; insurgents could no longer overrun police stations, run their own checkpoints, train and organize en masse, or directly control the population. Presence mitigated intimidation as well, though it remained a problem. Shi'a forces could operate effectively in this environment, and local Sunni forces could survive with great effort.

Additionally, contrary to proponents of the indirect approach, presence *improved* the coalition relationship with the population. Iraqis became more willing to interact with the coalition as presence restricted insurgent freedom of movement and mitigated intimidation. Intelligence improved and local governments formed. Most importantly, more Sunnis agreed to join indigenous forces.

Limitations

Notwithstanding its strengths, the clear-hold-build approach had four significant limitations. First, it demanded substantial numbers to saturate a city and control the population. Success in Al Qa'im and Fallujah only occurred after operations involving 5 to 10 coalition and Iraqi battalions. Over time, insurgent tactical adaptation meant that more and more forces were needed to secure a given area. The effects of insufficient forces have been most notable in Ramadi, which I MEF tried to secure for most of 2004 with a single Marine battalion. One battalion proved unable to control the city of 450,000. The coalition added battalions from late 2004 to mid-2006, but even the major operation by I MEF in the summer of 2006 lacked sufficient forces. At that point, five coalition and six Iraqi battalions could still not clear the city; insurgents had begun to develop better tactics to survive amid coalition presence, reducing the marginal benefit of each battalion. I MEF's higher headquarters could not find enough forces for the clear-hold-build approach to succeed.

Second, the clear-hold-build approach could not entirely suppress insurgent activity. Small incidents and intimidation persisted. This is not surprising. Historically, car bombs, roadside bombs, and murders can last throughout an insurgency, including one near defeat. Military operations in urban areas had difficulty capturing one to four men laying a roadside bomb or driving a car bomb. Even in Fallujah in 2006, roadside bombs, sniper attacks, and occasional suicide bombings occurred as insurgents tried to reassert influence. Nevertheless, the clear-hold-build approach suppressed insurgent influence sufficiently for local forces to develop and reconstruction to occur.

Third, units employing the clear-hold-build approach suffered higher casualties than those employing an indirect approach. Intense urban operations incurred steady casualties from roadside bombs, small arms fire, and car bombs. Casualties wore on units and challenged long-term presence.

Fourth, while improving the relationship with locals, the clear-hold-build approach never won them over. After 6 to 12 months, locals grew tired of the constant coalition patrolling, raids, outposts, and checkpoints. They preferred not to see Americans. Moreover, clearing operations, such as the first battle of Fallujah, second battle of Fallujah, the entry into Haditha, and Operation *Steel Curtain*, caused civilian casualties, which sometimes outraged Sunnis. If the coalition had not built Iraqi political support or taken measures to mitigate civilian casualties, the operation could even have been called off, as in the first battle of Fallujah. The negative effects of the clear-hold-build approach on public support for the coalition and Iraqi government should not be overrated. Presence did not upset locals enough to generate higher levels of attacks. Local relationships were better with large numbers of coalition forces operating amid the population than away from it, as under the indirect approach.

every Marine battalion partnered with two to three Iraqi battalions, training and operating alongside them

Iraqi police patrol in Ramadi

1st Marine Logistics Group (Gabriela Garcia)

This article has examined whether operations involving few coalition forces (the indirect approach) would have produced better results in countering the insurgency in Al Anbar than operations involving substantial forces (the clear-hold-build approach). The answer appears to be *no*. The indirect approach was not a viable alternative because insurgent numbers and the ability to intimidate could cripple indigenous forces. The problem was worsened by the fact that most Sunnis refused to work with coalition forces out of sympathy for the insurgency. Nor did the absence of coalition forces win Sunni hearts and minds and magically produce indigenous forces. Rather, it merely left the local recruit base under insurgent control.

units employing the clear-hold-build approach suffered higher casualties than those employing an indirect approach

As the war progressed, the potential for the indirect approach increased. With insurgent dominance broken in Fallujah, and then Hit and Al Qa'im, indigenous forces with small advisory teams could operate effectively without the presence of coalition battalions in certain areas. The removal of direct insurgent control meant that a critical mass of recruits was available to form local Sunni units. Additionally, the arrival of predominantly Shi'a Iraqi army battalions (totaling two divisions by 2006) improved the prospects of an indirect approach by offering more steadfast soldiers. That said, the key point is that the indirect approach became viable only after sustained coalition presence.

The inability of the indirect approach to counter the insurgency in Al Anbar argues against the idea that the United States could have succeeded in Iraq without deploying more forces. Rather than lessening the insurgency, fewer forces *fanned* it. Scarcity of forces was the major inhibiting factor on the employment of the clear-hold-build approach. Presence in the key cities of Fallujah and Al Qa'im could not have been established without substantial reinforcements from outside Al Anbar. In other words, even the oil slick method of concentrating in key cities and then expanding outward was infeasible, unless the coalition wanted to abandon Al Anbar entirely and focus on Baghdad. The deployment of a larger number of forces in 2003 or 2004 might have lessened the insurgency in Al Anbar, and perhaps Iraq as a whole. The clear-hold-build approach witnessed similar success elsewhere in Iraq—such as in Mosul and Tal Afar—while the removal of the clear-hold-build approach witnessed similar failure—such as in Baghdad and Samarra.

What does it matter that the United States needed to send more forces to Iraq? As Americans increasingly question the odds of success in Iraq, the comparison between the clear-hold-build approach and the indirect approach sheds light on the effects of pulling coalition forces back from populated areas or withdrawing from Iraq entirely. Some advocates of the indirect approach have been calling for its implementation as an alternative to the surge strategy of 2007. Other opponents of the surge are now calling for outright U.S. withdrawal. The answer is not as clearly in favor of maintaining a substantial presence as one might think. The reinforcement of coalition forces in Ramadi in 2006 delivered lackluster results. Furthermore, the indirect approach has now witnessed success in certain areas. Nevertheless, the situation absent coalition forces has usually been far more violent than when those forces have been present. Consequently, it would be reckless to presume that a reduction in forces will not be followed by an increase in violence. Given historical precedent, the United States should expect hardcore insurgent groups, such as AQI, to gain influence in the wake of a reduction in U.S forces, if not to dominate Al Anbar and other Sunni areas. It would also not be surprising if Iraqi army and police units suffered setbacks. Even if the surge succeeds, U.S. decisionmakers need to realize that reducing forces prematurely stands a good chance of forfeiting hard-won gains. These forecasts are not meant to endorse a U.S. strategy of staying the course but to provide a full understanding of the implications of reducing forces. **JFQ**

NOTES

[1] Michael Gordon and Mark Mazzetti, "General Warns of Risks in Iraq if G.I.'s Are Cut," *The New York Times*, November 16, 2006; Steven Metz and Raymond Millen, *Insurgency and Counterinsurgency in the 21st Century: Reconceptualizing Threat and Response* (Carlisle, PA: Strategic Studies Institute, 2004), 32; Lawrence Freedman, "Rumsfeld's Legacy: The Iraq Syndrome?" *The Washington Post*, January 9, 2005.

[2] James T. Quinlivan, "Force Requirements in Stability Operations," *Parameters* 25 (Winter 1995–1996), 59–69.

[3] On counterinsurgency, see John Nagl, *Learning to Eat Soup with a Knife: Counterinsurgency Lessons from Malaya and Vietnam* (Chicago: University of Chicago Press, 2005); Frank Kitson, *Low Intensity Operations: Subversion, Insurgency, Peace-keeping* (Harrisburg, PA: Stackpole Books, 1971); Robert Thompson, *Defeating Communist Insurgency: The Lessons of Malaya and Vietnam* (New York: Praeger, 1966); Field Manual 3–24, *Counterinsurgency* (Washington, DC: Department of the Army, December 2006).

[4] Melvin Laird, "Iraq: Learning the Lessons of Vietnam," *Foreign Affairs* 84, no. 6 (November/December 2005), 28–29; Charles Dunlap, "The Asymmetric Advantage," *Armed Forces Journal* (September 2006); and Thomas E. Ricks, *Fiasco: The American Military Adventure in Iraq* (New York: Penguin Press, 2006), 192, 301.

[5] John Murtha, press release, November 17, 2005, available at <www.house.gov/list/press/pa12_murtha/pr051117iraq.html>.

[6] This group was known as the Iraqi Civil Defense Corps at the time. In June 2004, its name changed to the Iraqi National Guard.

[7] Philip Skuta, "Partnering with Iraqi Security Forces," *Marine Corps Gazette* (April 2005), 36–39; Jason Goodale and Jon Webre, "The Combined Action Platoon in Iraq," *Marine Corps Gazette* (April 2005), 40–42.

[8] Hannah Allam and Mohammed al Dulaimy, "Iraqis Lament Call for Help," *Philadelphia Inquirer*, May 17, 2005.

[9] Christopher Allbritton, "Making Tribal War Work for the U.S. in Iraq," *Time*, November 8, 2005.

[10] Ellen Knickmeyer and Omar Fekeiki, "U.S. Warplanes Target Alleged Rebel Havens Along Iraq-Syrian Border," *The Washington Post*, August 31, 2005.

[11] Ellen Knickmeyer and Jonathan Finer, "Insurgents Assert Control over Town near Syrian Border," *The Washington Post*, September 6, 2005.

[12] Ibid.

[13] John Sattler and Daniel Wilson, "Operation *Al Fajr*: The Battle of Fallujah—Part II, Dousing the Bright Ember of the Insurgency," *Marine Corps Gazette* (July 2005).

COMBATING TERRORISM WITH SOCIOECONOMICS

Leveraging the Private Sector

BY MIEMIE WINN BYRD

U.S. Army (Robert Brogan)

State Department representatives meet with Iraqi Ministry of Agriculture to discuss farming conditions in Salah Ad Din Province in Iraq

Fleet Combat Camera (Troy Latham)

General Martin Robeson, USMC, speaks in Basilan about U.S.-Philippine humanitarian mission there

It is widely recognized that leaders of terrorist organizations come from the ranks of the educated and are mostly driven by extremist ideologies. The foot soldiers of terrorism, however, are often recruited from the deprived masses at the bottom of the socioeconomic and political pyramid. The leaders exploit impoverished and hopeless environments and circumstances to attract the large numbers of people needed to advance their agendas.[1]

Recently, the U.S. Army War College hosted a conference on the underlying conditions of terrorism and the military role in addressing these conditions. The participants agreed that the U.S. military has been successful in its efforts to attack and disrupt key terrorist organizations since 9/11; however, these organizations are able to replenish their ranks faster than we can reduce them because "poverty and inequality still prevail in many parts of the Muslim world with high illiteracy rates, lack of human development, and poor infrastructure."[2] Moreover, the "center of gravity for war and terror are the populations that can provide sanctuaries, safe havens, and/or recruitment for terrorists."[3] These conditions are pervasive throughout the Asia-Pacific region.

According to Asian Development Bank statistics, for example:[4]

- The Asia-Pacific region is home to two-thirds of the world's poor.
- Nearly 1.9 billion people in the region live on less than US$2 a day.
- At least 30 percent of the population in countries such as Cambodia, Laos, the Philippines, and Vietnam still live in extreme poverty.
- A conservative estimate of Asian unemployment is 500 million, and 245 million new workers are expected to enter the labor markets over the next decade.

Millions of Muslim boys in Asia are coming of age and creating a "youth bulge." When governments are not able to deliver a vision of hope, mutual respect, and opportunity, these young men end up desperate, frustrated, and humiliated. These are ripe conditions for religious extremism, which can provide a perversely attractive escape from the grinding hopelessness and despair.[5]

According to Lieutenant General Wallace Gregson, former commander, U.S. Marine Forces Pacific, the decisive terrain of the war on terror is the vast majority of people not directly involved, but whose support, either willing or coerced, is necessary to insurgent operations around the world.[6] This populace is equivalent to American swing voters, whose ballots have contributed significantly to the outcome of many U.S. Presidential elections. As President Ronald Reagan said during the midst of the Cold War, we have to turn these potential enemies into friends.

Thus, it is crucial for U.S. Pacific Command (USPACOM) to develop a concept of operations to alleviate these conditions. Since the launch of Operation *Enduring Freedom–Philippines* in 2002, the island of Basilan, where a reign of terror had ruled since the early 1990s, has achieved a secure environment. However, as we have seen in Iraq, this success will be short-lived if the local, state, and central governments are unable to provide a sustained secured atmosphere and meet the expectation of the populace. In a recent interview, Lieutenant General Peter Chiarelli, USA, commander of Multinational Corps in Iraq, stated, "If we don't follow up with a build phase, then I don't think Baghdad can be secure." The same article pointed out:

Major Miemie Winn Byrd, USAR, is Deputy Economic Advisor for U.S. Pacific Command.

The imperative to provide economic benefits to ordinary Iraqis is not born out of some vague humanitarian impulse, U.S. military officials [in Iraq] *emphasize, but one that directly affects the security of the country and the viability of the government.*[7]

Although Basilan has made great strides in achieving better economic conditions in recent years, poverty and lack of opportunity are still pervasive. Therefore, our long-term counterterrorism efforts by, through, and with the government of the Philippines must focus on creating sustainable socioeconomic conditions on Basilan island.

Applying Principles of War

To put this concept in terms of a principle of war, this is equivalent to conducting an exploitative offensive operation following a successful attack. Exploitation takes advantage of tactical opportunities gained by the initiative. It pressures the enemy and compounds his disorganization.[8]

Creating sustainable socioeconomic conditions should be viewed as an exploitative offensive operation. We conduct this type of operation by shaping, changing, and maintaining the popular support for the armed forces of the Philippines and its government on Basilan. How do we maintain long-term popular support for our cause—that is, how do we deny popular support for the terrorist organizations? We do so by encouraging socioeconomic development that creates jobs, opportunities, and alternatives to violent extremism.

Network of Stakeholders

The U.S. military alone does not have the skills or resources to create sustainable socioeconomic development. This type of operation requires an extensive network of stakeholders: the host-nation government (including the military), local populace, international organizations, nongovernmental organizations, private sector, academia, and the U.S. Government (including the military). To attract all the necessary stakeholders, we need to activate the interagency process because the core competency needed for this phase lies in other Federal agencies, such as the Department of Commerce, the Department of State's Bureau of Economic and Business Affairs and Coordinator for Reconstruction and Stabilization, and the U.S. Agency for International Development (USAID).

citizen-Soldiers can open doors to the business community as we develop the nontraditional network and partnerships

However, the Department of Defense (DOD) should and could be a proactive member of this interagency team.

Building this nontraditional network of stakeholders with varying interests and organizational cultures will be an arduous task. Therefore, all interagency players, including the military, must think and act outside the box. The Quadrennial Defense Review Execution Roadmap published in May 2006 directed DOD to develop a long-term, focused approach to build and increase the capacity for the international partners to deny sanctuary to terrorists and to separate terrorists from populations by utilizing all instruments of national power. To do so, DOD was authorized to partner and cooperate with:

- other departments and agencies of the U.S. Government
- state and local governments
- allies, coalition members, host nations, and other nations
- multinational corporations
- nongovernmental organizations
- the private sector.

Leveraging the Private Sector

DOD does not have to look far to reach into the private sector. The U.S. military employs thousands of Reserve and Guard citizen-Soldiers, Sailors, Airmen, and Marines who work in the private sector. Many of them hold significant decisionmaking positions with multinational corporations and regional and small firms. Many have valuable skills in such fields as public relations, marketing, business development, supply-chain management, finance, economics, agribusiness, and investment banking. We need to tap into not only this wealth of skills from these citizen-Soldiers, but also their relationship with the business community. They can open many doors to the business community as we develop the nontraditional network and partnerships.

The story of Lieutenant Colonel Allen McCormick, USAR, demonstrates the power of our Reserve and Guard members as invaluable assets already embedded inside the U.S. military. McCormick, an Army Reserve officer with Special Operations Command, Pacific (SOCPAC), is a brand manager who leads marketing campaign developments for Procter & Gamble in Cincinnati. He holds a Masters of Business Administration from Webster University.

While participating in an exercise at Camp H.M. Smith, Hawaii, in September 2006, McCormick heard about the USPACOM initiative to partner with the private sector. He quickly put us in touch with the appropriate point of contact at Proctor & Gamble, and we are communicating with the company to explore how it can collaborate with USPACOM in Indonesia. Proctor & Gamble has been working on water purification products to be marketed in developing countries such as Indonesia and the Philippines. They also collaborated with USAID and the Centers for Disease Control during the relief efforts after the tsunami of late 2004. Lieutenant Colonel McCormick is teaching SOCPAC to apply commercial marketing methods to trigger, diffuse, and measure the penetration of messages in "word-of-mouth" cultures to counter extremist messages.

Also, there is a remarkable phenomenon of new thinking gaining ground within the business community. The concept of eradicating poverty through profits involves ways that businesses can gain advantage in today's highly competitive global environment by servicing the needs of those who are at the bottom of the socioeconomic pyramid. By doing so, they trigger sustainable economic growth in those areas. Peace through commerce enhances the powerful role that commerce plays in promoting peace. According to *The Wall Street Journal*, many U.S. business schools are adopting the new mission of promotion in this way.[9] The Association to Advance Collegiate Schools of Business (AACSB), which accredits business schools around the world, has assembled a program called Peace through Commerce, with the aim of raising awareness about what business schools can do to promote peace. Michael Porter, a professor at Harvard Business School and a leading authority on competitive corporate strategy, stated:

it is becoming more and more apparent . . . that treating broader social issues and corporate strategy as separate and distinct has long been unwise [and] *never more so than*

Meeting with members of International Red Cross in Baghdad

U.S. Air Force (Cherie Thurlby)

today. . . . [W]*e are learning that the most effective way to address many of the world's most pressing problems is to mobilize the corporate sector. . . . In modern competition, economic and social policy can and must be integrated. . . . Not only can corporate and social needs be integrated, but the success of the developing world in improving prosperity is of fundamental strategic importance to almost every company.*[10]

We must tap into and harness this new thinking. A recent strategy paper published by the Department of State's Bureau of Economic and Business Affairs stated that it is trying to explore ways that the private sector can help eradicate the underlying conditions that terrorists exploit.[11] The bureau convened a meeting in September 2006 to discuss this initiative, and USPACOM was asked to participate as a member of the interagency community. This meeting demonstrates that the U.S. Government is beginning to accept the idea of engaging the private sector and recognizing the untapped resources and capabilities that the business community possesses.

Military partnership with the private sector is not a new concept. Close cooperation at both the political and technological level gave the United States an advantage during World War II in aviation, communication, and radar developments.[12] Civilian-military collaboration was a critical ingredient for innovations necessary for America to gain an advantage over the enemy. Specific circumstances for including the private sector may be different today, but the concept is the same. The private sector has the capabilities, skills, resources, and innovations to solve the underlying socioeconomic conditions that foster terrorism.

Beyond Economics

While this article focuses primarily on the sustainable economic development and partnering with the private sector, it is not suggesting that this approach is a universal solution. The purpose is to bring attention to the importance of the economic element in shaping and changing the environment as we prosecute the war on terror. Other strategic elements—diplomatic, informational, and military—cannot be dismissed. An economic development can begin to occur only when basic security and physical needs are met. Efforts toward improved infrastructure (such as transportation systems, power, water, and telecommunications), developed human/social capital (health care and education), and good governance (to include sound macroeconomic policies) are the prerequisites for a continuous and sustained economic development. Enduring development strategies require equity, populace participation, and ecological preservation.[13] Therefore, the capabilities and interests of other stakeholders, in addition to the military and the private sector, are still needed to develop and maintain the foundation for sustainable economic development.

To initiate this process of engagement with the various stakeholders, a series of meetings may be warranted. These gatherings should facilitate an environment for these diverse organizations to explore and understand each other's organizational goals, capabilities, and requirements. By holding them, we hope to overcome organization-level cultural biases, build trust, and develop working relationships to generate synergy among the participating organizations. The military role within the network would be to facilitate the gatherings, point out the areas that are most vulnerable to terrorist recruitment, and provide assessments of the security situation in specific locations, such as the island of Basilan. A unified vision and situational awareness among the participants would be the expected outcome from these gatherings.

In addition to sponsoring the meetings, we need to attend private sector roundtables, such as AACSB annual meetings, Business Executives for National Security board meetings, conferences sponsored by the Institute for Defense and Business, FLOW (a grass-roots global network of entrepreneurs practicing conscientious capitalism for sustainable peace) networking events, and the Global Microcredit Summit. We need to let the private sector know that the U.S. Government and international community need their business expertise in creating products, services, and jobs for those who are at the bottom of the socioeconomic pyramid. By doing so, they can create hope and opportunities for the populace as well as additional markets for their products and services. The byproduct is creating environments inhospitable to violence and terrorism.

Beyond the Basilan Model

The success of Operation *Enduring Freedom–Philippines* has been attributed to the Basilan model, which built host-nation capacity, met basic physical needs of the local populace, enhanced Filipino government legitimacy and control, and disrupted insurgent safe havens. The emphasis on civil-military operations resulted in improved infrastructure, increased availability of water, and secured mobility for commerce. Therefore, this model was extremely effective in winning back public support and improving security in Basilan by reducing terrorist strongholds. It also laid the cornerstone for the beginning of social and economic prog-

ress in Basilan, but more work is needed for sustainable socioeconomic development.

Since 2002, the U.S. military, USAID, local and international nongovernmental organizations, and the government of the Philippines have been working together. We need to expand this network to include additional stakeholders, such as private businesses, multinational corporations, local and international investment firms, local and international financial institutions, and academe to build the capacity of the local populace and of the host-nation government.

For example, the Asian Development Bank initiated a process to cultivate a strategy for the Philippines to achieve long-term sustainable economic growth. In March 2005, the bank hosted the Philippines Development Forum, which was a meeting of the Philippines Consultative Group and other stakeholders. The forum addressed development issues and other factors, such as instability, weak infrastructure, an inefficient financial sector, corruption, large bureaucracy, and extensive national debt. The group recognized that the private sector accounted for 86 percent of gross domestic product and is responsible for the majority of job creation. Accordingly, it is the key to sustainable economic development.

We should leverage the Asian Development Bank's ongoing efforts and synchronize our plans, programs, and activities with them and facilitate the further expansion of the stakeholders' network. We should also leverage its expertise, interests, goals, and resources toward creating sustainable social and economic progress in Basilan. That island and the Philippines in general could be the next success story in the same line as Ireland, which was one of the poorest countries in Europe 15 years ago. Evidence shows that the unprecedented economic growth there had significant impact on reducing violence in Northern Ireland, which was considered the most violent region of northern Europe for the previous 40 years. In 20 years (1986 to 2006), unemployment declined from 17.6 percent to 4.5 percent.[14] Ireland's steady economic growth was led by private sector businesses.

It is crucial that we expose a critical mass of international business sector players to Basilan. As always with new startup investments and companies, the risk is extremely high, so the failure rate could be high also. Therefore, attracting a critical mass of private sector players, maintaining the network, and preserving their interests are the keys to netting a handful of successful new ventures and a steady stream of new investments.

economic development can begin to occur only when basic security and physical needs are met

A Horizontal World

A big challenge for the U.S. military would be to overcome its need for control. It is embedded in our organizational DNA to want to run things because military organizations are traditionally hierarchical and have a top-down structure. We must recognize that the military will be unable to exercise any control over the actions of its nonmilitary partners. We have to inspire them into collaborating with us. Hierarchical relationships are dissolving and more horizontal and collaborative ones are emerging within businesses, governments, and many organizations across the spectrum.[15] Therefore, success depends on how well we are able to influence and persuade them to help us. This can only be accomplished if we truly take the time and effort to understand their requirements, interests, and concerns. This is where we could leverage our Reserve and Guard members of the Armed Forces. **JFQ**

Representatives of the United Nations, USAID, and other agencies meet onboard the USS *Abraham Lincoln* to coordinate aid to Aceh, Indonesia, after tsunami disaster

U.S. Navy (Elizabeth Edwards)

NOTES

[1] Jesus Felipe and Rana Hasan, *The Challenge of Job Creation in Asia*, ERD Policy Brief Series No. 44 (Manila, The Philippines: Asian World Development Bank, April 2006), available at <www.adb.org/Documents/EDRC/Policy_Briefs/PB044.pdf>.

[2] Statement by Datuk Seri Abdullah Ahmad Badawi, Prime Minister of Malaysia.

[3] Kent H. Butts, Terry Klapakis, and Art Bradshaw, *The Military's Role in Addressing the Underlying Conditions of Terrorism*, Issue Paper (Carlisle Barracks, PA: U.S. Army War College, June 2006), 2, available at <http://www.carlisle.army.mil/usacsl/Publications/IP05-06.pdf>.

[4] Felipe and Hasan.

[5] Stuart Hart, *Capitalism at the Crossroads: The Unlimited Business Opportunities in Solving the World's Most Difficult Problems* (Philadelphia: Wharton School Publishing, 2005), 215.

[6] Wallace C. Gregson, "Ideological Support: Attacking the Critical Linkage," in *The Struggle Against Extremist Ideology: Addressing the Conditions That Foster Terrorism* (Carlisle Barracks, PA: U.S. Army War College, 2005), 22.

[7] Linda Robinson, "The Battle for Baghdad," *U.S. News and World Report*, September 5, 2006, 56.

[8] Field Manual 3–0, *Operations* (Washington, DC: Department of the Army, June 2001), 7–22.

[9] Rhea Wessel, "Business School's New Mission: Promoting Peace," *The Wall Street Journal*, June 2, 2006.

[10] World Resource Institute, *Tomorrow's Markets: Global Trends and Their Implications for Business* (Baltimore: World Resource Institute, 2002).

[11] Department of State's Bureau of Economic and Business Affairs, *Using Economic Power to Combat Terrorism* (Washington, DC: Department of State, September 2006).

[12] Allan R. Millett, "Pattern of Military Innovation," in *Military Innovation in the Interwar Period*, ed. Williamson R. Murray and Allan R. Millett (Cambridge: Cambridge University Press, 1998), 365.

[13] Robin Broad, John Cavanagh, and Walden Bello, "Development: The Market Is Not Enough," in *International Political Economy: Perspectives on Global Power and Wealth*, ed. Jeffry A. Frieden and David A. Lake, 3d ed. (New York: St. Martin's, 1995), 397.

[14] Michael Strong, "Understanding the Power of Economic Freedom to Create Peace," available at <www.flowproject.org/Downloads/Economic-Freedom-and-Peace.pdf>.

[15] Thomas L. Friedman, *The World Is Flat: A Brief History of the Twenty-first Century* (New York: Farrar, Straus and Giroux, 2005), 45.

Joint Ground Logistics in the Falklands

By RAYMOND E. BELL, JR.

June 14, 2007, marked the 25th anniversary of the recapture of the Falkland Islands by a British joint task force. The victory was a spectacular exhibition of military power by the United Kingdom's professional armed services, which had to overcome many unique and difficult challenges on the ground, at sea, and in the air. The principal land battle was fought on East Falkland Island, where most of the islands' population and settlements, major seaport and airfield, and government center and town of Stanley are located.

The British land campaign lasted for only 3 weeks, from May 21 to June 14, 1982. The fighting ended with the surrender of the Argentines after a 3-day battle for the major objective, the Argentine defenses concentrated in the hills around Stanley, the port, and the airfield.

Overshadowed by international negotiations and combat operations of the campaign, however, was the key role joint ground logistics played in this short war. An impressive sea movement over 8,000 miles placed two reinforced infantry brigades, one each from the British army and the Royal Marines, in position to fight an Argentine military contingent of some 13,000. The British troops, eventually amounting to approximately 10,500, were presented with such major logistic challenges once ashore that, at the end of campaign, it was agreed by British combatants that the victory was a "close run thing."

Limiting Physical Factors

Logistic support for the Falkland Islands campaign was framed by significant factors, including the distance from the United Kingdom, the harsh, unpredictable weather of the approaching winter, and particularly the islands' geography. The terrain of East Falkland Island consists not only of large

Royal Marine Commandos march toward Port Stanley in the Falklands

Imperial War Museum

plains filled with peat bogs and stone runs (vast stretches of various sized rocks) but also rugged mountains. The coastline of the island is a continuum of coves, small bays, larger sounds, and beaches with varying degrees of accessibility. There are no major rivers, but there are streams of varying depth and width. The peat bogs provide the islanders with their fuel in winter as there are no trees for burning. The bogs are difficult to traverse because the water table is only about a foot beneath their surface, making them spongy.

As for movement over the island terrain, large vehicles have a difficult time, and islanders motor about using small tractors and four-wheel-drive vehicles. The British, based on prior knowledge of the terrain, brought no large-wheel vehicles to provide overland logistic support. The British troops, however, found that their tracked vehicles, because of their low ground pressure, were able to move over the bogs with relative ease.

If the terrain was not challenging enough, the weather made the campaign even more arduous. June is the middle of winter in the Southern Hemisphere, and the combatants could not have been thrust into battle at a worse time. The British came to the Falklands during their own summer, which may have influenced the thinking of those responsible for outfitting the soldiers for battle. The Royal Marine commandos, having exercised often in Norway, came better prepared than the Guardsmen, who had to use political influence to obtain funds for purchasing adequate cold weather clothing and gear.

The first suggestion of bad weather conditions the ground combat force encountered was at sea. Although that year's Falklands' winter was to prove relatively mild, the temperatures and winds still did not auger well. Ships sailing south in April encountered temperatures of -3 Celsius and 55-knot winds with a wind chill of -15 Celsius.

Once on land, the ground troops suffered in frequent cold rain squalls, bitter hail, sudden snow showers, fine drizzle, enveloping mists, and dense fog. Among these weather difficulties were the sharp winds with their adverse effects on helicopters transporting heavy sling-loaded artillery ammunition pallets. Yet some days brought brilliant sunshine and calm winds, which helped Argentine aircraft locate and attack British ships and ground troops. With autumn fast giving way to winter, the weather became altogether unpredictable.

Finally, there was the impact of the distance from the United Kingdom to the Falklands, which affected logistic operations. Timely resupply of large items of equipment was impossible because of the thousands of miles separating Great Britain from the islands. Small items and critical personnel could be flown to the theater of operations, but movement by ship took weeks.

The Commando Logistic Regiment

The British organization charged with the logistical support of the ground forces was the Commando Logistic Regiment (CLR) of the Royal Marines 3 Commando Brigade, which was supplemented by helicopters, naval landing craft, and later in the campaign elements of three British army logistical units. The regiment was the base for logistical support to the ground forces involving amphibious operations.

Brigadier General Raymond E. Bell, Jr., U.S. Army (Ret.), served in the New York Army National Guard and commanded the 5th Psychological Operations Group and 220th Military Police Brigade in the U.S. Army Reserve. He was on the staff and was a faculty member at the National Defense University from 1982 to 1985.

At first glance, it would appear that the CLR was as large as what the U.S. Army formerly considered a division support command capable of providing logistical support for up to 11 maneuver battalions, plus artillery, engineer, signal, aviation battalions, and other units. But in the British force structure, such an organization as the CLR is only of U.S. battalion size.[1] Under normal operating procedures, the regiment would have only supported three Royal Marine commandos (also battalion size) and the Royal artillery's commando regiment plus an assortment of other small organic units composed of commando-qualified personnel.[2]

What was significant about the CLR force structure was that it was a true joint organization. The commander of the regiment in the Falkland Islands was a commando-qualified British army lieutenant colonel of the then–Royal Corps of Transport. The medical squadron of the regiment, commanded by a Royal Navy surgeon commander, had among his subordinate elements an army parachute clearing troop and Royal Navy surgical support teams. The three other CLR combat service support elements were a reduced transport squadron of the Royal Corps of Transport,[3] a workshop squadron (equivalent to a U.S. ordnance company) of the Royal Electrical and Mechanical Engineers, and an ordnance squadron (equivalent to a U.S. quartermaster company) of the Royal Army Ordnance Corps. The squadrons were manned by a combination of Royal Marine commandos and commando-trained British army personnel.

The CLR was the key to enabling eight infantry battalions, two artillery battalions, a reinforced engineer battalion, numerous aviation units, and a number of smaller units to defeat a division-size Argentine land force.

Helicopter and Naval Landing Craft Support

The 3 Commando Brigade had no organic medium or heavy lift helicopter elements. The brigade's air squadron consisted of nine Gazelle and six Scout light helicopters that were employed principally for command, control, reconnaissance, liaison, and evacuation of wounded. These helicopters, although called upon to deliver small amounts of ammunition in the battle for Goose Green, were inadequate for moving large loads of ammunition, heavy equipment, supplies, and troops.

The aerial logistic burden fell on the Royal Air Force and Royal Navy Chinook, Sea King, and Wessex helicopters that were deployed to the region. Unfortunately, the loss of three of the four Chinook heavy lift helicopters and six Wessex helicopters placed a huge strain on the remaining helicopter lift assets. The limited number of heavier lift helicopters, for example, often led to "hijacking" or improper diverting of helicopters from their assigned missions to other, possibly less critical missions. This seriously complicated mission planning and allocation of assets where they were most needed.

The mix of helicopters showed a joint image. The one Chinook that carried a tremendous burden in the logistic effort belonged to the Number 18 Squadron of the Royal Air Force. Demonstrating its air worthiness, the helicopter was constantly in use and lifted loads that often exceeded design limits. It was particularly valuable in moving the artillery pieces and heavy artillery ammunition pallets. The Wessex helicopters belonged to the Royal Navy's 845, 847, and 848 Naval Air Squadrons (NAS). The helicopters were capable of transporting troops and lesser loads of supplies and equipment. The larger Sea King helicopters also belonged to the Royal Navy. Three squadrons of Sea Kings (824, 825, and 846 NAS) proved to be the standard work horse in the logistic effort.

the British came to the Falklands during their own summer, which may have influenced those responsible for outfitting the soldiers

For naval watercraft ship-to-shore and shore-to-shore operations, the Royal Navy had three types available: eight landing craft vehicle and personnel, eight landing craft mechanized (LCM),[4] and six manned landing ships logistic (LSL). These latter ocean-going vessels transported large amounts of equipment and supplies along with significant groups of personnel. But the Royal Navy was not the only armed service to furnish watercraft. The Royal Marines moved limited supplies and troops on small fiberglass Rigid Raiders and rubber Geminis. The British army's Royal Engineers brought their high-speed combat support boats that operated as general harbor support craft. The Royal Corps of Transport's 51 Port Squadron of 17 Port Regiment operated a float raft system called the Mexejlote, a type of pontoon or barge used to move heavy equipment from ship to shore.

British Strategy and Tactical Operations

The British strategy called for isolating the battlefield by establishing a "total exclusion zone" (TEZ) to shipping around the islands, creating a standoff anchorage area for unarmed and combatant ships, conducting diversionary operations on West Falkland Island, and landing on the west coast of East Falkland Island. Initially, the tactical plan was to establish a presence on the island for negotiation purposes. But when negotiations broke down, the plan was changed to an overland advance on Stanley and the defeat of the Argentine force there.

On May 21, 1982, 3 Commando Brigade, reinforced by the 2d and 3d Battalions of the Parachute Regiment, made an unopposed landing on the west coast of East Falkland Island in the large sound called San Carlos Water. The brigade proceeded to establish a beachhead and started a buildup of supplies with the CLR setting up a beach support area (BSA) to administer the logistic effort.

The Ministry of Defence (MOD) in London was anxious to conclude the campaign quickly, preferably before the full force of winter arrived or renewed negotiations frustrated the effort to defeat the Argentine occupiers. As a result, the MOD brought great pressure on the commando brigade commander, Julian Thompson, to initiate combat operations even before adequate supplies for the contemplated operations could be accumulated. On May 28, with the change in mission from a "presence" on the island to advancing and attacking the Argentineans around Stanley, Thompson sent the 2d Battalion of the Parachute Regiment against the reinforced Argentine garrison at Goose Green and nearby Darwin (small settlements on the southwest coast of East Falkland Island). At the same time, he dispatched the 3d Battalion and 45 Commando, Royal Marines, on an "extreme" foot march some 40 miles eastward into position for a final assault along a northern axis on Argentine positions around Stanley.[5]

On June 1, 5 Infantry Brigade—consisting of the Scots Guard's 2d Battalion, the 1st Battalion Welsh Guards, and the 1st Battalion 7th Duke of Edinburgh's Own Gurkha

Rifles—began landing on East Falkland Island. Once ashore, the brigade moved by helicopter and LSL east on a southern axis to be in position for the planned assault on Stanley. The move was marred by a successful aerial attack on the LSL *Sir Galahad* and *Sir Tristam* by Argentine aircraft that resulted in the death or wounding of approximately half of the Welsh Guards Battalion along with the sinking of the *Sir Galahad* and crippling of the *Sir Tristram*.

With the arrival of 5 Infantry Brigade under Brigadier Anthony Wilson, the command of the land campaign passed to Major General Jeremy Moore of the Royal Marines. He planned for a three-phase attack on Stanley commencing the night of June 11. Three Commando Brigade would advance on Stanley from the north while 5 Infantry Brigade would attack from the south. The night attacks of June 11–12 were successful, but the small amount of available ammunition for the five supporting artillery batteries made it necessary to delay phases two and three until June 13. After a hard fight, the Argentine force surrendered on June 14, ending its occupation of the Falkland Islands.

Logistical Plans and Initial Operations

Initially, the logistic plan called for operating the support of the ground troops from the landing ships logistic. On April 10, well before even the location of the landings was determined, the commando logistic staff offered Brigadier Thompson a two-option plan. One called for supporting an amphibious landing with all the reinforced brigade's subordinate elements landing in close proximity to each other. The second called for two landing operations in noncontiguous areas. Neither of the options contemplated an amphibious assault of East Falkland Island. The British joint task force did not have the capability of making a forced landing against enemy resistance, which would have greatly influenced how logistic support was to be provided ashore.

During the landing phase after the troops went ashore, it was first necessary to make the beach support area secure. The logistic effort was then to be controlled from the assault ship HMS *Fearless*. Because the British never gained complete air superiority, the Argentine aerial threat made it necessary to move the control and operation of the logistic effort ashore to the BSA. At the same time, while limited ship-to-shore movement could initially be made during daylight hours, frequent Argentine air attacks soon made it necessary to bring supply ships into the combat operations area and unload at night. The nighttime restrictions applied particularly to the civilian merchant ships, which had little means of protecting themselves against aerial attack.

The first resupply requirements were for such items as ammunition and rations. These necessities were met by employing helicopters to ferry the supplies ashore. The rotary wing aircraft, however, also had to contend with possible attacks by Argentine aircraft. Luckily, the Argentine air force and naval aircraft concentrated on attacking British combat naval vessels, essentially leaving the troop transports and supply ships alone.

Once the beachhead was firmly established and sufficiently expanded, the BSA, which evolved into the brigade maintenance area (BMA), became the CLR's primary ground logistic node and served as the link between the supply vessels and advancing troops. The locations for the various activities and supply dumps were determined by the regiment's amphibious beach unit. Helicopter landing zones, under standard operating procedures, would also have been set up for control, maintenance, and organization of the aircraft by mobile air operations teams. Unfortunately, none of these teams were available to the regiment during the campaign, and the tasks were accomplished by organic regimental staff personnel.

The BMA for the amphibious landing force was an abandoned refrigeration plant with limited hardstand and no overhead concealment at Ajax Bay on San Carlos Water. Located in a very constricted area around the plant were a prisoner-of-war camp, supply dumps, a helipad for sling loading helicopters, and a helicopter landing zone for medical evacuation. In the main plant building were a mess hall and the medical squadron's main dressing station (MDS). In small buildings close by were the CLR headquarters and the ordnance squadron's warehouse. The entire complex was exposed to enemy air attack, and the hardstand was surrounded by ground that quickly turned to mud.

In spite of the BMA's complete exposure, however, Argentine aerial attacks continued to be directed at British naval combatants, allowing for a buildup of supplies and equipment. To bring fuel ashore for the land-based helicopters, emergency fuel handling equipment moved petroleum from ships to bladders to customers. Air portable flexible containers holding 450 gallons of fuel, capable of being moved about by helicopter, were also put into operation, as were the ubiquitous 5-gallon jericans, some 9,000 of which eventually made their way to the Falklands.

Because there were few land battle casualties until the attack on Goose Green on May 28, the MDS at first saw limited activity, but it was ready, as it proved the day before the 2d Battalion of the Parachute Regiment went into action. Its first surgical operations took place on May 27, when the BMA was bombed by Argentine aircraft. The refrigeration plant was hit by several bombs that set fire to the mess hall, killing or wounding several and destroying quantities of supplies and

Ministry of Defence, Navy

MV *Leicesterbrook* offloads cargo at a mobile port at the Falkland Islands

Ministry of Defense, Royal Air Force

RAF Hercules preparing for takeoff from Wideawake Airfield on Ascension Island

Ministry of Defence, Navy

HMS *Sir Percivale* heads to the Falkland Islands loaded with helicopters and other heavy equipments for British troops

ammunition located nearby. Luckily, the MDS escaped damage, but two unexploded bombs lodged in the ceiling and remained there for the campaign's duration while the surgeons cautiously went about their work.

Logistic Operations Continue

The battle for Goose Green and Darwin that began the day after the air attack on the BMA revealed glaring logistical deficiencies. The drawdown on ammunition for the fight was especially significant. On May 29, the day the battle ended, only 83 rounds of 105mm artillery ammunition were on hand along with only 30 Milan antiarmor missiles. This shortage could have caused difficulties had the Argentines contested the advance across the island to Stanley. As it was, the loss at the BMA of ammunition in the bombing had already contributed to the deteriorating situation.

Another deficiency was revealed when the need for better cross-country mobility became apparent. The British initially underestimated the utility of tracked vehicles. Bringing ammunition forward to the Goose Green battleground had to be accomplished by manhandling and helicopter, both of which proved barely adequate. Because of the proximity of Goose Green and Darwin to the BMA, battle casualties could be quickly brought to the MDS by helicopter. Timely evacuation of the wounded, both British and Argentine, saved several men who were promptly treated at the dressing station.

In addition to the casualties sustained at Goose Green, which impacted on the present-for-duty strength of the parachute battalion, there was a serious shortage of available supplies in the BMA besides ammunition. There were no individual ration packs on site. There were no hexamine tablets to furnish heat to boil ground water, the primary source of drinking liquid for the marines and paratroopers. There was no spare clothing and only 3 days' worth of medical stocks.

The march on Stanley beginning on May 28 presented its own logistic challenges. The weather continued to worsen. For the individual marine commando or paratrooper who had waded ashore a week earlier, the salt particles in the water had crystallized in his boots, and it was almost impossible for the footgear to dry out. This was to lead to serious medical problems. At the same time, the helicopters were having to move supplies greater distances, requiring additional fuel and longer flight times.

As the 3d Battalion of the Parachute Regiment and the 45 Commando Royal Marines reached their intermediate objectives some 40 miles east of the BMA, the Royal Navy's landing craft and LSL assumed an increased logistical role. Once the units arrived at Teal Inlet, where an advance Royal Marine BMA was established, the LCM and LSL began making resupply runs that continued throughout the remainder of the campaign.

the limited number of heavier lift helicopters often led to "hijacking" or improper diverting of the helicopters from their assigned missions

On June 1, 5 Infantry Brigade landed in San Carlos Water and began moving east. Although helicopters carried supplies forward and the Chinook transported elements of the 2d Battalion of the Parachute Regiment to the vicinity of Bluff Cove, other troops sailed in LSL to the assembly areas for the final attack on Stanley. It was during this time that the exposed ships with the 151 Battalion, Welsh Guardsmen, on board were attacked by Argentine Skyhawk aircraft in broad daylight.

In the meantime, Sea King helicopters were bringing the 30 105mm light field pieces of 29 Commando Regiment Royal Artillery and 4 Field Regiment Royal Artillery forward into position to support the attack on Stanley. The helicopters then lifted 16,000 rounds of artillery ammunition to the guns' positions. Yet it was a shortage of artillery rounds at the field pieces after phase I of the attack on Stanley that caused the next phase to be postponed from June 12 to the next day. It was calculated that it would take an additional day to restock the ammunition supply. Sea Kings, flying through darkness and snow showers, led by 3 Commando Brigade Air Squadron pilots equipped with night vision devices in their light helicopters, nevertheless continued to bring ammunition forward. Nearly 530 rounds per artillery piece were expended during the final attack. When the Argentines surrendered, some of the weapons were down to six rounds each.

While the heavier lift helicopters were bringing ammunition, rations, and supplies forward, the lighter aircraft were evacuating casualties to the two forward field dressing stations and the MDS. In an impressive performance, one Scout light helicopter evacuated 16 Scots Guards casualties off Tumbledown Mountain in high winds and falling snow. The casualty evacuation helicopters' efforts kept the medical facilities working at a high pitch. The MDS alone received 50 admissions and performed 32 operations after the final assault.

Royal Air Force, Navy, and Marine helicopters were indeed major contributors to the success of the logistic effort. The aircraft crews and mechanics worked without rest under the worst of operating conditions. Even as the weather became increasingly bitter, the pilots flew regardless of flight conditions. The mechanics kept the aircraft flying with the minimum amount of downtime for maintenance. Operating restrictions went by the board as the helicopters flew men, supplies, fuel containers, field artillery pieces, and pallets of ammunition about the battlefield, always under the threat of an attack from Argentine Mirage and Skyhawk aircraft.

Manmade Complications

In 1982, the British Army of the Rhine was where the bulk of British armed services were to be found. Troops remaining in the British Isles could look forward to rotating to Germany for extended periods. The focus was on the Warsaw Pact nations and the large Soviet presence in East Germany. Although British forces were still to be found in places such as Belize, Cyprus, and Hong Kong, the Falkland Islands merited little more than a detachment of Royal Marines. It is small wonder that when the Argentines invaded the islands, the British government was unprepared to immediately eject them. It was to take time to get to the Falklands, and therein lay a major reason why logistics suffered from the beginning.

Confusion reigned in preparing the joint task force for deployment. There was no plan for a land logistical effort some 8,000 miles from the United Kingdom. The CLR, however, was well attuned to the demands of supporting the brigade's three commandos, its artillery battalion, and assorted other elements. It constantly practiced not only deploying to northern regions but also moving a great amount of heavy equipment, particularly BV

206 tracked vehicles. But there was no such storage of equipment in the Falklands. Everything that was to be employed there had to be transported in ships, and the haste in loading at the ports in the United Kingdom led later to great supply deficiencies.

Because there was no previous planning but great urgency, supplies and equipment of all kinds were dispatched to the embarkation ports without any regard to priority. As ships taken up from trade were assembled, they were loaded with whatever happened to be at dock. There was no combat loading or accountability for what items went on which ships. The Commando Logistic Regiment played its practiced role in outloading, but it had to adapt to the expanded requirements and the available shipping. These requirements had to take into consideration that the regiment was being tasked to support logistically not only its own organic formations but also two additional infantry battalions, plus a plethora of smaller attached army units such as the two troops of the Blues and Royals Medium Mechanized Reconnaissance Regiment. The CLR, reinforced with additional manpower from small army logistic units when 5 Infantry Brigade arrived in the Falklands, was then expected to provide combat service support to an entire division-size force.

The hastily conceived plan by the MOD to correct the abject loading was to have the task force stop at Ascension Island, some 4,000 miles from both the United Kingdom and the Falkland Islands, and there rearrange the supplies and equipment, placing them on the correct ships and properly accounting for what was afloat. What was a good idea in theory, however, turned out to be less than effective in practice.

When the ships got to the Falklands, they operated from a station at sea called the transport area (TA). The dispatch of supply vessels from the TA was soon complicated by the lack of information about cargo on the various ships. The 4-day redistribution of supplies and equipment off Ascension Island before the task force sailed further south only partially rectified the loading mistakes made in Great Britain. The CLR control cell could never be sure whether its request for a particular ship to transport certain needed supplies to the BMA was actually carried out. Too often these ships, which had to come into San Carlos Water at night because of the Argentine air threat, had to be turned around and sent back to the TA without unloading. Unfortunately, while there was a shortage of ammunition on East Falkland to support the final assault, a cargo ship loaded with additional ammunition was available on demand in the TA but never brought forward.

frequent Argentine air attacks made it necessary to bring supply ships into the combat operations area and unload at night

Once British troops landed, the Ministry of Defence and the commander of the naval task force became upset about what they perceived as the inactivity of 3 Commando Brigade in preparing to move on Stanley. They exhibited little appreciation for the requirement of a supply buildup that was adequate to sustain a campaign conducted in unfavorable weather and over poor terrain conditions against a foe that was determined to hold on to its newly won islands.

One significant factor that affected the ground logistic effort, but one that the Commando Logistic Regiment could not influence, was the May 25 loss of the three Chinook and six Wessex helicopters. The Royal Navy could perhaps be criticized for not dispersing the critical heavy lift helicopters to more than one ship before they were to be transferred from sea to shore. Had the aircraft been brought to flying status while the Atlantic Conveyor was still in the TA or outside the TEZ (when it was decided to deploy the helicopters), the shortage of required airlift to move troops into position for the final assault would probably have been avoided. The immediate result of the loss, however, was the need for commandos and paratroopers to make the famous "yomp"—the extreme foot march to the required lines of departure for the final attack on Stanley.

The successful logistic effort by the CLR on East Falkland Island leads to some thoughts pertinent to supporting future small-scale expeditionary operations:

- recognize that proper logistic planning drives maneuver planning and subsequent operations
- consider the desired objective in planning
- prepare to accept the fact that outside political pressure or influence may require a flexible logistic response
- change plans to adapt to local conditions as they relate to logistics
- attend to the level of logistic support required for combat operations, such as distance, weather, and terrain
- scrutinize the expenditure of assets, such as ammunition, fuel, and rations, especially when unanticipated exigencies are possible.

The Commando Logistic Regiment and its rotary wing assets deserved a major share of the credit for the success of the campaign. But undoubtedly it was the individual serviceman who deserved the most. Whether it was the solitary guide on the ground in freezing wet weather and under fire directing where a helicopter pilot was to drop his load, or the tired and cold soldier or commando manning a fuel pump alone and filling 5-gallon cans for the Rapier antiaircraft missile units, all were key contributors to the victory.

The short campaign was fought under abominable weather conditions over indescribable terrain by brave British servicemen, who took numerous risks to accomplish their mission. But for the dedicated and effective, if not necessarily efficient, logistic operations, the soldiers, sailors, airmen, and marines who put their boots on the ground would have had to face the possibility that the campaign could have ended in a quagmire and not a signal victory. As it was, it was a "close run thing." **JFQ**

NOTES

[1] British infantry units are termed battalions, with regiments being administrative headquarters. Other battalion-size organizations, however, are termed regiments.

[2] The three Royal Marine Commandos were 40, 42, and 45 Commandos. The artillery battalion was 29 Commando Regiment Royal Artillery, made up of commando-qualified soldiers.

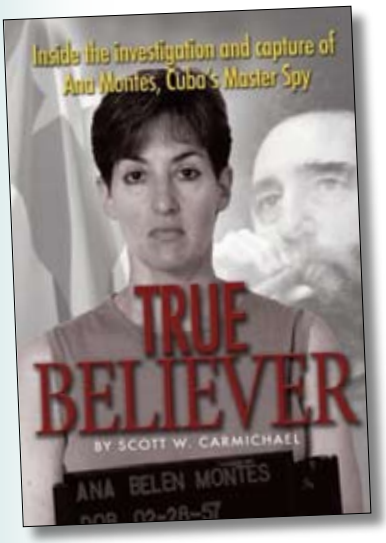
[3] Because it was thought that overland motor movement would be sharply limited, the squadron brought only 28 vehicles to the Falklands.

[4] Some literature calls this landing craft a landing craft utility.

[5] This extreme foot march became known as the famous *yomp*. Royal Marines and paratroopers made the march laden with heavy packs called *bergens*.

Off the Shelf

Intelligence is a precious commodity that nations seek to gather, protect, share, or distort, depending on the particular need at any given time. As described in this issue's Forum, the application of high technology to all aspects of intelligence collection and handling is changing the way consumers use this commodity. But technological gadgets are only as useful as the human elements designing them, operating them, and analyzing the information they collect. For every technology created to gather or protect intelligence, determined adversaries tend to find a way to defeat, overcome, or circumvent it. Low-tech methods of intelligence-gathering can cause high-value damage, and high-tech devices can be crippled by the power of the human brain.

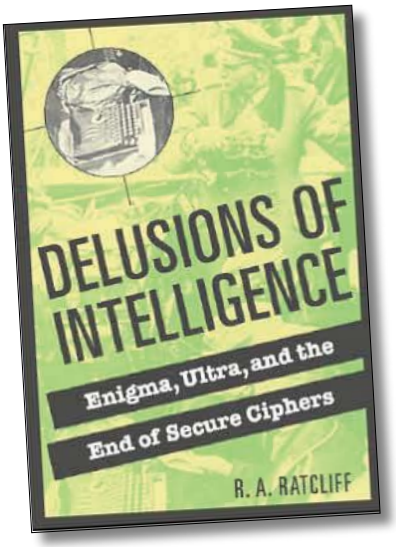


True Believer: Inside the Investigation and Capture of Ana Montes, Cuba's Master Spy
by Scott W. Carmichael
Annapolis, MD:
Naval Institute Press, 2007
187 pp. $27.95
ISBN–13: 978–1–59114–100–6

On September 21, 2001, the Nation was still reeling from the terrorist attacks that occurred 10 days earlier. Thus, the arrest of Defense Intelligence Agency (DIA) analyst Ana Montes as a Cuban spy on that day garnered less attention than such an event normally would have. The timing of the arrest was not coincidental; Montes would have had access to information regarding the impending U.S. attack on Afghanistan—information that, had it reached Cuba, would "naturally have found its way to nations such as Russia, China, Libya, Iraq, Iran, Syria, North Korea, and potentially any country or political movement that opposes the United States" (p. 138).

Technology no more sophisticated than a short-wave radio, a personal computer, and public pay phones allowed Montes to pass information to the Cuban government for 16 years. And technology as sophisticated as a polygraph, while known to be an inconclusive measure of guilt or innocence, was no match for Montes, who defeated a counterintelligence examination in 1994. Montes received taskings at her home via encrypted radio messages. Rather than smuggling material from DIA, she kept information in her head until she got home, where she recorded the day's events on a computer disk. Montes then passed the disks to her handler or used prepaid phone cards at public telephones to make operational calls to her handler's pager.

The author, Scott Carmichael, is the senior security and counterintelligence investigator at DIA; he was the lead agent on the Montes case from 1996, when she first came under suspicion, until her arrest in 2001. Using information that has come to light since Montes' arrest, Carmichael has been able to link her treachery to the death of SFC Gregory Fronius, USA, in El Salvador in 1987.

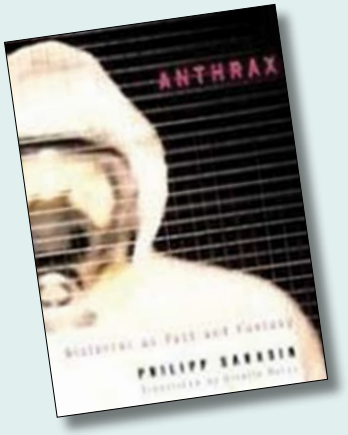


Delusions of Intelligence: Enigma, Ultra, and the End of Secure Ciphers
by R.A. Ratcliff
New York:
Cambridge University Press, 2006
313 pp. $30.00
ISBN–13: 978–0–521–85522–8

The full story of the Allied penetration of Germany's Enigma enciphering system before and during World War II started emerging in the 1970s, when the British government admitted to reading thousands of encrypted messages during the war—an admission that stunned many German cryptologic experts familiar with the system. Between its statistical complexity and the compartmentalization of information needed for its use, German confidence in Enigma's security was high. Despite offering 3×10^{114} possible combinations of letter substitutions, however, Enigma proved to be as unbreakable as the *Titanic* was unsinkable.

Ratcliff argues that "Enigma's defeat arose less from a technological flaw than from the systemic failure of an entire intelligence system" (p. 9). The same compartmentalization that the Germans touted as a security feature, combined with the lack of centralization in the Wehrmacht's intelligence-gathering apparatus, allowed the Allied penetration of Enigma to go undetected. In addition, long-term strategic intelligence was not a priority for the Germans, who reacted to problems rather than avoiding them in the first place. The nature of German society itself in the 1940s, in which admissions of error or acknowledgment of the possibility of compromise could end a career (if not a life), discouraged scientists from constructive criticism of Enigma's performance and security.

The reverse side of the coin was the Allied approach to cracking Enigma: a flexible, collaborative, sometimes combative, but ultimately successful effort. Ratcliff endorses the spirit of that Allied approach as we face modern-day security challenges: "Success will come to those who keep changing and adapting to new advances. Technology cannot solve our problems. Human brains do" (p. 236). **—L. Yambrick**



Anthrax:
Bioterror as Fact and Fantasy
by Philip Sarasin
Suhrkamp Verlag
Frankfurt am Main, 2004
Trans. Giselle Weiss
Cambridge and London:
Harvard University Press, 2006
322 pp. $24.95
ISBN: 0–674–02346–3

Reviewed by
ZYGMUNT F. DEMBEK

Philip Sarasin, a professor of modern history at the University of Zurich, attempts to demonstrate that the threat of bioterrorism is disproportionate to our societal fears of such events—in part because media fascination with biological weapons has allowed reality to be influenced by fiction. Sarasin describes how the 1998 publication of Richard Preston's bioterrorism novel *The Cobra Event* became a cause célèbre that had a disproportionate influence. After President Bill Clinton read his novel, Preston was invited to appear in 1998 before the Senate Subcommittee on Technology, Terrorism, and Government Information, in a joint meeting with the Select Committee on Intelligence. Tom Clancy's bioterrorism novel *Rainbow Six*, in which bioterrorists fly in four airplanes from a base in Kansas, was also published in 1998. Both Preston's and Clancy's fictional works contained enough scientific facts to make their scenarios partially plausible, as the authors had such information provided to them by subject matter experts. Subsequent meetings were held at the highest levels of the U.S. Government to address a lack of national preparedness for bioterrorism. And international concerns for bioterrorism certainly grew with the 1999 publication of the book *Biohazard*, a nonfiction account of the Soviet Union's biological weapons program, written by one of its former military chiefs, Ken Alibek (which Sarasin oddly omits as a source document).

Some of the more cogent points Sarasin makes are that modern Western society (especially the United States) has long had a morbid fascination with disease and biological weapons of mass destruction; that this fascination has led to a "death wish" on the part of modern civilization; that disease outbreaks in the West have historically been blamed on foreign individuals; and that our cultural absorption with bioterrorism has distorted our perceptions of actual cultural threats.

Unfortunately, Sarasin's book largely comprises a rambling essay of opinions, such as why and how the U.S. anthrax mailings (4 letters delivered by the postal service that caused 5 deaths and 18 cases of illness) subsequent to the September 11 attacks occurred. Sarasin bases much of the proof of his assumptions on media reports (print and Internet postings), which lead him to the inference that the anthrax mailings were the work of an American perpetrator trained by the military and were composed of highly purified anthrax spores mixed with special adjuvants for aerosol dispersal—suppositions that are at present either unproven or disputed. A recent publication by a scientist from the Federal Bureau of Investigation describes the anthrax mailings of 5 years ago as containing a crude preparation of spores that may have been created by an individual or small group without ties to government sponsorship. Interestingly, in a June 2005 media interview that Sarasin references, Ken Alibek made the similar observation that the anthrax used in the U.S. attacks could have been manufactured "somewhere in a forest, in a car, without a microscope," to which Sarasin responds, "[it] just goes to show where even expert discourse can lead: into a quagmire of speculation and phantasms" (p. 257).

There is also considerable vitriol in this book, much of which appears to be directed at the United States; witness such passages as, "'Bioterror' is the dream dreamed by postmodern society in the throes of a self-determined state of war, and 'anthrax' its wish fulfillment" (p. 11); "'Typhoid Mary' . . . was a sexist and racist construction" (p. 239); "The claim that the American government was totally surprised by the [September 11] attacks does not seem to hold water" (p. 141); "'anthrax' was crucial in extending [President] Bush's long and unconventional 'war on terror'" (p. 7); "The feverish anticipation of a bioterrorist attack started slowly in the years leading up to September 11 and increased sharply from the moment of the World Trade Center attack until it reached the anthrax frenzy" (p. 149).

By using fiction and media accounts rather than scientific documentation to argue his points, and in the absence of much-needed editing throughout his book, Sarasin has produced a rambling diatribe against Western culture and U.S. biodefense policies. This politicized, acrimonious commentary provides a strongly opinionated and biased viewpoint of recent history for anyone seeking such accounts.

Dr. Zygmunt Francis Dembek (Lieutenant Colonel, Medical Service Corps) is a mobilized Reservist at the U.S. Army Medical Research Institute of Infectious Diseases. He is adjunct Assistant Professor at the Uniformed Services University of the Health Sciences and an Assistant Clinical Professor at the University of Connecticut School of Medicine.

Learning Large Lessons: The Evolving Roles of Ground Power and Air Power in the Post–Cold War World

by David E. Johnson

Santa Monica, CA: RAND, 2007,
Monograph MG–405–1
264 pp. $28.00
ISBN: 978–0–8330–3876–0

Reviewed by
BARRY D. WATTS

American Airmen have been disagreeing with American Soldiers and Marines over the relative utility of airpower as opposed to ground power since World War I. This longstanding debate has rarely changed opinions on either side, despite the emphasis on jointness mandated by the 1986 Goldwater-Nichols Department of Defense Reorganization Act. Instead, discussions over the years have largely consisted of the participants talking past one another.

David Johnson's *Learning Large Lessons* sheds some long-needed light on this debate. The book first appeared in 2006. This year, RAND published an updated version both to satisfy demand for the book and to address the new Joint Publication 3–0, *Joint Operations*. Johnson, a retired Army colonel and former artillery commander, has briefed the implications of *Learning Large Lessons* to the Air Force secretary and four-star generals at Corona, the semiannual senior leader conference, as well as to classes at the Army and Air Force command and staff colleges. Air Force chief General T. Michael Moseley has added the book to his professional reading list. Insofar as evidence and balanced analysis can be brought to bear on the ever-divisive issue of modern airpower versus "boots on the ground," *Learning Large Lessons* is a gem. It deserves to be read—thoughtfully—by Airmen, Sailors, Soldiers, and Marines alike.

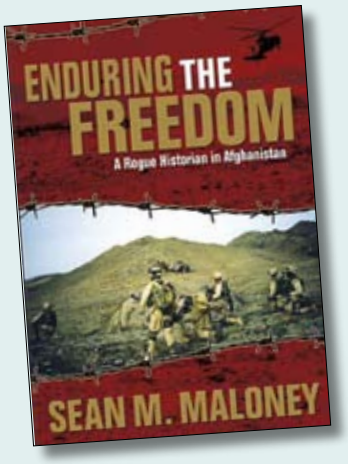
Why is *Learning Large Lessons* so important? The simple answer is that even though the debate it addresses goes back to 1917, there has been an astonishing lack of intellectual or doctrinal convergence right down to the present day. Consider, for example, the extent of disagreement that persists between the U.S. Air Force and Army over their relative shares of Iraqi tanks destroyed during Operation *Desert Storm* in 1991. Postwar imagery analysis indicated that airpower, prior to the beginning of the ground offensive on February 24, had eliminated a minimum of 40 percent of all Iraqi tanks destroyed by February 28. Yet retired Army Lieutenant General William Odom opined in a 1997 *Foreign Affairs* article that the Army alone killed 70 to 80 percent of the Iraqi tanks, and in his 1999 book *The Gulf War: A Complete History*, based on long-after-the-fact interviews and recollections, Thomas Houlahan reduced the total share of Iraqi tanks destroyed by fixed-wing aircraft to 13 percent.

Much of the reason Soldiers, Airmen, Marines, and even Sailors have had so much difficulty agreeing on airpower's utility is that all sides have viewed the debate as a zero-sum competition for resources within the Pentagon's annual budget. In the wake of the 1991 Persian Gulf War, Airmen appeared—at least on the surface—to gain the upper hand. The outcome of the North Atlantic Treaty Organization's 1999 air campaign aimed at compelling Slobodan Milosevic's regime to cease ethnic cleansing in Kosovo seemingly strengthened the hand of airpower advocates because the political aim was ostensibly achieved before any ground forces entered the fight. Operation *Enduring Freedom* in late 2001 had more mixed results. Laser-guided bombs and the all-weather joint direct attack munitions were instrumental in providing the fire support that enabled Northern Alliance forces to overthrow the Taliban in Afghanistan and scatter al Qaeda. But the precise targeting of U.S. fixed-wing airpower was largely done by special forces and Central Intelligence Agency operatives on the ground—in some cases riding on horseback.

Since May 2003, Soldiers and Marines have become even more ascendant. As coalition forces have grow increasingly bogged down in a "long, hard slog" against various foreign jihadists, insurgents, religious militias, and plain criminals inside Iraq, ground-force advocates have pressed the need for more "boots on the ground," and the administration has agreed. In January 2007, Defense Secretary Robert Gates and President George W. Bush endorsed a 92,000-troop increase in Army and Marine end strength over 5 years. Although these additional troops could do much to relieve the grinding pressure of current operations in Iraq and Afghanistan on the Army and Marine Corps, the majority of them are unlikely to be trained or equipped before the 2008 Presidential election, after which U.S. troop levels in Southwest Asia are likely to be substantially reduced. Thus, there is a serious question as to whether the extra 92,000 troops address the longer-term challenges of, say, dealing with a rising China or merely today's problem of overstretched ground forces.

Given this strategic dilemma, proponents on both sides of the argument over airpower versus ground power would benefit from reading Johnson's *Learning Large Lessons*. His *Fast Tanks and Heavy Bombers* (Cornell University Press, 1998) provided a penetrating examination of the follies of extremism among the Army's infantry branch, cavalry branch, and aviators from 1917 to 1945. *Learning Large Lessons* extends this line of research by examining five recent conflicts as a basis for drawing conclusions about the changing roles of air and ground power. The five conflicts are Operations *Desert Storm* (1991), *Deliberate Force* in Bosnia (1995), *Allied Force* in Kosovo (1999), *Enduring Freedom* in Afghanistan (2001), and *Iraqi Freedom* (2003). Johnson's basic conclusion is that, since 1991, airpower, employing precision munitions, informed by advanced sensors, and linked by targeting networks, has shown "growing levels of effectiveness and robustness and played commensurately growing roles" (p. 137). Nevertheless, Army doctrine in particular is not being revised to "accommodate this new reality," and joint doctrine "still defers to the surface components" (p. 138). The reason is a lack of trust, especially between the Army and Air Force. "The Army," Johnson observes, "does not trust the Air Force to be there when it is needed, and the Air Force does not trust the Army to employ air power properly if it is in control of the resource" (p. 197). Perhaps it is time for Soldiers and Airmen to begin trusting one another.

Barry Watts is a Senior Fellow at the Center for Strategic and Budgetary Assessments, where he has recently published *Six Decades of Guided Munitions and Battle Networks: Progress and Prospects*. He is also the author of *Clausewitzian Friction and Future War* (National Defense University Press, 2004).



Enduring the Freedom: A Rogue Historian in Afghanistan
by Sean M. Maloney
Dulles, VA: Potomac Books, 2005
320 pp. $27.50
ISBN: 1574889532

Reviewed by
JAMES SNYDER

In late summer 2006, North Atlantic Treaty Organization (NATO) forces in Afghanistan engaged in the first sustained infantry action in the Alliance's history. Surprising observers and some Allies alike, NATO found itself at war far from Europe, against a resurgent Taliban in Kandahar and Helmand provinces.

This was an extraordinary development. NATO's mission in Afghanistan is barely 4 years old, having begun in 2003 and rapidly evolving from policing the capital into conducting a comprehensive security and reconstruction operation involving 32,000 Allied and partner soldiers deployed across the entire country. The International Security Assistance Force (ISAF) mission now ranges from peacekeeping to virtual counterinsurgency in some parts of the country. Along the way, it has evolved into the most complex operation ever undertaken by the Alliance.

Canadian military historian Sean Maloney visited Afghanistan in early 2003, observing ISAF before the NATO takeover and Operation *Enduring Freedom* (OEF) just as war in Iraq began to eclipse them. Maloney is an accomplished historian who served with the Canadian Army in Europe during the Cold War and now teaches at the Royal Military College in Kingston, Ontario. He has written extensively on NATO missions, particularly in the Balkans, and is a cheerleader for a more robust Canadian role in the world—a controversial opinion, especially now, as Canada takes on more responsibilities, and casualties, in Afghanistan.

ISAF at the time of Maloney's visit was a small operation limited to Kabul, a force constituted by various nations under the authority of the Bonn Accords and the United Nations. Maloney spent time with German and Dutch units in the capital—Bulgarians, Romanians, Macedonians, Spaniards, and Hungarians also make appearances—when they were still dressing in green fatigues to differentiate themselves from the desert uniforms worn by the *talibanjaeger* (Taliban hunter) Americans and their coalition partners. It was a dangerous time, then as now, as Afghanistan began to emerge from 30 years of Soviet occupation, civil war, and Taliban rule.

Maloney begins with a precise summary of the 2001 invasion and follows his freelance trip from Kabul to Bagram and then to Kandahar, recording his experiences along the way. His intent in Afghanistan is to document the deeds of brave men, a laudable aim even after the fall of the Taliban. But he records very little history here beyond the rich tradition of particular units he encounters, and his descriptions of various subunit activities—psychological operations, the Joint Visitors Bureau, a German field hospital—are cursory at best. Beyond that, Maloney simply does not have the material or skill to make a compelling first-person narrative of his experience. A comparison of coalition operations in Afghanistan to NATO's experience in the Balkans might have been useful and interesting, but he makes no attempt at contrast. He exudes natural bonhomie with members of other uniformed services and drips cheap contempt for almost everybody else he encounters (Geraldo Rivera appears twice, providing an easy target). The text is littered with embarrassing misspellings and typographical errors.

Nonetheless, a useful portion of this book focuses on Maloney's experience with a company from the U.S. 82d Airborne Division (mostly Bravo Company, 2d Battalion, 504th Parachute Infantry Regiment) operating with OEF in Zabol province. While nothing particularly remarkable happens—the company efficiently carries out a series of raids in Taliban territory, resulting in huge arms seizures—the mission gives a flavor of the kinds of routinely perilous actions ISAF and coalition forces must carry out there and elsewhere across the country.

The sheer remoteness and hostility of the Afghan terrain present an enormous challenge to airborne troops sustaining themselves for days on end at high altitude. The troopers begin to place bets on how long the 35-year-old Maloney will last (he manages, but admits he is not packing the 100 pounds most young soldiers carry). Cultural complexity provides another challenge; for example, the company requires a section of female Military Police to handle local women sensitively. Maloney expresses the same bewilderment that the troopers no doubt feel when trying to assess local motives and actions in such an alien culture; he finds himself unnerved by what the soldiers dub "Hadji TV," when locals come outside simply to watch the company conduct a sweep. Operating in this environment requires the judgment to know whether something is out of place or whether a local "person under control" is telling the truth. Such judgment can only be developed with experience, and even then confusion reigns.

Ironically, these early raids in Taliban country that Maloney records seem to foreshadow the return of those fighters whom ISAF and the coalition forces today confront again. The mission of securing all of Afghanistan now places NATO squarely against the Taliban and other forces of disorder. More examination of the everyday danger in these routine operations should follow, because it is in such routine actions that Afghanistan will be won or lost.

James Snyder is the U.S. Information Officer on the International Staff at NATO Headquarters in Brussels.

NEW Titles from NDU Press

NDU Press

Center for the Study of Weapons of Mass Destruction Occasional Paper 5

The Future Nuclear Landscape

Co-authors Paul Bernstein, John Caves, and John Reichart argue that the world is at a nuclear crossroads. The complex and dynamic nuclear landscape presents us with challenges along at least four axes: regional nuclear proliferation, nuclear terrorism, great power nuclear relations, and the security implications of increased interest in nuclear energy. These problems are interrelated in ways that the national security community does not fully understand. Strategy and policy frameworks do not address them in sufficiently integrated fashion. New conceptual thinking is required to develop a more unified understanding of and approach to managing the risks and opportunities posed by these 21st-century nuclear challenges.

INSS Special Report

Sino-Japanese Rivalry: Implications for U.S. Policy

For the first time in modern history, a rising China and a reemerging Japan face one another as East Asia's preeminent powers. This report stems from a series of workshops by the Institute for National Strategic Studies, Center for Naval Analyses, Institute for Defense Analyses, and Pacific Forum/Center for Strategic and International Studies. Experts from these institutions examine the troubled Sino-Japanese relationship and the implications for American interests. Their conclusions underscore the fact that both countries (as well as the United States) have a stake in the future stability and prosperity of East Asia that vastly exceeds whatever each could gain from the pursuit of unbridled rivalry. (*Available from NDU Press only*)

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

Got MERLN??

The award-winning National Defense University (NDU) Library is pleased to announce that MERLN—the Military Education Research Library Network—is up and running after being offline briefly earlier this year. Researchers not already familiar with MERLN are encouraged to visit it at:

<http://merln.ndu.edu>

MERLN is a public Web site that offers one-stop, timely access to a variety of unique electronic resources contributed by a network of military libraries led by the NDU Library.

MERLN's resources are organized for easy access by researchers, scholars, and practitioners in the fields of military affairs, international relations, and security studies. Resources include:

MiPALS (Military Policy Awareness Links) **focus on current topics such as national security strategy, terrorism, Afghanistan, and Iraq. MiPALs provide direct access to current U.S. Government policy statements, as well as resources from think tanks, nongovernmental organizations, research institutions, and scholarly journals.**

White Papers include defense white papers and national security strategy documents from more than 70 countries throughout the world.

Publications and the *Professional Military Journal Reading Room* link users directly to military journals, newsletters, and conference proceedings.

Digital Collections are compilations of personal papers, historical documents, and government reports.

The *MERLN Group Catalog* allows users to search the online catalogs of more than 30 military libraries with one search.

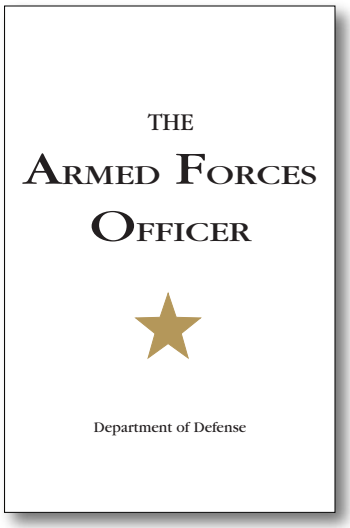
NDU LIBRARY

MERLN

New Books *from* NDU Press

The Armed Forces Officer

by a joint team of the U.S. Department of Defense
Nearly 60 years ago, journalist-historian S.L.A. Marshall wrote the first edition of The Armed Forces Officer at the behest of General George C. Marshall. The general believed that officers of all Services needed to base their professional commitment on a common moral-ethical grounding. Ever since, subsequent editions of The Armed Forces Officer have provided a foundation of thought, conduct, standards, and duty for American commissioned officers.



This latest edition takes the series' inspirational premise into the new century. It educates officers of all Services, as well as civilians, about the fundamental moral and ethical requirements of being a commissioned officer in the Armed Forces of the United States. Understanding the common foundation of commissioned leadership and command of U.S. military forces is essential for achieving excellence in the joint operations of today's combat environment. This philosophy unites the officers of the uniformed Services in the common calling of supporting, defending, and upholding the Constitution in service to their country.

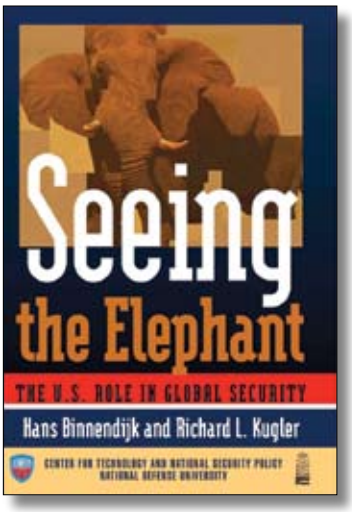
Faculty members of the Service academies and the Marine Corps University wrote this new edition. The Department of Defense coordinated and sponsored the work. Forewords by General Peter Pace, Chairman of the Joint Chiefs of Staff, and Congressman Ike Skelton, ranking member of the House Armed Services Committee, place this volume in the context of the challenges the American officer faces in the 21st century.

Jointly published by National Defense University Press and Potomac Books, Inc., this new edition helps ensure that current and future generations of American military leaders will have an ethics handbook for their profession, a calling unlike any other. The Armed Forces Officer defines the honor and obligations of being an officer in the U.S. military.

Published by National Defense University Press and Potomac Books, Inc.
Washington, DC: Potomac Books, 2007 Order online at: <www.potomacbooksinc.com>
Clothbound $24.95, Paperback $14.95
Individuals qualify for a 25 percent discount and should use the following code when ordering: NDUV07
Institutions and organizations wishing to place bulk orders qualify for special discounts. For details, please contact: Sam Dorrance,
Director of Marketing, Potomac Books, Inc., Email: sam@booksintl.com or telephone: (703) 996–1028

162 pp.
Hardcover
ISBN–13: 978–1–59797–166–9
Softcover
ISBN–13: 978–1–59797–167–6

Seeing the Elephant:
The U.S. Role in Global Security



by Hans Binnendijk and Richard L. Kugler
What is the current state of the global security system, and where is it headed? What challenges and opportunities do we face, and what dangers are emerging? How will various regions of the world be affected? How can the United States best act to help shape the future while protecting its security, interests, and values? How can the United States deal with the threats of terrorism and weapons of mass destruction?

Seeing the Elephant: The U.S. Role in Global Security, an intellectual history of U.S. national security thinking since the fall of the Soviet Union, is an attempt to see the evolving international security system and America's role in it through the eyes of more than 50 perceptive authors who have analyzed key aspects of the unfolding post–Cold War drama. These experts include Graham Allison, Zbigniew Brzezinski, Wesley K. Clark, Tommy Franks, Thomas L. Friedman, Francis Fukuyama, Samuel P. Huntington, Robert D. Kaplan, John Keegan, Paul M. Kennedy, Henry Kissinger, Bernard Lewis, Daniel Patrick Moynihan, Joseph S. Nye, Jr., Michael E. O'Hanlon, Alvin Toffler and Heidi Toffler, and Martin van Creveld. Its premise is that, like the blind men in the Buddhist fable who each feels a different part of an elephant, these authors and their assessments, taken together, can give us a better view of where the world is headed.

319 pp.
ISBN–10: 1–59797–099–9

Published for the Center for Technology and National Security Policy
by National Defense University Press and Potomac Books, Inc.
Washington, DC: Potomac Books, 2006
Order online: http://www.potomacbooksinc.com/Books/BookDetail.aspx?product=148989
Clothbound $48, Paperback $24
Use code NDUV07 for a 25 percent discount (Expires December 31, 2007)

coming next in… JFQ

U.S. Pacific Command

Winners of CJCS and SECDEF Essay Contests

plus

Enduring Choices in British Defense Policy

The Phoenix Program and Contemporary Warfare

. . . and more in issue 47,
4th Quarter 2007 of *JFQ*

JFQ

JOINT FORCE QUARTERLY

A Professional Military and Security Journal
Published for the Chairman of the Joint Chiefs of Staff
by National Defense University Press
Institute for National Strategic Studies
National Defense University, Washington, DC

NDU Press

1070-0692()46;1-N