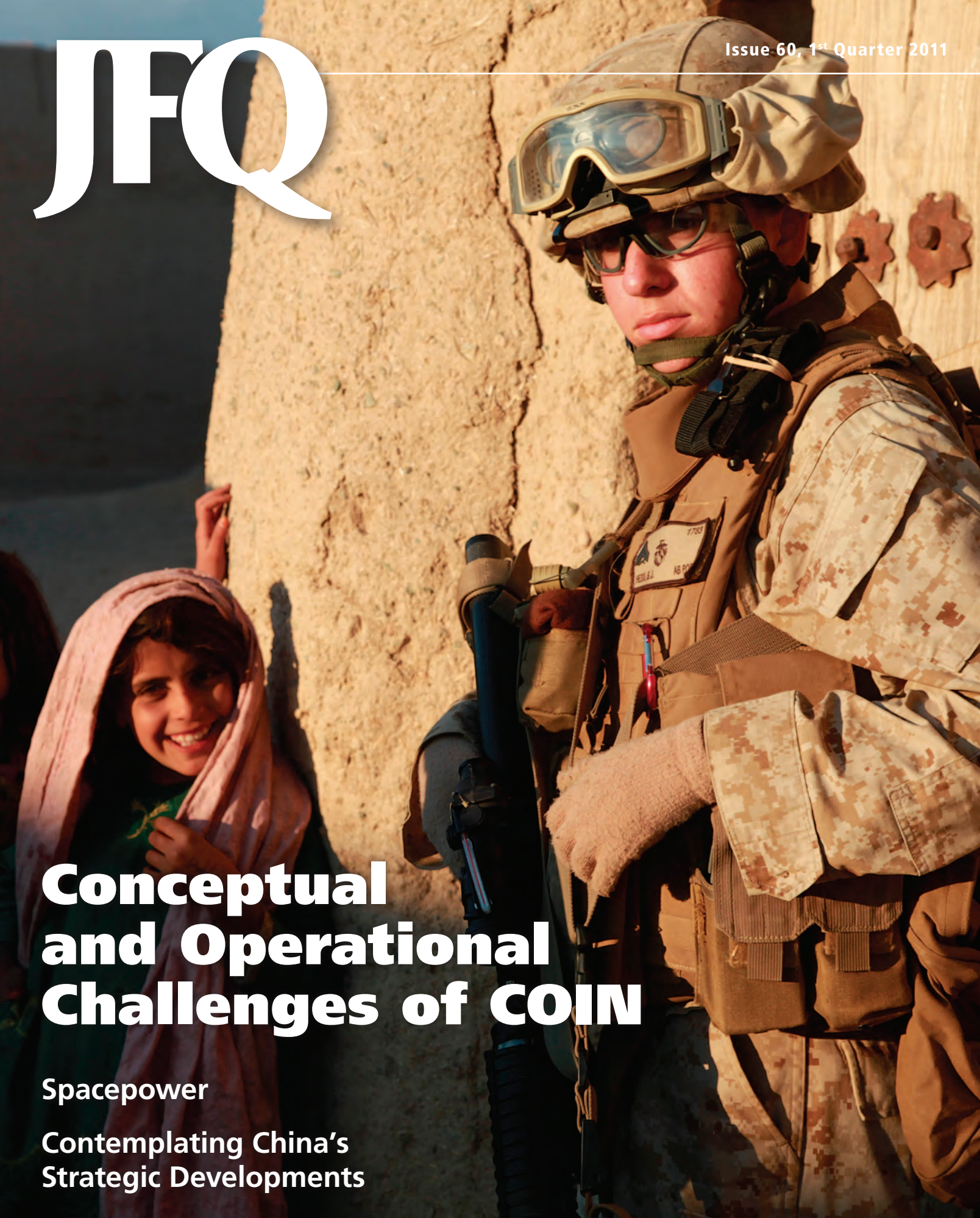
JFQ

Issue 60, 1st Quarter 2011



# Conceptual and Operational Challenges of COIN

## Spacepower

## Contemplating China's Strategic Developments

JOINT FORCE QUARTERLY

# Inside

Issue 60, 1st Quarter 2011



*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, journals, policy briefs, occasional papers, monographs, and special reports on national security strategy, defense policy, interagency cooperation, national military strategy, regional security affairs, and global strategic problems.



**COMMUNICATIONS**

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

**Editor, *Joint Force Quarterly***
**National Defense University Press**
**260 Fifth Avenue, S.W. (Building 64, Suite 2500)**
**Fort Lesley J. McNair**
**Washington, DC 20319**

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

**1st Quarter, January 2011**
ISSN 1070-0692

## JFQ Dialogue



## Forum



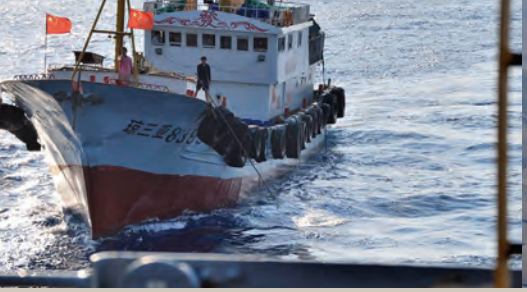
## Special Feature



## Commentary



## Features



# JFQ

## Features



## Book Reviews



## Joint Doctrine



### ABOUT THE COVERS

Front cover: Corporal Bethany Hess, USMC, assigned to the 3d Battalion, 4th Marine Regiment Female Engagement Team, talks to children during patrol in Khwaja Jamal, Afghanistan (U.S. Marine Corps/Albert F. Hunt). Table of contents (left to right): Counter Improvised Explosive Device team moves through Afghan village (U.S. Army/Theodore Schmidt); MC–12W provides tactical intelligence, surveillance, and reconnaissance to ground commanders in Afghanistan (U.S. Air Force/Manuel J. Martinez); Chinese trawler observes USNS *Impeccable* in South China Sea south of Hainan Island (U.S. Navy); and E–8C Joint Surveillance Target Attack Radar System team participates in Joint Surface Warfare Joint Capability Technology Demonstration (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 JFQ1@ndu.edu "Attention A&R Editor" in the subject line. For further information, see the guidelines on the NDU Press Web site at ndupress.ndu.edu.


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





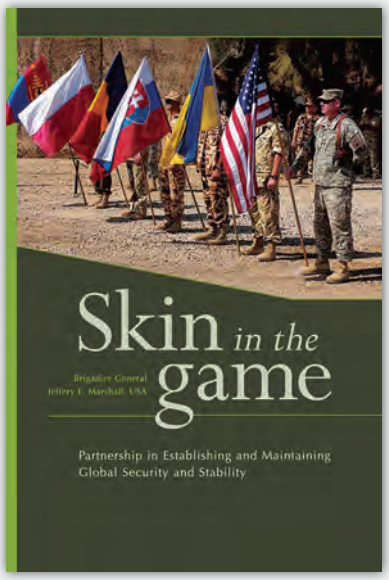
ndupress.ndu.edu

# NEW
## from *NDU Press*


### Partnership for the Americas: Western Hemisphere Strategy and U.S. Southern Command

*by James G. Stavridis*

Admiral James G. Stavridis, USN, reflects on his tenure as Commander of United States Southern Command. Not "your father's combatant command commander," Admiral Stavridis broke with tradition from day one, discarding the customary military model and creating an innovative organization designed not solely to subdue adversaries, but, perhaps more importantly, to build durable and lasting partnerships with friends. From his unique perspective as commander, Stavridis uses his engagingly personal style to describe his vision for the Americas, making the most of limited resources to create goodwill and mutual respect, while taking care of the serious business of countering illegal drug trafficking and responding to humanitarian crises. Citing the hemisphere's common geography, culture, economy, and history, Stavridis makes a passionate case for a common approach and strategy for defending our "shared home of the Americas."




### "Skin in the Game": Partnership in Establishing and Maintaining Global Security and Stability

*by Jeffery E. Marshall, with a preface by James G. Stavridis*

The United States cannot work alone in maintaining the global stability and security that are foundational requirements for all national vital interests. The size of the globe, the plethora of cultures and interests, and the high cost of maintaining stability and security mean that the United States needs partners who share those goals and will share the cost of maintaining them. Sharing the burden in this way actually helps to promote greater stability and security because more countries are invested in the outcome—they have "skin in the game." This book offers a detailed analysis of what the United States must do to build and sustain enduring partnerships, examines the current state of affairs, and provides a roadmap with specific, actionable recommendations to take a more holistic approach to partnerships.

NDU Press

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

# From the Chairman

Across the Nation, there is a growing recognition of the interconnection between energy, national security, and America's future. The emerging concept of *energy security* challenges us to take a holistic view of how we pursue and consume energy as we live and operate in an increasingly complicated world. For our military, enhancing energy security carries even greater benefit—doing so will reduce risk, improve efficiencies, and preserve freedom of action.

Of course, when I was a young naval officer in the late 1960s, energy wasn't something I spent a lot of time thinking about. In those days, serving on a destroyer on the gun line in Vietnam, "energy security" meant knowing where the next oiler was going to be. Like most of America at the time, my shipmates and I operated under a "burn it if you've got it" mentality.

We were not deliberately wasteful or reckless; we just held the conventional view that fuel was cheap, easy, and available without ever really connecting it to any broader geopolitical implications.

Clearly, that is not the world we live in anymore.

The cost, in terms of both blood and treasure, of providing energy to our forces in Afghanistan today and recent headlines of attacks on NATO fuel convoys remind us of these vulnerabilities.

Despite these challenges, there is no doubt that we are making some progress refining how we will consume energy in the future. Secretary Ray Mabus is leading the Navy on an ambitious path to cut nontactical petroleum 50 percent by 2015, and sail the Great Green Fleet by 2016. The Air Force is focusing on the three goals of reducing demand, increasing supply through renewable and alternative sources, and changing the culture. All the Services, in fact, are moving forward with many of our best innovations starting at the grassroots level.

Just recently, the Marines of India Company, Third Battalion, Fifth Marines, out of Camp Pendleton arrived in Helmand Province with a complement of solar-powered electricity-generation capabilities, insulated tents, and ultra-efficient electronics. When we consider that estimates of a fully burdened cost of diesel fuel approach $400 a gallon at some forward operating locations, these benefits can really add up.

This also translates to fewer Marines maintaining fuel distribution systems, fewer Marines dedicating their lives to protecting convoys used to deliver fuel, and more personnel following the theme conveyed at the recent Office of the Secretary of Defense Energy Security Conference: "Saving Energy Saves Lives."

And we cannot think about energy after we get there—wherever *there* may be. Energy security must be one of the first things that we think about before we deploy another soldier, before we build another ship or plane, and before we buy or fill another rucksack. When it comes to future platform design, we too often focus solely on capability while artificially ignoring the environmental and energy costs that all come with a price to pay—some financial, and some that are even more profound and generational.

And the demand for energy is not going to ease anytime soon.

My friend, columnist Tom Friedman, reminds us that this "hot, flat, and crowded" world has introduced 3 billion more people to the global marketplace, all wanting their own version of the American Dream, fueling an ever-growing need for energy to drive the goods and services they are buying to make their lives better.

U.S. Navy (Gregory N. Juday)

**Sailors conduct maneuvers aboard Riverine Command Boat (Experimental) powered by alternative fuel blend of algae-based biofuel and petroleum**

U.S. Navy (Ed Early)

**USNS *Guadalupe* refuels USS *Bonhomme Richard* and USS *Cleveland* while under way in Pacific Ocean**

In short, the world isn't what it used to be, and we can either lead change or be changed by the leadership of others.

In fact, in the National Security Strategy, President Obama writes of innovation being a foundation of American power and leadership. This concept will be critical to achieving energy security in a sustainable world, and we have seen government-led innovations such as GPS, cell phones, and the Internet dramatically benefit our nation and the world.

And this cannot be a top-down effort; true innovation does not work that way. Every one of us, every American, must play a part—changing how we live, how we work, and, perhaps most importantly, how we think about these challenges.

To start with, let's agree that our concept of energy must change.

Rather than look at energy as a commodity or as a means to an end, we need to see it as an integral part of a system that recognizes the linkages between consumption and our ability to pursue enduring interests. The National Security Strategy recognizes these interdependencies, and that strength and stability at home equate to credibility and influence abroad. More specifically, it tells us that the way our nation gains access to, develops, and consumes energy has significant security implications.

And every one of us bears responsibility. We may often think about energy efficiency relative to how we drive our ships, aircraft, and tanks—that is important, to be sure—but we can also make improvements closer to home.

In Twentynine Palms, California, for example, a new micro-grid controller promises to make the Marine Corps' largest base an even better neighbor by reducing its energy consumption, diminishing its carbon footprint, and better enabling it to be independent of California's power grid when needed.

Beyond these immediate benefits, we may even be able to help stem the tide of strategic security issues related to climate change. And regardless of what the cause of these changes is, the impacts here could be far-reaching:

*Near the polar cap, waterways are opening that we could not have imagined a few years ago, rewriting the geopolitical map of the world.*

*Rising sea levels could lead to mass migrations similar to what we have seen in Pakistan's recent flooding.*

*Climate shifts could drastically reduce the arable land needed to feed a burgeoning population as we have seen in parts of Africa.*

*As glaciers melt and shrink at a faster rate, crucial water supplies may diminish further in parts of Asia.*

This impending scarcity of resources compounded by an influx of refugees if coastal lands disappear not only could produce a humanitarian crisis, but also could generate conditions that could lead to failed states and make populations more vulnerable to radicalization. These troubling challenges highlight the systemic implications—and multiple-order effects—inherent in energy security and climate change.

Our efforts here will take planning, and they will take time. Like previous innovations, progress will not be linear—it will come with setbacks and dramatic leaps, just as we have seen in other technological revolutions in the past.

Ultimately, as we gain proficiency in generating sustainable, renewable energy sources, our nation will have the opportunity to pursue not just defense, but security; not just survival, but prosperity—in a word, *sustainability.*

Pursuing energy security, and the sustainability that it ensures, may well be the greatest challenge of our time, one that transcends conventional boundaries of government, business, and nation. We must recognize that this will not be easy and will not come without sacrifice. Yet the need is there, the right technology is emerging, and the time for change is now—our nation, our children, and yes, our grandchildren are counting on us. **JFQ**

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

# LETTERS

**To the Editor—** As a proponent of jointness, I applaud Servicemembers who take an interest in the force structures and operations of other Services and offer constructive suggestions. But as a proponent of careful research and creative and *thorough* analysis, I am appalled by Lieutenant Colonel Shrader's "The End of Surface Warships" *JFQ* 58 (3d Quarter, 2010). Any policy recommendation whose sole source of information is an entry from Wikipedia is premature.

To begin, a force of the "biggest, baddest battleships with the most powerful cannons" never controlled shipping lines. Balanced fleets built around the naval equivalent of combined-arms forces controlled shipping lines. In balanced fleets, battleships were screened, protected, and operated jointly with smaller, more specialized ships such as cruisers, destroyers, submarines, and so forth to provide sea control against possible threats. In the days of sail, supporting the ships-of-the-line were frigates, brigs, armed merchantmen, and a host of specialty attack craft such as mortar and fire ships. Like armor without infantry or air support, battleships never controlled the seas on their own because they would be vulnerable to asymmetric attacks.

What is most disturbing in Lieutenant Colonel Shrader's argument is his lack of understanding how *joint* maritime forces operate at sea and from the sea. The author cites the fact that cruise and ballistic missiles are, at a million dollars a copy, "cheap." But none of those ballistic missiles can actually hit a moving ship at sea. And the ones that might—which China claims to be developing—are not only expensive, but need an extensive and expensive infrastructure. The fact that Hizballah fired off 4,000 missiles to strike fixed land targets has nothing to do with a discussion of moving ships, submarines, and aircraft in maritime warfare. Many of the cheap *cruise* missiles he cites that the United States would face from potential opponents are carried on *surface warships*.

To strike a moving target at sea requires extensive infrastructure including satellites. So let's discuss the author's comments on satellites. Satellites have been considered part of naval warfare since the first satellites were launched; many early ones were developed by the U.S. Navy. Extensive planning was done concerning how surface warships could avoid, spoof, or degrade satellite detection. Thus, satellites did not "change everything." I think most experts would agree that satellites have actually made surface warships more lethal in both land and sea attacks.

Finally, we get to the author's alternative—cargo, troop, and aircraft carrying submarines. The author states that Japanese submarines, carrying one or two aircraft each, were "on their way across the Pacific to blow up the Panama Canal when the war ended." But he did not do enough research to discover that the Navy had recognized that threat in the 1930s; that the small number of aircraft could do little if any damage; or that *we* built or experimented with troop, aircraft, and cargo carrying submarines at the same time (or possibly before) the Japanese (and Germans) did. What *we* discovered is that they were not very effective—with the exception of stealth insertion of special operations forces, which we still do today.

As a retired surface warfare officer, it sometimes pains me (an "outsider" to the submarine force) to admit that the nuclear-powered submarine is indeed the *ultimate warship* for war at sea. But using them to move cargo, aircraft, or large numbers of troops is neither cost effective nor operationally effective. In fact, that would be a waste of a good submarine. Surface warships do missions that submarines cannot do, such as theater ballistic missile defense, or should not do, like counterpiracy. In a maritime campaign, they work together as combined arms, along with other joint forces. Neither replaces the other; even when operating independently, their combined effects are synergistic.

As the author states, "sometimes being an outsider is an advantage" concerning defense analysis. But first, outsiders must do their homework. To those outsiders who would like to understand naval and maritime forces, but with a less daunting learning curve, I can offer an excellent seminar.

**—Dr. Sam J. Tangredi**
**Strategic Insight, LTD**

**To the Editor—** By arguing for disobedience to legal orders in crucial situations at the top of our government, Andrew Milburn's "Breaking Ranks: Dissent and the Military Professional" (*JFQ* 59, 4th Quarter, 2010) threatens the good order and discipline of the U.S. Armed Forces. If his opinions evoke any sympathy among officers serving today, then the article, along with opposing viewpoints, should be assigned and discussed in every military school from precommissioning through CAPSTONE so that it can be exposed for what it is: an attack on military professionalism that would unhinge the American military and put the Nation's safety in jeopardy.

*First*, Milburn's argument makes no sense.

Officers possess no "moral autonomy" except as individuals. The profession of arms does not bestow moral autonomy on officers, and indeed the military in the United States possesses no autonomy whatsoever except that delegated by law and the civilian political leadership. The same goes for each individual officer, by law. Their oaths contain no statements of obedience because that is assumed in the military, as has been true since ancient times, for without discipline and subordination, militaries would be nothing less than armed mobs.

Not only is there no obligation to disobey, but there is no authority—either in law, history, tradition, professional norm, or professional practice. Furthermore, there is no way that officers even at the top are in a position to determine whether an order will "harm . . . the Nation, military and subordinates—in a manner not clearly outweighed by its likely benefits." By their very nature, military professionals possess neither the tools, experience, perspective, nor responsibility to decide the fate of the Nation. And if they did, by what moral or political standard would even the most senior officer make such a judgment about what is good for the country, a Service, or subordinates?

Military operations today are no more complex than those in the past. Throughout history, policy and strategy and operations have interacted often across very loose boundaries, as military thinkers as far back as Sun Tzu and as influential as Carl von Clausewitz have written. Milburn seems ignorant even of their overlap in World War II, often thought to be the model of differentiation between policy, strategy, and operations.

Using a glib trick of language, Milburn introduces the term *check and balance* as though the Constitution raises the military to a status equivalent to the three branches of government. Actually, the Constitution explicitly subordinates the military to each branch and specifically prohibits in every way possible the military from arrogating to itself the ability, much less the obligation, to defy constituted authority. It somehow sounds reasonable to argue that a military

officer should "exercise his discretion" if the three branches are about to commit or allow a disaster and "the military professional alone is in a position to prevent calamity," but how would that work in practice? What officer can make that judgment, on what basis, and how, without violating the oath to support and protect the Constitution? By every stricture of constitution, law, military professionalism, and tradition, the military is accountable to the civilian leadership, not the other way around. Milburn trots out that old, discredited distinction between loyalty and obedience to the Constitution and to the President that Douglas MacArthur used to try to justify his defiance of President Harry Truman's orders, directives, and policies. But everyone knows that the people properly elected or appointed to office embody the Constitution even if they (according to their critics or opponents or the Supreme Court) occasionally violate it. Our system of government operates only through the individuals that the document empowers to govern. How can an officer preserve, protect, and defend the Constitution by ignoring or blocking its proper functioning?

*Second*, the implications of Milburn's arguments promise disaster for the United States. No amount of hemming and hawing about complexity and uncertainty, or invocations of "moral autonomy," can support the disingenuous claims that his "argument does not challenge civilian control of the military." He cites Chile and Argentina, both countries that have experienced coups and military government in recent times. He uses such words as "public defiance." While he rejects his war college peers' endorsement of "leaking the story," "dragging their feet in execution," and other "covert actions" to block civilian authority as improper and unprofessional, Milburn then advocates disobedience, which could not be more improper or unprofessional. That has nothing whatsoever to do with "dissent," a thoroughly misleading word in the title of his article. Advising (and disagreeing with policy or decisions) in the executive branch or Congress in private, or when asked for personal opinions in open testimony, is perfectly proper and indeed obligatory. But trying to overturn or block the decisions of the officials put into office by the American people is altogether different. Think of George C. Marshall in 1942 refusing the Presidential order to round up Japanese Americans on the West Coast because the order might be immoral or illegal (the Supreme Court later ruled in support of the order), or refusing to invade North Africa because American soldiers might be unnecessarily sacrificed at the wrong time and place to defeat Germany (Marshall opposed that invasion). If attempted by more than one officer, or as the product of discussion, disobedience becomes conspiracy and revolt, not exactly "moral" or "professional" by any stretch of the imagination. Think of Vietnam in the 1960s: the chiefs and the commanders in chief (today's combatant commanders), and probably officers and enlisted down the line, joining the demonstrators (to the delight of the Left) in some "professional" version of "Hell no, we won't go!" Indeed, put into practice, what Milburn proposes would not only destroy the good order and discipline of the Armed Forces, as subordinates down the line react to the revolt of their leaders, but also destroy all trust between the military and its bosses—elected and appointed civilian leaders—and its client: the American people—with calamitous results for policy and decisionmaking.

*Last*, Milburn makes some elementary errors. He muddles the most famous historical example (MacArthur never made any "threat to cross the Yalu River"), asserts wrongly that "when the Constitution was written, the army was intended to be only a militia," and that the military has not since 1783 "overstepped its bounds by trying to influence Congress," and even misspells the name of the leading scholar of civil-military relations (Eliot Cohen, not "Elliott").

*In sum*, Milburn's article lacks all credibility: because his sloppiness calls into question his knowledge; because his arguments lack logic and evidence; and because their implications would destroy the armed forces, the Constitution, and democratic government in the United States.

**—Richard H. Kohn, Ph.D.**
**University of North Carolina at Chapel Hill**

**To the Editor—** Civilian control of the military is a cornerstone precept of the American constitutional republic. It brooks no exceptions, no qualifications, no sliding scale of obligation, and no too-clever-by-half reformulation. It is absolute and fundamental—inherited from the British system after Oliver Cromwell's coup was set aside, clearly (even if tacitly) enshrined in the Constitution, and reaffirmed throughout the American military history. Among these affirmations, George Washington's leadership in arresting the Newburgh Conspiracy, Abraham Lincoln's firing of a series of inept and garrulous Union generals, the subjugation of the Combined American Chiefs of Staff's strong preference for a 1943 cross-channel invasion to the strategic priorities favoring invasion of North Africa and then Sicily/Italy as determined by President Franklin Roosevelt in consultation with Winston Churchill, and the sacking of General Douglas MacArthur for failure to align his rhetoric and activities in Korea to the Truman administration's strategic restraint stand supreme.

The immutable concepts and their consistent application have been the subject of ample scholarship and opinion, both by members of the academy and senior uniformed leaders. All have uniformly agreed that the bedrock tenet of service in the American profession of arms is that the military must be servile to elected civilian leadership. It is an instrument of American democracy, not an independent political voice within it.

Lieutenant Colonel Andrew Milburn's article ("Breaking Ranks: Dissent and the Military Professional," *JFQ* 59 [4th Quarter, 2010]), in which he submits that "[t]here are circumstances under which a military officer is not only justified but also obligated to disobey a legal order," dramatically breaks faith with the norm of absolute civilian control in a way that is historically unsound, legally unsupported, morally reckless, and practically dangerous. Fortunately, I find his opinions to be without a uniformed constituency. At most, they may be held by an insignificant minority of fellow officers—and may actually be held by none beyond Milburn himself. In my experience, Marine Corps officers honor the traditional view, casting some doubt on the precise contours of the opinions that Milburn claims represented in his small sample set of War College classmates.

Milburn's theory constitutes authority theft: taking, without permission or sanction, power that constitutionally, legally, ethically, and historically belongs to our civilian masters. This theft breaks faith with the officer's oath, which comes with no stipulation on unwavering obedience of the type Milburn proposes. There is neither precedence nor rationale in American military history for officer obedience to civilian authority only "when morally warranted in the eyes of the assessing uniformed officer." The duty of an officer is *defined* by the orders of civilian superiors—in the administration, Congress, and courts. Therefore, it does not exist independent of civilian direction.

As military professionals, we expect unwavering loyalty and obedience to legal orders, and this is a standard to which our civilian superiors are likewise entitled.

**—LtCol Robert Gray Bracknell, USMC**
**CMC Fellow, The Atlantic Council**

# *Executive Summary*

In this issue's Forum section, *Joint Force Quarterly* examines several issues of contemporary prominence and theoretical concern for counterinsurgency (COIN) operations. Some of the author issues are conceptual and some are operational. Each one impacts the ongoing national security debate regarding America's ability to effectively conduct, much less succeed in, our present wars and in the kinds of conflict we anticipate in the future.

We begin this issue's Forum with an article from Stephen Melton of the U.S. Army Command and General Staff College. Professor Melton takes exception to the broader notions of American military jointness and interagency coordination that have increasingly underwritten overseas U.S. military operations since World War II. He questions the wisdom of strategic-level planning for military operations now conducted within theater-level commands such as U.S. Central Command, calling for a return to pre–Goldwater-Nichols Act days when Service staffs and Joint Staff were the preeminent fashioners of campaign strategy and the operational framework for field commander execution. Melton challenges, directly and indirectly, the recent chorus of policymaker voices championing nonmilitary, interagency leadership in expeditionary operations such as reconstruction, development, governance, and law enforcement. A skeptic of other government agencies in wartime activities, Melton lionizes U.S. military leadership in the successful reconstruction and development efforts in post–World War II Germany and Japan. Bucking the present Washington rhetoric in favor of both more military jointness and a broader interagency mandate and better capacity to lead in complex contingency operations, Melton argues that we would do better to take a step back in organization, doctrine, and policy if we wish to organize, plan, and operate in a manner best able to secure American "victory" in future conflicts.

U.S. Air Force (John Barton)

**Nangarhar Provincial Reconstruction Team members conduct quality assessment of PRT-funded project near Jalalabad, Afghanistan**

Next, Sebastian Gorka and David Kilcullen weigh in on the debate between American COIN proponents and their most ardent critics. They find the parameters of ongoing debate to be narrow and confining, noting that the contemporary American practice of COIN in places such as Afghanistan and Iraq is but one of many historic approaches taken by established states to combat asymmetric threats and irregular military formations. Gorka and Kilcullen assert that the conspicuous American post-9/11 formulation of COIN traces to a construct framed by RAND in 1958, developed by American thinkers and practitioners during the turbulent period of the Vietnam War in the 1960s, and limited to serious study of no more than two dozen anticolonial insurgencies out of nearly 200 irregular warfare events documented in the 20th century, most of which were fought for reasons other than anticolonialism. In this context, they assess contemporary COIN to be but a subset of the far older and much richer vein of strategic thought and practice called counterinsurgency: the art of effectively countering irregular foes. Their appeal? Beware the contemporary COIN formulation as the only, much less the correct, template for modern counterinsurgency. Counterinsurgent states must clearly establish the context of the conflict and define the characteristics of the irregular opponent. Only then can they choose the doctrine and apply the tactics most likely to prevail.

Then, prominent George Washington University sociologist Amitai Etzioni offers some thoughts on the complexities associated with contemporary counterinsurgency operations. Professor Etzioni reminds us that external party participants in COIN operations—such as the United States in Iraq and the North Atlantic Treaty Organization International Security Assistance Force (NATO–ISAF) in Afghanistan—face a host of cultural, religious, ethnic, and subnational challenges. These make objective realization of counterinsurgency goals challenging. The challenges exist within the country of conflict and from the interest group alignments found in the polity of the external participants. Assessing the "perspectives gulf" between these diverse sets of subnational actors to be underappreciated, Etzioni chronicles a host of important, yet seemingly innocuous, areas where divergent perspectives can decisively frustrate the most well-intentioned counterinsurgency aims. His Iraq- and Afghanistan-based examples should resonate with American strategists and practitioners, as they include samples of cognitive divergence in concepts including corruption, gender roles and rights, judicial fairness, and the role of religion. Etzioni's caution is one of prudence in aim, for third-party overambition in objectives can only doom to failure the inherently complex undertaking of counterinsurgency.

This Forum also presents two articles addressing a major challenge faced by the United States in its protracted counterinsurgency ventures in Iraq and Afghanistan: civil-

U.S. Marine Corps (Evan Barragan)

**Members of Marine Female Engagement Team interact with Afghan women and children through an interpreter in Helmand Province, Afghanistan**

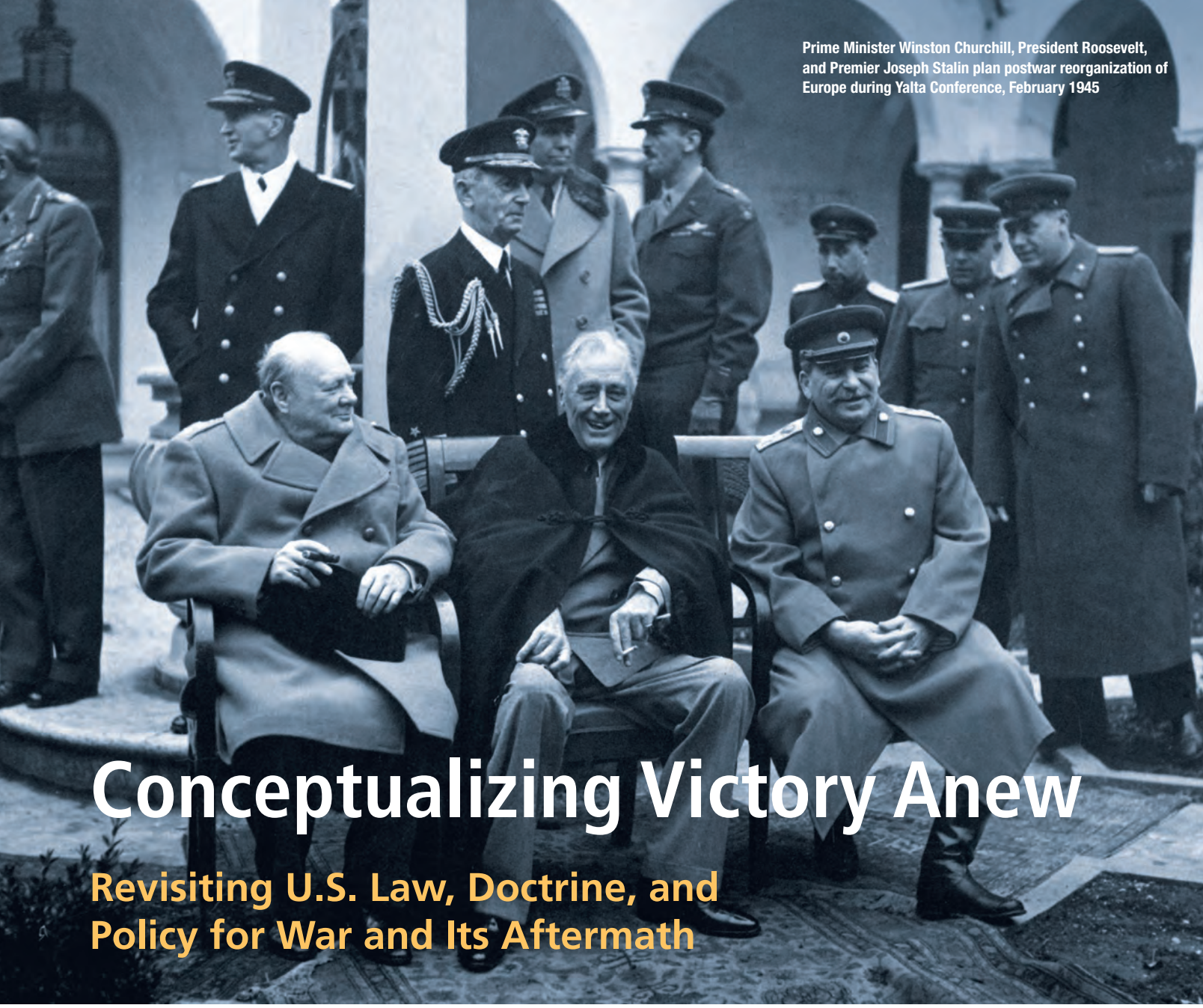
ian contractors and approaches toward local contracting in conflict zones.

T.X. Hammes of the Institute for National Strategic Studies (INSS) at the National Defense University presents conclusions from his recent INSS *Strategic Forum* on the topic of contractors in conflict zones. He chronicles the multifaceted implications—good and bad—presented by the phalanx of contractors working astride U.S. military forces in Afghanistan, Iraq, and states across the Near East and South Asia. Dr. Hammes confirms the indispensable role performed by contractors in support of American military operations since 9/11, including the manner in which their expansive presence has alleviated pressures for a wider American military mobilization to prosecute ongoing wars. But he also catalogues the plethora of issues arising from the roles performed and the relationships established by contractors in America's ongoing COIN efforts. These issues run the gamut from those of contractor accountability, to host-country perceptions of contractor behavior in relation to U.S. strategy and its legitimacy, to the potential for understatement of human and financial costs in American military planning for future contingency operations. Hammes's recommendations for new policies and procedures that maximize the value and minimize the risks from contractors in conflict zones might not sit well with those wedded to the present system. Yet they should resonate with the millions who have served as, or have directly worked with, U.S. contractors in the expansive areas supporting Iraq and Afghanistan.

The Forum section concludes with U.S. Army Captain Jonathan Pan offering a personal review and a policy critique of U.S. and NATO local contracting efforts in Afghanistan. Informed by his experiences as an economic development officer for the Army's 5th Brigade/2d Infantry Division Stryker Brigade Combat Team deployed near Kandahar in 2009–2010, Captain Pan paints a vivid picture of the adverse tactical effects from standard NATO contracting practices in that city and its surrounding area. Pan highlights the challenges from standard Western contracting practices and procedures applied to the unique, Spartan environment of southern Afghanistan. His vignettes stand as testimony to frustrations experienced by a legion of nongovernmental and governmental organizations attempting to do contract business in incredibly poor countries with few skilled workers, still fewer qualified companies, and a culture of local strongmen profiteering from outside financial investment. Captain Pan points out the desperate need for a coherent NATO contracting policy in Afghanistan, one clearly absent during his time there. For Pan, any viable policy should first recognize the inherent, and uncomfortable, tradeoff faced by local contracting agents between accomplishing time-sensitive contracted outcomes (brick and mortar as well as those to do with human services) with the often negative second- and third-level governance and economic effects from the contracting process itself. Captain Pan's recommendations seem to be in line with the thinking of NATO–ISAF senior leaders, for they empowered a special contracting task force during the spring of 2010 to resolve growing concerns that Western contracting was exacerbating local Afghan corruption. It remains to be seen if that task force can get to the heart of the challenges chronicled—and fulfill the recommendations made—by Captain Pan.

In the Features section, *JFQ* offers four articles that speculate directly and indirectly about the possibilities and "what-ifs" that America and its allies might face in the event of some future military confrontation with China. U.S. national strategy remains focused on dialogue, engagement, and the prevention of such a clash. The May 2010 U.S. National Security Strategy calls for deeper cooperation with China, India, and Russia, naming them as three of the important emerging centers of influence in the 21st century. In its 2010 report to Congress on China, the Department of Defense highlighted that it continues to prioritize exchanges with the Chinese military to help build cooperative capacity, foster understanding, and develop common views on the international security environment and related security challenges. Secretary of Defense Robert Gates met with his Chinese counterpart, Liang Guanglie, on the side at an October 2010 Southeast Asian Defense Conference in Hanoi, Vietnam. There, the Secretary accepted Liang's invitation to visit China in 2011, thawing a chill in military-to-military relations that had dominated 2010 after the January announcement of additional U.S. weapons sales to Taiwan. At the same time, American defense policymakers and China experts remain broad-minded in thinking about and planning for unwelcomed outcomes. The 2010 Quadrennial Defense Review observes that "China has shared only limited information about the pace, scope, and ultimate aims of its military modernization programs, raising a number of legitimate questions regarding its longterm intentions." Our civilian and military Features authors write concerning these questions. *JFQ* readers might best consider their thoughts as insights into what the future may hold *if* American aims for a collaborative future with China go unrealized, *not* from a conclusion that such an outcome is desired or inevitable. **JFQ**

**—T.F. Lynch III**
**Acting Editor**



Prime Minister Winston Churchill, President Roosevelt, and Premier Joseph Stalin plan postwar reorganization of Europe during Yalta Conference, February 1945

NARA

# Conceptualizing Victory Anew

## Revisiting U.S. Law, Doctrine, and Policy for War and Its Aftermath

*By* STEPHEN L. MELTON

*The victorious strategist seeks battle only after the victory has been won, whereas he who is destined to defeat first fights and afterwards looks for victory.*

—Sun Tzu

**Lieutenant Colonel Stephen L. Melton, USA (Ret.), is an Assistant Professor in the Center for Army Tactics at the U.S. Army Command and General Staff College. His most recent book is *The Clausewitz Delusion: How the American Army Screwed Up the Wars in Iraq and Afghanistan (A Way Forward)* (Zenith Press, 2009).**

As we lick our many wounds and salvage what we can from our costly and confused wars in Iraq and Afghanistan, it is urgent that we address the intellectual errors that paved the way for our lack of success, lest we risk underperforming in future military endeavors as well. This article introduces four strategic "reframes" of our postmodern conceptualization of warfare that are needed to restore the effectiveness the American military was accustomed to through World War II. The goal is not to rehash the sins of the past few wars, which have been amply exposed in numerous writings, but to illuminate a path forward.

### Reframe 1

Wars must be won first at the strategic level, then at the operational level, and then at the tactical level. Our strategic-level lodestones—the National Security Act of 1947 and Goldwater-Nichols Department of Defense Reorganization Act of 1986—have created cross-purposes at the strategic level of war and have proven inadequate in producing victory in war. These laws must be rewritten to ensure strategic unity of command.

Sadly, the record of the U.S. military since World War II is mainly half-victories and defeats: Korea, Vietnam, Iraq, and Afghanistan. Despite valiant efforts by Servicemembers in the tactical units, numerous battlefield victories, and enormous costs

borne by the taxpayers for standing forces and wartime supplemental expenditures, the Department of Defense (DOD) has produced disappointing results in the conflicts it has directed. The systemic failure occurs at the strategic level.

Because our military professes to have "strategic corporals," theater-level strategic commanders, and battalion commanders performing operational art—all of which are oxymoronic formulations—I propose the following clarification regarding the strategic, operational, and tactical levels of war, which are consistent with Army doctrine prior to 1986.

The *strategic* level resides primarily in Washington, DC, and consists of the President, his Cabinet and advisors, Congress, DOD, and Departments of the Army, Navy, Air Force, and other agencies. These are the organizers of victory who calculate and justify the need for war, determine its aims and objectives, and raise and train the various armed forces needed to fight it. They fund war, declare it, coordinate and prioritize responses to the various unforeseen events, and finally terminate it once its political objectives are reached. Moreover, the strategic level must conceptualize and institutionalize the tactical and operational methods the military units will employ to win the war, to include training and equipping individual Servicemembers and units of all sizes. A seamless synthesis of the entire war effort across all levels and warfighting functions—from the Oval Office, to the industrial base, to the individual foxhole or battle station—can only be done at the strategic level.

The military's *operational* level commanders, the four-star combatant commanders in U.S. Pacific Command, U.S. Central Command, U.S. European Command, and elsewhere, are entrusted to execute the decisions made in Washington within their areas of operation and with the forces they are assigned. They may advise the strategic decisionmakers, but they are executors, not deciders, of strategic policy. Their job is to employ the forces assigned to them in the most efficient and effective manner possible within the constraints of the overall strategy. The *tactical* level consists of the Servicemembers and units—Army divisions, air wings, naval task forces—that actually do the fighting, dying, and rebuilding.

The current failure of the Nation to properly organize its strategic center traces back to the National Security Act of 1947, which placed overall responsibility for coordination and integration of the military effort in the civilian-dominated National Security Council and Office of the Secretary of Defense. A primary shortcoming was that the act deliberately opted "not to establish a single Chief of Staff over the armed forces nor an overall armed forces general staff."[1] Having eschewed the successful models of strategic leadership offered by the World War II era, during which both the Army Chief of Staff and Chief of Naval Operations exercised staff as well as command authorities, the ambitious 1947 reform sacrificed a clear and enforceable system for centralized military command in favor of assured civilian control, hoping that the creation of an overarching DOD would enable coordination, integration, and unity of effort among the various departments, agencies, and staffs. The act created the national security system that failed to win in either Korea or Vietnam.

Attempting to fix the inter-Service rivalries and other shortcomings of the 1947 reform—made manifest by Vietnam, Operation *Desert One*, and Grenada—the Goldwater-Nichols Act further diminished the role of the Pentagon by making the *operational* commanders the primary war planners, moving a critical *strategic* function away from Washington. Rather than reforming the flawed warfighting abilities of the Pentagon, the 1986 law sought to bypass the established strategic military structure altogether and create new "theater strategic" headquarters around the combatant commanders. The act enhanced the relationship between the highest civilian leaders and operational combatant commanders overseas, but by doing so relegated the military's strategic center—the Joint Chiefs of Staff and military departments—to an advisory and supporting role.

The results in these two-and-a-half decades since Goldwater-Nichols have been embarrassing for the country: not thinking through the cease-fire terms during *Desert Storm*, the vacuum of effort in Afghanistan after the fall of Kabul, and the failure to adequately plan for the occupation of Iraq.

The theater strategic model has failed for two main reasons. First, the inherent lack of strategic vision and experience in the operational headquarters militates against getting the planning right, except perhaps the kinetic part. For instance, who on General Tommy Frank's 2001 U.S. Central Command (USCENTCOM) staff had previously planned and executed a successful invasion and occupation of a hostile foreign country and then installed a new government acceptable to both that country's population and the United States? The necessary perspective and experience, largely dating from World War II and its aftermath, reside mainly in the historical archives in Washington. The young men on the USCENTCOM staff, rotating through their billets on their all-too-brief assignment cycles, could never match the institutional wisdom that must be maintained in Washington. Neither can an operational commander employ troops and units that the strategic level has not already envisioned, procured, equipped, trained, and deployed to the theater of war. Force creation, flow, and rotation are strategic functions largely beyond the control of the operational commander.

*the military's operational level commanders may advise the strategic decisionmakers, but they are executors, not deciders, of strategic policy*

Second, the multiple centers of strategic thinking and authority—political leaders, the Joint Chiefs of Staff, and various combatant commanders—lack the firm central direction that can assure the needed unity and consistency of effort. Indeed, the proliferating ranks of four-star generals and admirals, with their overlapping and competing responsibilities, often seem more interested in staking out turf and pursuing pet agendas than winning wars. As a result, Service chiefs quarrel with overseas combatant commanders; combatant commanders spar with their operational commanders; political appointees bicker with the uniformed Service chiefs; and opportunistic politicians publicly champion like-minded generals and admirals. Acting as the main referee in this chaotic system, the President has been forced to relieve or replace operational commanders in all our major conflicts of the past 60 years—General Douglas MacArthur in Korea, General William Westmoreland in Vietnam, Lieutenant General

U.S. Navy (Todd Frantom)

**Airmen pose at monument in Baghdad commemorating Saddam Hussein's declaration of victory in Iraq-Iran war**

Ricardo Sanchez in Iraq, and Generals Stanley McChrystal and David McKiernan in Afghanistan. The National Security Act and Goldwater-Nichols have led to the piecemealing of authority and culpability at the military's strategic level and created the conditions for poorly conceptualized, planned, orchestrated, and resourced wars, resulting in Pyrrhic battlefield victories and disappointing postwar governance and stability outcomes. Too often we have been lured by operational commanders into, to paraphrase and expand on General Omar Bradley's assessment of the Korean War, fighting the wrong war in the wrong place against the wrong enemy in the wrong manner.

Somehow, we must simplify the military's strategic apex, better subordinate the operational commanders to the Pentagon, and insist that the Pentagon do its job. The strategic leadership should not be allowed to dodge its warmaking responsibility by proclaiming it is giving the operational commander what he requested. Rather, it is the role of the strategic leadership to determine and provide the ends, ways, and means of the war, and allow the operational commanders to focus on the critical functions only their headquarters can accomplish—the detailed coordination and integration of the actions of the tactical units under their respective commands.

Consequently, strategic *command* of all operational forces must be invested in the Joint Chiefs of Staff. Supported by a joint planning and operations staff, the up-gunned Joint Chiefs would become a warfighting headquarters directly supervising subordinate combatant commanders in their areas of responsibility around the world. The military's strategic leaders should not be burdened with mundane bureaucratic requirements as are our current Service chiefs. Freeing the various chiefs of staff to think through and organize victory, uniformed deputy chiefs of staff from the respective Services would support Joint Chiefs decisions with the necessary programming, coordination, and budgetary requests, while also exercising oversight over force generation, equipping, training, and other support tasks. At the highest level, busywork should never be allowed to drown out purposeful thinking about global military strategy and victory in war.

## Reframe 2

The current joint and Army focus on *operations*, however relevant at the operational level of war, is not helpful in winning *wars*, which must of necessity be conceived, resourced, and executed at the *strategic* level.[2] From a strategic level, wars are most powerfully described as offensive, defensive, and limited objective, and the operations and tactics of a war are best understood in that typological context. Current joint and Army doctrine, known as full-spectrum operations, denies that there are distinct types of wars, promulgates no positive theory for obtaining victory in war, and is not a sufficiently powerful way of thinking about present or potential wars.

The Army's first version of full-spectrum operations doctrine was published in June 2001, having been drafted in the strategic abyss that began with the end of the Cold War. The doctrine boils down to two banal

observations: that Army forces work as part of a joint and interagency all-of-government team, and that Army units conduct a gamut of offensive, defensive, and stability tasks in different proportions for each mission as required. Our wars since 9/11 have not vindicated the doctrine, but rather have exposed its manifold flaws: its failure to state a positive theory of victory in warfare, its failure to acknowledge types of wars, its operational and tactical focus, and its failure to properly affix primary responsibility for occupation and stabilization.

As bad as Army doctrine has become, the problem is worse at the joint level, not because the doctrine is different than the Army's, but because it merely mimics the Army's full-spectrum operations themes. Focused on the overseas joint force commander—the operational level of war—the joint doctrine fails to discuss or clarify for the reader the most important level of war: the strategic. Rather, the doctrine assumes that the strategic guidance delivered by the proper authorities is appropriate for the situation at hand, meaning the burden for delivering victory now rests with the operational commander. Amazingly, the terms *war* and *victory* are never defined or discussed in joint doctrine as it attempts to mention and categorize the full range of military *operations* against a backdrop of "persistent conflict."

In the view of the full-spectrum operations theorists, wars contain a combination of offensive, defensive, and stability *operations*, but wars themselves are not considered to be *strategically* offensive, defensive, or stabilizing in nature. Our doctrine makes no *strategic* distinction, for example, between the historical World War II that actually happened—the one that began with Germany invading its neighbors—and an alternative hypothetical war that would have begun with the Allies invading Germany. Both wars are equivalent "contests of will."

The failure to distinguish between types of wars constitutes a mortal doctrinal flaw. The terms *offense* and *defense* should categorize not only different types of operations and tactics, but also different kinds of wars at the strategic level.

*Offensive wars* are characterized by the invasion of another country with the intent of replacing its government with one more suitable to the invader's purposes. Success in these wars requires conventional offensive military operations, unconventional counterinsurgency operations, and the invader's governance of the occupied population until a new indigenous government installed by the occupier gains the acceptance of the population. These wars not only are difficult to win, but also require tremendous resources and a decade or more of effort, as Iraq and Afghanistan illustrate. Modern history demonstrates that initiators of offensive war rarely achieve the enduring victory they promise.

*Defensive wars* are fought to protect a nation's government from foreign or internal enemies, as well as to safeguard the property and citizens of that nation and its allies. Success requires the defender to raise the aggressor's real or perceived cost of pursuing the war to the point that initiating or continuing the war becomes disadvantageous to him. Defensive wars tend to follow a progression of strategies—beginning with deterrence and proceeding in turn to conventional defensive operations, guerrilla warfare, terrorism, civil disobedience, and finally useless and costly passivity. The modern historical record counsels that one of these strategies, whether sooner or later, will likely succeed in making the attacker cut his losses and return home. Counteroffensive operations to liberate occupied territory are often part of defensive wars. Similarly, stability operations and security force assistance missions are correctly seen as defensive in nature because they support and strengthen established governance systems. The Cold War, from the North Atlantic Treaty Organization perspective, was conducted as a preparation for defensive war.

*Limited objective wars* are fought to change other nations' behaviors, to redraw boundaries, or for other purposes, but are not aimed at changing the governance of either of the combatants. Often one party is clearly the aggressor, but just as often opinions differ regarding which side is in the right. The main point is that the domestic governance in both combatant countries is not at issue and both sides strive to contain their violence to resolving the specific issue at hand. Controlling escalation is a primary concern. The Falklands War of 1982 is a recent example of a limited war.

The differences between the three types of war are supremely significant not only at the strategic level, but also at the operational and tactical. Not only are the war aims distinct, each envisioning different postbellum outcomes, but each type of war requires radically different ways and means, to include diplomacy, justifications, narratives, phasing, force structure, defeat mechanisms, expense, troop organization and training, and time horizons. The nature of these differences—so critical to properly organizing for victory in any envisioned war—is lost in the military's new and disappointing doctrine.


NARA

**UN forces withdraw from Pyongyang, North Korea, 1950**

**Reframe 3**

In *offensive war*, the land component commander, who is generally the senior Army commander, must be tasked to perform military governance over the occupied population, and the Department of the Army must be tasked to provide him the necessary specialized units—manned, organized, trained, and equipped—to execute the military governance mission. Our current "unity of effort" approach led by the Department of State is a blueprint for disappointment at best, but more probably failure.[3]

Basic Field Manual 27–5, *Military Government*, published in 1940, was the pithy (only 57 paragraphs) doctrinal publication that paved the way for our occupation and rebuilding of our World War II enemies, which we rapidly and successfully transformed into willing partners and allies. Its ideas were simple but powerful: unity of command; specially selected and trained governance Soldiers in military uniform, organized to supervise the preexisting enemy government; Army responsibility to generate and train the military government forces in the needed numbers; and the requirement to establish military governance immediately on the heels of offensive combat operations.

Had we repeated our World War II doctrinal prescription in Iraq and Afghanistan, we might have been able to seize the "golden hours" provided by our successful initial combat operations. Instead, we ad-libbed our occupations, and in doing so left vacuums of authority in both countries that still damage our credibility, undermine our noble purposes, and play into the hands of forces opposed to our interests.[4] After failure seemed imminent in both countries, the President had to order military "surges" as a belated effort to retrieve the situations and build something positive.

Our path in our current wars was first to ignore or minimize the governance problems our invasions would create, then to place State Department civilians in charge of the stabilization and reconstruction missions (consider Ambassador L. Paul Bremer and the Coalition Provisional Authority in Iraq, 2003–2004, and National Security Presidential Directive 44, "Management of Interagency Efforts Concerning Reconstruction and Stabilization," in 2005). As these approaches failed, DOD found it necessary to issue Directive 3000.05, "Military Support for Stability, Security, Transition, and Reconstruction (SSTR) Operations," acknowledging the State Department lead but cautioning that "U.S. military forces shall be prepared to perform all tasks necessary to establish or maintain order when civilians cannot do so."[5] Still, employing mostly Army capabilities within the framework of a civilian-led effort has proven only marginally successful, due to the "lack of integrated capability and capacity of civilian agencies with which the military must partner."[6] Nearly a decade into our occupation of Afghanistan, the civilian-led "all-of-government" approach is still understaffed, poorly resourced, and producing inadequate results.

The final coordinating draft of Joint Publication 3–07, *Stability Operations*, dated April 22, 2010, greets the reader with more than 200 pages of vague and confused text. A testament to the State Department's new lead in postconflict stability, the manual tasks no Service chief or military commander to be responsible for anything specific, but merely enumerates stability operations functions and considerations, all the while stressing their criticality. The thrust of the manual is that "we" collectively have much to do, with no one "tasked" specifically to do it. This is, of course, a doctrinal blueprint for disaster.

*having the military responsible for winning the kinetic war, but not the peace, creates a schism at the all-important moment when populations assess their new occupiers*

Having the military responsible for winning the kinetic war in what the military has come to term *phase 3*, the decisive fight, but not responsible for winning the peace in phase four, stability and reconstruction, creates a counterproductive schism in command authority and accountability at the all-important moment when populations assess their new occupiers and form lasting impressions. The precedents established in that critical transition, for better or worse, will color all the efforts that follow. Commanders must employ armed force in a manner consistent with the peace ultimately desired, the former leading directly into the latter.

It is probably too late in the game to salvage "victory" in Iraq and Afghanistan; our moments of opportunity in both those countries are likely long gone. But we can at least recognize and correct the faulty constructs that led us to unsatisfactory results in our current wars. Offensive war and its aftermath—occupation—must be a land component commander—that is, Army—responsibility, supported by the other Services and agencies.

NARA

**Sailors spell out "Victory" at Great Lakes Naval Training Station, 1917**

### Reframe 4

The urgent doctrinal need now is to develop strategic concepts likely to deliver victories in defensive and limited wars. The disappointments and costs of Iraq and Afghanistan make it less likely that we will initiate new offensive wars in the near future, and more likely that we will have to defend our interests abroad.

Not all wars need to end with our occupation of foreign populations, converting our former enemies into future allies at enormous cost. We can defend our interests and allies without invading enemy nations. We can challenge the threatening behaviors of our adversaries without demanding their unconditional surrender. However, we will need to abandon our recent grand strategy of military expansion, largely through offensive war, and instead hone our thoughts regarding defensive war.

Urgently, we must prioritize our interests abroad and balance means, which are likely to shrink as we reduce our budget deficit, with ends. We must also review our methods of defense, choosing lower cost options whenever possible. Inevitably, we must force our allies to shoulder more of their own defensive burdens as we increasingly assume a supporting role. The U.S. military should never be the reflexive force of first employment abroad, it being better for us to assist allies than to assume their burdens outright.

Our strategic adversaries are expert at using proxy wars—wars fought for them by their local allies rather than their own forces—to advance their interests and damage ours. Our counterstrategies to date have been largely ineffective and wasteful, failing as they do to affix responsibility and punish accordingly.

Our primary challenge going forward will not be our current focus, the radical Islamic terror campaign against American modernity and power, but rather the ascent of China, which could become the world's hyperpower within decades. That nation will force us to adopt a defensive strategy, testing our alliances in the Pacific and Asia and, indeed, throughout the world.

It is unlikely that China will be satisfied with incorporating itself into the American "Washington Consensus" that we built and institutionalized after World War II; rather, it will endeavor to pigeonhole the United States into a subsidiary role in China's emerging global version of the old "Middle Kingdom."[7] The Chinese are foreign power realists, not liberals, and tend to view power as a zero-sum game.[8] Their relative national power can rise only if ours falls.

Chinese notions of harmony suggest that we must be taught to accept our new tributary status. Reward (for example, profitable trade for U.S. corporations and U.S. Treasury debt purchases for now) will increasingly be mixed with punishment, as China asserts its interests through hybrid or "unrestricted" warfare.[9] Many of the lessons will be delivered by China's growing global network of proxies—that is, North Korea, Iran, and perhaps Venezuela. Others may be delivered directly by Chinese forces following their new doctrine of "high-tech local wars."[10]

Strategically, we must determine the art of the possible regarding our relationship with Beijing and develop an achievable endstate for the emerging new world. Operationally, we must think through how we will respond to Chinese strikes, military and nonmilitary, within that strategic context. We must appreciate that our reactions will set precedents that will redefine our relationship with China and, indeed, the world, and that we have a low probability of reacting correctly if we have not anticipated and thought through our counteractions ahead of time. Accordingly, we must develop defensive and limited war doctrine and plans, focused on parrying challenges without risking unwanted escalation or setting adverse precedents.[11]

### No Substitute for Victory

The American citizenry needs to establish higher expectations for military competence—a new standard that the Pentagon must get the war right before it even begins, not blunder through years of painful and costly heuristic learning as the prospect of victory diminishes. Modern kinetic wars are measured in a handful of days. Golden hours in occupation are ephemeral. The opportunity for military success is often presented only once. Miss that precious moment, and we will ultimately fail, even though we may labor many more years before we come to that realization. We have simply got to wage the war right the first time.

A military as lavishly supported with both talented people and resources as America's can—and must—do better than it has over the past decades in defining and achieving victory. As we honored our dead this past Memorial Day, I could not help but consider whether our strategic military establishment is "organizing the victory" as effectively as it could, or needs to. As heroic as our Servicemembers are at the tactical level where the bullets fly and the dying gets done, our privates, sergeants, and lieutenants cannot redeem the strategic errors made in Washington. We should heartily question whether the Nation's legal and intellectual constructs regarding war are as powerful and productive as they proclaim, or are flawed to the point that we are squandering the power of the Nation and the efforts of our most patriotic young citizens. The evidence gathered from our recent wars suggests the worst case. We can and should do better. **JFQ**

#### NOTES

[1] The National Security Act of 1947, section 2.

[2] For a more detailed discussion, see Justin Kelly and Mike Brennan, *Alien: How Operational Art Devoured Strategy* (Carlisle Barracks, PA: Strategic Studies Institute, September 2009).

[3] See also Russell R. Hula, "Stability Operations and Government: An Inherently Military Function," in *Short of General War: Perspectives on the Use of Military Power in the 21st Century*, ed. Harry R. Yarger (Carlisle Barracks, PA: Strategic Studies Institute, April 2010).

[4] An excellent firsthand account of our ill-considered and poorly executed stability efforts can be found in Sarah Chayes, *The Punishment of Virtue: Inside Afghanistan after the Taliban* (New York: Penguin Press, 2006).

[5] As cited in Roger S. Marin, "Finding an Exit: Delineating Battle Handoff in Phase IV," in *Short of General War*, 234.

[6] Ibid.

[7] For starters, read Martin Jacques, *When China Rules the World: The End of the Western World and the Birth of a New Global Order* (New York: Penguin Press, 2009).

[8] John J. Mearsheimer, *The Tragedy of Great Power Politics* (New York: W.W. Norton, 2001), 375.

[9] Qiao Liang and Wang Xiangsui, *Unrestricted Warfare* (Beijing: People's Liberation Army Literature and Arts Publishing House, February 1999).

[10] Peng Guangquin and Yao Youzhi, eds., *Science of Military Strategy* (Beijing: Military Science Publishing House, 2005).

[11] Forrest E. Morgan et al., *Dangerous Thresholds: Managing Escalation in the 21st Century* (Santa Monica, CA: RAND, 2008)

Soldiers and Afghan National Police coordinate security for Afghan national election, September 2010

U.S. Army (Chris G. Neeley)

# An Actor-centric Theory of War

## Understanding the Difference Between *COIN* and *Counterinsurgency*

*By* SEBASTIAN L.v. GORKA
*and* DAVID KILCULLEN

*Everything in war is very simple,*
*but the simplest thing is difficult.*

—Carl von Clausewitz

**Dr. Sebastian L.v. Gorka teaches on the Faculty of the College of International Security Affairs at the National Defense University and is Military Affairs Fellow with the Foundation for Defense of Democracy. Dr. Gorka is contributing author and coeditor of *Toward a Grand Strategy Against Terrorism* (McGraw Hill, 2010). Dr. David Kilcullen is a Counterinsurgency Advisor to the North Atlantic Treaty Organization, International Security Assistance Force, the U.S. Government, and other governments. Dr. Kilcullen is the author of *The Accidental Guerrilla* (Oxford University Press, 2009).**

The United States, the most powerful nation in the world, is reassessing its approach to war. With America entering the 10th year of what was originally called the global war on terror, the Nation finds itself engaged in conflicts in Central Asia and the Middle East that challenge decades of planning, training, and doctrine. Although collectively this series of campaigns recently crossed the marker-point for America's longest combat engagement ever, arguments persist—even in the pages of this publication—as to whether we have the correct approach.[1]

This debate is, for the most part, limited in scope.[2] In general, it can be summarized as revolving around one contentious point: whether one agrees with the idea that the United States must redefine its fighting capacity based upon irregular threats—such as insurgency—or not. On the one hand, we have the proponents of a counterinsurgency, or COIN, approach often associated with one of Washington's newest think tanks, the Center for a New American Security, and its energetic president, retired U.S. Army Lieutenant Colonel John Nagl.[3] In brief, the argument on this side of the current debate is that the U.S. Army (note, *not* the U.S. Marine Corps) deliberately shunned irregular warfare, and counterinsurgency in particular, after it was "not allowed" (politically) to win the Vietnam war.[4] Only when faced 30 years later in Iraq with an insurgency that seemed to be winning did the uniformed establishment return to the library of irregular warfare and, under the leadership of General David Petraeus, rewrite and embrace this form of war in the shape of revised Field Manual 3–24, *Counterinsurgency*.[5] This doctrinal revival, so the story goes, was operationalized in the "surge" that stabilized Iraq. The strongest proponents of this rediscovery and renewed emphasis on counterinsurgency see the future as predominantly shaped by irregular challenges and thus argue for an approach to the use of force that sees conventional warfare as passé (at least for the time being). Some go on to assert that future conflicts will be determined less by the kinetic effect of our units and their weapons than by the "shaping" and influence that we bring to bear nonkinetically and, additionally, that the adaptability of America's forces is paramount.[6]

On the other side, we have experienced experts, such as Army Colonel Gian

Gentile—who has made a name for himself by writing of the "cult of COIN"—who are convinced that the recent war on terror–driven overemphasis on COIN seriously degrades the essential core combined arms competencies of the Army, such as artillery, and that we must "return to basics" if we are to maintain essential national security capabilities.[7] To some observers and commentators, COIN is an ambiguous concept that has gained such popularity because either side of the political aisle can emphasize very different policies under the same doctrinal banner—aggressive kinetic approaches for the right, softer nation-building priorities for the left.

We believe that neither side of this argument has a monopoly on the truth. Rather, the question of how America should and could apply force in the post–Cold War and post-9/11 environment can be answered only after taking a more historic perspective, which places Iraq and Afghanistan into a far broader and richer context than just the last few decades. Additionally, we need to be aware of the fact that *COIN—in the American mode—is but one small reflection of the much older, even ancient, practice of countering* insurgents, or irregular enemies. Finally, we propose that a theory of war based on who is using violence against us makes much more sense today than theories based on putative generational changes in warfare or the asymmetry of combatants.

## Irregular Warfare at the Meta-level

COIN, as the U.S. Armed Forces and policy elites currently understand it, is an intellectual fad, a way to think about irregular warfare. Before COIN, there was "asymmetric warfare," before that, "AirLand Battle." Next will come another transitory doctrinal lens such as "stability operations" to replace COIN, and another lens after that. While war against nonstate actors using unconventional means has existed for millennia and under many names (such as "tribal warfare" and "small wars"),[8] COIN, as the Western world understands and uses the concept, developed out of key meetings at the RAND Corporation in 1958.[9] Yet the activities so described should be understood as a specific subset of the overarching, far older activity of counterinsurgency. The doctrinal principles that resulted—eventually in FM 3–24—were shaped not by the lessons of past centuries of war against nonstate actors but by the limited experiences of Western nations during the 20th century. In fact, COIN is but one small example of the various forms of warfare the world has witnessed over time. These forms can be classed with regard to the characteristics of the parties involved—State versus State, State versus nonstate actor, or conflict among nonstate actors (see figure). We argue that these constricted foundations upon which classical COIN doctrine was built have not only distorted our understanding of the current threat environment but also dangerously limits our ability to defeat current and future enemies.

## Data and Doctrine

The Army's rediscovery of COIN theory following the U.S. invasions of Afghanistan and Iraq led scholars and officials to revisit case studies and doctrinal texts on the subject long overlooked by political and policy analysts. The drastically deteriorating events in Iraq were followed by the wholesale return of serving officers and strategists to the study of classic texts on previous insurgencies, foremost among them Frank E. Kitson on Northern Ireland, Roger Trinquier and David Galula on the French experience in Algeria, as well as Robert Taber's original *War of the Flea,* and, of course, the works of T.E. Lawrence (of Arabia), in an effort to relearn that which we once knew.

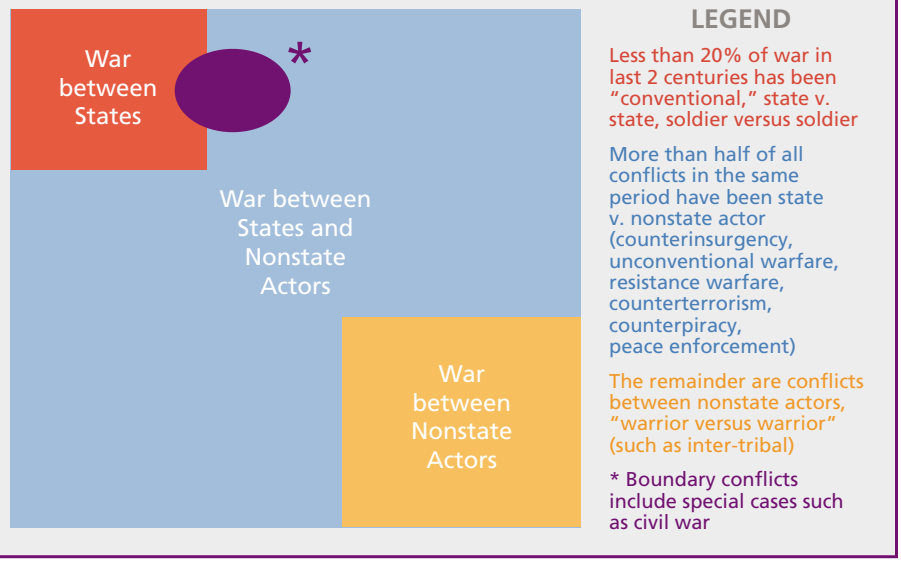
As a result, thanks in part to mass media coverage and the exposure of theater commanders such as Generals Petraeus and Stanley McChrystal, millions of people across the Nation are familiar with COIN concepts such as "winning hearts and minds" or "clear, hold, build." Nevertheless, despite this nationwide doctrinal revival, two disturbing issues lay unresolved.

First, for some opaque reason, the list of conflicts that the military and academic worlds examine under the category of "insurgencies" is incredibly restrictive and ignores many cases of irregular warfare that could be included without undue justification. (In most cases, these ignored conflicts have for some reason been labeled civil wars or revolutions and not insurgencies.) Second, despite the number of canonical texts and individual and comparative studies, no one has attempted a categorization of previous COIN cases that differentiates among the original conditions at the start of a given conflict and the eventual strategic endstate that it wished to achieve.

Together, these two factors—the restriction of COIN analysis to just a handful of famous 20th-century cases and the mistake of examining each doctrinally without first separating them based upon the strategic aims of the government and the political, economic, and military point of departure—have greatly distorted what can be learned from existing examples of irregular warfare and what in fact the lessons for today may be. If the data set of COIN analysis is enlarged to include other 20th-century conflicts that were not analyzed as insurgencies by the RAND team (and others), the results are striking.

The disturbing truth that modern Western COIN theory is built on a handful of books based upon practitioner experiences in

**Figure. Typology of Conflict: The Reality of War**



a handful of 20th-century conflicts is not mitigated by the less famous but broader COIN works. Country studies by lesser known writers are similarly restricted. The core texts cover Vietnam (French Indochina), Algeria, Northern Ireland, the Philippines, and Malaya. The less-well-known writers will go on to discuss Mozambique, Angola, El Salvador, or Afghanistan under the Soviets. Only the most adventurous writers and theorists braved traveling as far as Kashmir or India to look at what could be learned there. Subsequently, the modern study of counterinsurgency and the doctrine it gave birth to are limited to less than two dozen conflicts in a century that witnessed more than 150 wars and lesser conflicts, domestic and interstate (see table 1).

Just as worrying and influential to the formation of a comprehensive modern COIN doctrine is the fact that almost all of the better known examples of counterinsurgency are limited to cases where a colonial or postimperial government was fighting on the territory of its dependent (ex)colonies. In the vast majority of these cases, the insurgent was interested in self-determination or similar politically (as opposed to religiously) motivated goals. Limiting our understanding of insurgency to such historically particular anticolonial and areligious cases seems very hard to justify in today's decidedly postcolonial, post–Cold War era. Most importantly, none of the insurgents discussed within the canon of classic COIN studies was religiously motivated with the aim of initiating a global revolution, as is al Qaeda and its associated movements. As a result, any translation of classic COIN doctrine to the threat posed by a religiously informed and globally ambitious al Qaeda would seem forced, to say the least, and misguided at best. There must be a distinct limit to how useful a doctrine based on what used to be called colonial "policing actions" on the sovereign territory of the counterinsurgent can be to a United States fighting a religiously motivated enemy with global ambitions that outstrip older ideas of nationalism and self-determination.[10]

If we were more scientifically rigorous and broadened the scope of COIN analysis to include other examples of irregular warfare that occurred in the 20th century, our doctrine might be far more relevant. Such a list, if it is to be intellectually sound, must include those instances—internal or international—where unconventional warfare was used by one or both sides, to include civil wars and revolutions. Such a list would include conflicts that classic COIN strategists, both pre- and post-9/11, rarely discuss, such as the Boer War, the Hungarian Revolution of 1956, partisan and resistance efforts in Europe during World War II, and even the Chechen-Russian conflict of the 1990s. Such an expanded pool of case studies would include dozens of conflicts and enrich the field of data that can be examined by the counterinsurgency theoretician, strategist, and practitioner alike.

This expanded set of case studies lends itself to at least a preliminary classification (see table 2). Several of those listed are rarely, if ever, examined as instances of insurgency or counterinsurgency, such as the Hungarian Revolution or French Resistance. Additionally, and most importantly for the current threat environment, several in this newly expanded data set are irregular conflicts wherein actors were substantially informed or influenced by religion as well as politics (for example, the Chechen wars and the Iranian revolution), and which therefore have greater relevance to today's threat environment.

There is no scientific reason why the study of these "nonclassic COIN" conflicts has been all but ignored by those wishing to find doctrinal answers as to how to defeat today's irregular foe. By enlarging the pool of conflicts to be studied, we automatically include cases far closer to the current challenges we face. Not only do we include more cases where the enemy was religiously as well as politically motivated—as are Osama bin Laden and his Salafi allies—we now include examples of conflicts similar to Iraq and Afghanistan insofar as the goal of the counterinsurgent was not a return to the status quo ante, a return to previolence normalcy, but instead a drastic alteration of political, economic, and social structures, the forcible reengineering of a nation.

Given the heterogeneous categories within this new data, it becomes evident that a single unified counterinsurgency doctrine is not possible, that there can be no universal set of best practices evolved over time that can cover such diverse starting points, endstates, and local contexts. After all, how can the same guidelines be used to reestablish order by a strong central government that has been challenged by a minority (such as was the case in Northern Ireland or even Malaya) but also guide the use of force in creating a completely new economic, political, and social system in a country that was formerly controlled by a fundamentalist religious regime (Afghanistan) or a secular dictatorship (Iraq)? To illustrate by comparison, would we ever have insisted on using a doctrine based on lessons learned in mass-maneuver warfare in a conventional campaign in Europe (for example, World War II) for a campaign consisting of unconventional raiding missions in Central Asia (for example, America's support to the anti-Soviet mujahideen in the 1980s)? At the very least, we need to have doctrine in each case bounded by two fundamental variables: the starting point for the intervention and the ultimate (political) goal for the intervention.[11]

When one discusses the former, it is useful to ask whether the initial predeployment situation is one of unrest and low level violence among people tied to us historically, culturally, and linguistically (the colonial scenario), or the use of force in a nation-state that suffered under a dictatorship for decades (Iraq) or that has a failed and corrupt central government of its own (Afghanistan). In the

**Table 1. COIN Data Set of Case Studies**

| |
|---|
| **Most Analyzed:** |
| Malaya |
| Algeria |
| Vietnam |
| The Philippines |
| Burma |
| Nicaragua |
| Northern Ireland |
| **Less Popular:** |
| Angola |
| Afghanistan (Soviet) |
| Greece |
| Mozambique |
| Zimbabwe |
| East Timor |
| Congo |
| Oman |
| El Salvador |
| Colombia |
| China |
| India (Naxalite) |
| Jammu and Kashmir |
| Sri Lanka |
| **TOTAL: 21** |

latter two instances, we need to think about whether our objective is simply the suppression of relatively low levels of violence, or the radical reengineering of the political and economic reality of another country previously unconnected to us directly.

On top of the need to recognize the differences in the strategy that one would adopt based on these underexamined factors, there is also the question of religion. If counterinsurgency is, in the final analysis, about which side has the greatest legitimacy, then we cannot simply measure that legitimacy as a function of political recognition by the majority of the population (representation, as opposed to "democracy"). It should be obvious that if our forces are not only from a different ethnic, linguistic, and cultural group from those communities in which they are operating, but also not of the same faith, then this will drastically affect the legitimacy of our intervention and the chances for success. At the least, it will affect our credibility in the eyes of a different faith community. Put another way, if after World War II, U.S. troops had had to occupy Saudi Arabia or Turkey for a number of decades, would they have used the same rules and doctrines—and been as successful—as they were in their occupation of (West) Germany?[12]

**Table 2. Broadening the Counterinsurgency Data Set**

| | |
|---|---|
| **Colonial Policing Action** | Algeria |
| | Boer War |
| **Domestic Regime Change/Revolution** | Russian Revolution |
| | Cuban Revolution |
| | Hungarian Revolution |
| | Iranian Revolution |
| **Separatist/Self-Determination** | Northern Ireland |
| | Chechnya |
| **International Regime Change** | Afghanistan 1979 |
| | Afghanistan 2001 |
| | Iraq 2003 |
| **Domestic Resistance/Partisan** World War II: | Yugoslavia |
| | Finland |
| | Norway |
| | Estonia |
| | The Ukraine |
| **Internationally Assisted/ Coordinated Resistance** World War II: | France, etc. (Special Operations Executive, Office of Strategic Services) |

## COIN's Proper Place

The observations above on the limitations of today's "best practices" approach to COIN are based upon how little our understanding of this type of conflict is actually a reflection of the realities of unconventional warfare in the 20th century. Classic COIN is simply the current lens we use to try and comprehend an ageless form of conflict that is in fact more prevalent than conventional war.

Within the 464 conflicts recorded on the *Correlates of War* database since 1815, we can identify 385 in which a state was fighting a nonstate actor.[13] Surprisingly, despite the conventional wisdom, in 80 percent of conflicts, the government defeated its irregular foe (victory measured by whether the counterinsurgent government stayed in power and was able to vanquish the threat for at least a decade). Irregular warfare is, therefore, more regular or conventional than our strategic lenses would propose. (If we understand that *regular* is another word for *regulated*, the observation seems almost tautologous, since states monopolize the regulation of war and therefore any conflict involving a nonstate actor will necessarily fall outside of the regulated sphere of war.) If we shift from the more doctrinal and philosophical to the programmatic and historically demonstrable, we find more unsettling evidence.

To begin, if we look at the recorded insurgencies, we find certain conditions for success. Governments that usually win against nonstate opponents are most often those that fight on their own sovereign territory.[14] Contrast this to the challenge that America faces today in Central Asia and the Middle East. Second, winning governments are usually prepared to eventually negotiate with their nonstate enemy.[15]

Additional data show that on average, the successful counterinsurgent will need 12 to 15 years to defeat an insurgency. According to several studies, those insurgencies that defeat governments do so in 5 to 9 years. Therefore, time is an important factor in this type of conflict since the grievances that fuel a threat to the sovereignty of the government will take a long time to ameliorate. It is not, however, simply a question of just throwing resources at the problem. One cannot artificially accelerate the resolution of complicated economic, social, and political problems. We have seen this in Iraq and especially Afghanistan. A functioning state and the provision of fundamental services must be arrived at in an organic fashion that is self-sustaining. Throwing money at a deficit does not engender growth in complex systems bounded by human agency and embedded structure.[16]

Also, the historical data do not support the prevalent winning-hearts-and-minds hypothesis. In a protracted conflict between a state and nonstate actor, making a population "like" the government is much less important than the population believing that there is a sense of order and predictability to their lives—in other words, the perception of what social scientists call a normative system. A successful insurgency provides an alternative normative structure, a predictable "box" of its own within which an ever larger part of the population defines its life. Counterinsurgency is therefore about breaking alternative normative systems (for example, the system of justice provided by the Taliban in increasingly greater areas of Afghanistan).

## Actor-based Approach to War

The depth of the strategic conversation in the United States has bogged down at a superficial level of analysis. We remain at the level of debating COIN versus traditional military capabilities, or COIN versus counterterrorism. We must go deeper, or rather higher. The first step toward this level of richer debate requires recognition of the fact that COIN—as defined in the classic theory of the 1950s—is not the same as "countering insurgency"—the

age-old activity of countering insurrections. The United States must accept that what it has attempted to do in Central Asia and the Middle East is not directly comparable to the experience Western nations gained in postcolonial policy actions of the 20th century. The description of our missions there as COIN, or COIN plus stabilization operations or nation-building, is inadequate. For what we are trying to accomplish is not even an updated COIN 2.0, but in fact nation-formation and the establishment of representative nation-states where before there were none. Subsequently, should the political masters of our military establishment deem it necessary to execute similar missions in the future, we would do well to broaden our scientific catchment of scenarios used to inform our doctrine. This would allow us to move toward a more stochastic approach to 21st-century warfare.

Instead of approaching the threats we face solely on the plane of tactical or operational questions and making the choice of which field manual we should use in theater a primary issue—rather than treating this properly as a doctrinal issue—we should start by establishing the context of conflict. Such a stochastic approach to war today would not posit new qualities of war, or new characteristics of our foe, but ask the simple question: whom are we fighting? Why are they fighting us? For it is highly unlikely that the Taliban fighter whom our Soldiers and Marines face on the ground in Afghanistan or the al Qaeda operative who intends to kill Americans on U.S. soil wakes up and chooses to fight irregular war, or network war, or fourth-generation war. They simply choose war. It is who they are that shapes their approach, not some detached, independent, quality of "modern" war. For although the Great Prussian may have been shaped conceptually by the crucible of state-on-state conventional war, Carl von Clausewitz was so very right when he warned us that we must remember that the nature of war is immutable. Who fights us, why they wish to kill us, and to what end they wish to destroy us will always be different. As the living legend General Carlos Ospina, who more than anyone else was responsible for defeating that very unconventional foe, the Revolutionary Armed Forces of Colombia, stated: "War is war."[17] **JFQ**

## NOTES

[1] See the heated Nagl versus Gentile debate in *Joint Force Quarterly* 58 (3d Quarter, 2010), or the more strident writings of Andrew Bacevich, such as *Washington Rules: America's Path to Permanent War* (New York: Macmillan, 2010). For a workmanlike analysis of why the latest Quadrennial Defense Review represents a weak appreciation of current warfighting needs, see Roy Godson and Richard H. Schultz, "A QDR for All Seasons? The Pentagon Is Not Preparing for the Most Likely Conflicts," *Joint Force Quarterly* 59 (4th Quarter, 2010). See also Sebastian L.v. Gorka, *Al Qaeda and von Clausewitz: Rediscovering the Art of War*, U.S. Joint Special Operations University Symposium: "Countering Global Insurgency," May 5, 2006, available at <www.itdis.org/Portals/11/JSOUStrategy.pdf>.

[2] Two exceptions that prove the rule are, of course, Phil Bobbitt's masterly *The Shield of Achilles* (New York: Anchor, 2003), and numerous works of Martin van Creveld, but especially *The Transformation of War: The Most Radical Reinterpretation of Armed Conflict since Clausewitz* (New York: The Free Press, 1991).

[3] Some label the one side of this debate the "COIN-dinistas." See the swinging observations of Kelley Vlahos such as "One-Sided COIN," *The American Conservative*, August 1, 2009, available at <http://amconmag.com/article/2009/aug/01/00038/>; and *Gian Gentile: Exposing Counterfeit COIN*, Anti-War.com, May 7, 2009, available at <http://original.antiwar.com/vlahos/2009/05/06/gian-gentile-exposing-counterfeit-coin/>; as well as Mehdi Hasan, "Two Sides of the Coin," NewStatesman.com, November 2009, available at <www.newstatesman.com/asia/2009/11/mehdi-hasan-afghanistan-coin-counter>.

[4] John A. Nagl, interview on National Public Radio, "Army Unveils Counter-Insurgency Manual," December 15, 2006, available at <www.npr.org/templates/story/story.php?storyId=6630779>.

[5] See John A. Nagl, *Learning to Eat Soup with a Knife: Counterinsurgency Lessons from Malaya and Vietnam* (Chicago: University of Chicago Press, 2005). Dr. Nagl was heavily involved as part of General David Petraeus's team in the drafting of the new COIN manual.

[6] One of the authors had the pleasure of being informed at a North Atlantic Treaty Organization–funded seminar by a representative of the UK Ministry of Defence that "The British Army doesn't do kinetic operations anymore. It's all about influence now."

[7] See Gentile's remarks at the Atlantic Council conference "NATO Beyond Afghanistan," September 28, 2010, available at <www.acus.org/event/nato-beyond-afghanistan-conference-strategic-implications-nato-isaf-mission>.

[8] David Kilcullen, "Building a 'Ladder of Tribes,'" keynote address, Tribal Engagement Workshop, March 24, 2010.

[9] For a survey of RAND's work and the evolution of the U.S. COIN approach, see Austin Long, *On "Other War": Lessons from Five Decades of RAND Counterinsurgency Research*, available at <www.rand.org/pubs/monographs/2006/RAND_MG482.pdf>. For one of the original works that catalyzed the analytic process in the United States, see David Galula, *Pacification in Algeria*, available at <www.rand.org/pubs/monographs/2006/RAND_MG478-1.pdf>.

[10] For a lengthier discussion of the data set problem and its limiting effect on modern COIN doctrine, see Stephen Sloan and Sebastian L.v. Gorka, "Contextualizing COIN," *Journal of International Security Affairs*, no. 16 (Spring 2009), 41–48, available at <www.ciaonet.org/journals/jisa/v0i16/f_0016438_14210.pdf>.

[11] On the latter point, if some readers hear echoes of Carl von Clausewitz, that is no accident. While it has become passé, if not clichéd, to stress today that a counterinsurgency campaign (run by a democracy) cannot be won by use of force alone, the subtler point is that we must first define the political goal of the COIN campaign. Clausewitz would agree.

[12] While one could here mention the case of post–World War II Japan as an example of the occupier and the population not sharing the same ethnicity, culture, or language, the use and monopoly of atomic weapons by the United States clearly makes that case strategically sui generis.

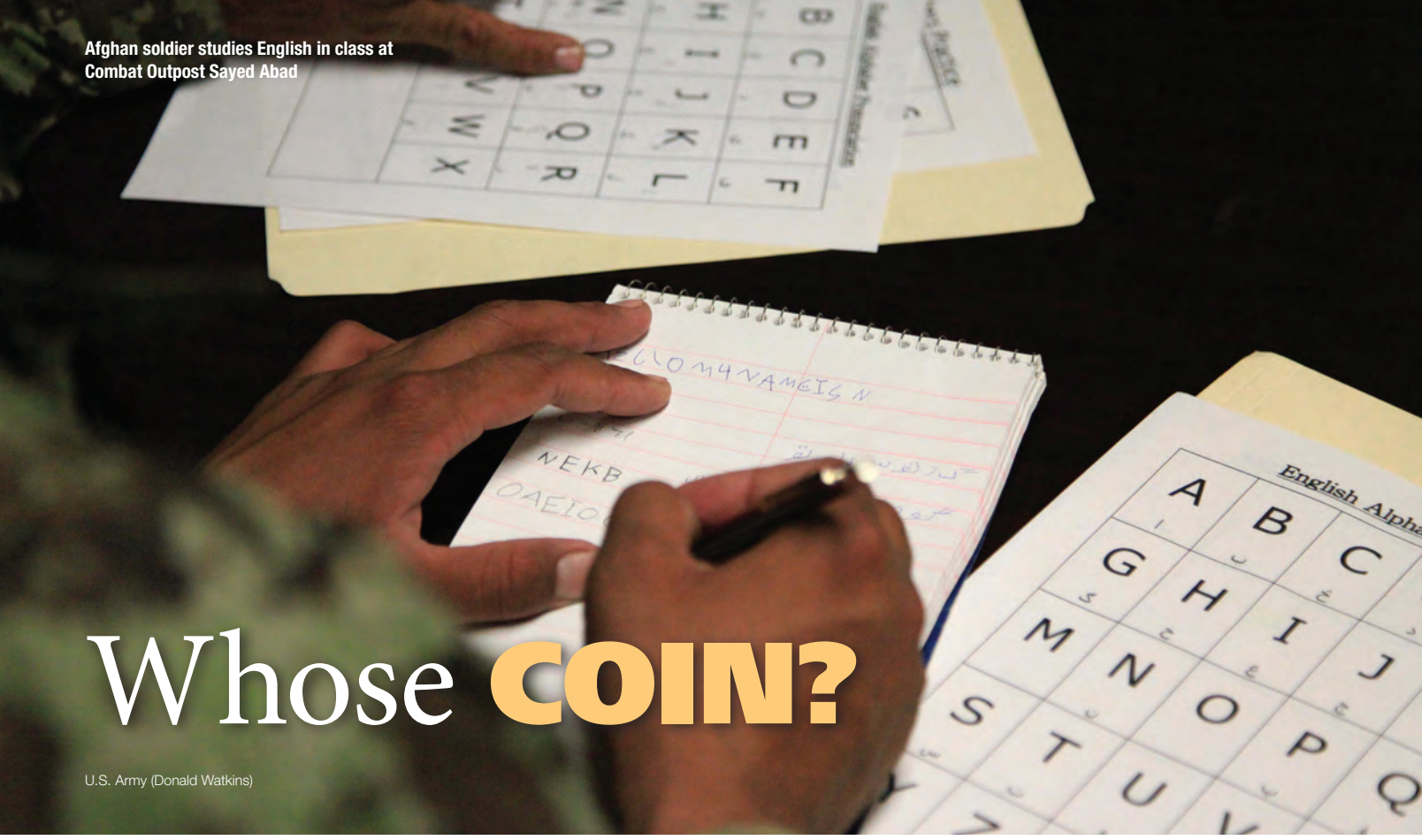
[13] See <www.correlatesofwar.org/>.

[14] Put mathematically, the data show that if the counterinsurgent government is fighting on its own territory and also willing to negotiate, it has an 80 percent chance of success. If neither condition holds, then it is down to 20 percent

[15] With regard to the significance of the primary condition, and in an attempt to grasp the level of the challenge that we face in combat theaters today, think of the analogy of Iraqi police officers suddenly being deployed to New York City to do the job of the New York Police Department. (Or even worse, the Iraqi army being asked to do so—let alone the Afghan National Army.) That is the nature of the current counterinsurgency challenge we face on foreign soil.

[16] We are grateful to Professor Thomas A. Marks, Head of the War and Conflict Studies Department at the College of International Security Affairs at National Defense University, for illuminating this point.

[17] Carlos Ospina Ovalle, "Insights from Colombia's 'Long War': Counterinsurgency Lessons Learned," *Counterterrorism* 12, no. 3 (Fall 2006), 29.




Afghan soldier studies English in class at Combat Outpost Sayed Abad

U.S. Army (Donald Watkins)

# Whose COIN?

*By* **AMITAI ETZIONI**

When American and Iraqi army units were integrated to foster closer cooperation between the groups and to intensify Iraqis' training, a number of challenges arose with regard to the latrines they were to share. The Iraqi soldiers, many of them farm boys, were used to relieving themselves by squatting above holes. When they were made to use Western facilities, they squatted on the toilet seat rims, sometimes making, sometimes missing, their target. They also used their left hands instead of toilet paper and cleaned their hands by wiping them on the walls of the latrines. This situation left the Americans with three options: adapt to the Iraqi way, teach the Iraqis the American way, or let each group follow its own culture and set up separate latrines. The third option was selected.[1]

In trying to build a professional, national Afghan police, the United States posted members of one tribe in the territory of other tribes, on the grounds that the tribe members should give up their local identities and become loyal Afghan cops. As one observer put it, "They might as well paint targets on their foreheads."[2] Indeed, many of the new policemen refused to leave their compounds, and others simply vanished.

In Marjah, U.S. military officials have decided not to eradicate the poppy fields because they provide a major source of income for farmers—much more than they could make from the alternative crops the Americans were fostering. At the same time, the military is concerned that profits from poppy sales are a key funding source for the Taliban. Hence, the U.S. military is engaged in some eradication, some of the time.

These three situations illustrate a critical point that the champions of counterinsurgency (COIN)[3] have not worked out: are they going to accept the local culture and practices and work with and around them—a fixer-upper approach? Seek to change the culture extensively and follow a new construction approach? Or continue to treat this key matter in a confused and conflicted way?

In sorting out this issue, I do not rehash the well-covered debate over whether COIN, understood as a combination of military forces and political reconstruction, is a superior strategy to traditional warfare in which the enemy is defeated and U.S. forces withdraw. Nor will I compare COIN to the course Vice President Joe Biden advocated, which entails withdrawing all U.S. and allied ground troops from Afghanistan and suppressing the remaining terrorists through drone and bombing attacks and some remaining Special Forces—the way the United States currently does in Yemen.

My main argument takes for granted that COIN is called for, but holds that if COIN is to work, *it must be profoundly recast*. The recasting would best occur through three highly interwoven facets: setting much lower, but more realistic, goals for the political element; determining which elements can be introduced into the prevailing culture (rather than building new ones, Western-style) and which—optimally few—elements of the local culture must be rejected; and drawing much more on forces already in place (often local and tribal) rather than forging new, often national, forces. In their recent article on Afghanistan, T.X. Hammes, William McCallister, and John Collins, after demonstrating that the key assumptions that underlie COIN are not supported by evidence, called for a new strategy.[4] This article takes a stab at that mission.

The underlying sociological thesis, based on my 50 years of studying societal change, is that societal engineering is difficult to

**Amitai Etzioni is a University Professor and Professor of International Relations at The George Washington University.**

U.S. Army (David Franklin)

U.S. and Iraqi soldiers conduct first combined patrol in Taji

bring about; that advancing societal changes according to one's design (in contrast to societal changes that occur on their own account) typically requires a much greater commitment of resources over much longer periods of time than is widely assumed and available; and that most such projects are prone to failure.

This thesis gained traction in the 1980s when the neoconservatives pointed out that most of the liberal Great Society programs introduced in the United States in the 1960s failed. The government was unable to eradicate poverty, help minorities to catch up, improve public schools, or stop drug abuse. More generally, the neocons argued that it was wrong to assume that a combination of programs fashioned by civil servants and large amounts of money could solve social problems. Even so, as of 2003, the same neocons maintained—and COIN implies—that what the United States could not do in Los Angeles and Washington, DC, it could do in Helmand, Kandahar, Mosul, and Sadr City.

As a matter of fact, the difficulties in bringing about societal engineering are particularly severe when the change agent is a foreign power with a different culture, thousands of miles away, prone to optimistic, even idealistic, assumptions, and often not inclined to commit large amounts of resources to a given course for long periods of time. In other words, long-distance societal engineering is even more failure-prone than domestic societal engineering. An extensive 2006 report on the scores of billions of dollars that the World Bank invested since the mid-1990s in economic development shows that the "achievement of sustained increases in per capita income, essential for poverty reduction, continues to elude a considerable number of countries." Out of 25 aid-recipient countries covered by the report, more than half (14) had the same or declining rates of per capita income from the mid-1990s to the early 2000s. And the nations that thrived were not necessarily those that received much aid. Indeed, while the nations that received very little aid grew very fast (especially China, Singapore, South Korea, and Taiwan), the nations that received most of the aid (especially ones in Africa) developed least.

Many nations found foreign aid a "poisoned gift" because it promoted dependency on foreigners, undermined indigenous endeavors, and disproportionately benefited those skilled at proposal writing and courting foundations and foreign aid representatives, rather than local entrepreneurs and businessmen. Steve Knack of the World Bank showed that "huge aid revenues may even spur further bureaucratization and worsen corruption." Others found that mismanagement, sheer incompetence, and weak governments undermined many attempts at development (which is another term for *societal engineering*). All this is relevant to COIN, because it contains many of the elements of foreign aid and thus faces many of the same challenges.

All this is not to suggest that when one has an urge to engage in societal engineering, one should lie down until the urge goes away. It suggests that COIN is much more likely to succeed when it greatly limits the extent to which one seeks to change the society at issue, accepts large elements of the culture as it is, and draws as much as possible on native forces rather than vainly seeking to forge new ones. Less is more.

An obvious example is the now widely agreed upon observation that the United States would have been much better off in Iraq if it had left the Ba'ath army and civil servants in place. At the same time, this does not mean that the change agent cannot introduce some, albeit limited and carefully selected, modifications. For instance, the highest ranks (especially the political leaders) of the Ba'ath party could have been dismissed.

## The Scope Issue

COIN calls for an encompassing do-over of the societies at issue. Wendy Brown writes that:

*If the manual* [Field Manual 3–24, *Counterinsurgency*] *can be reduced to a single didactic point, it is that successful war against insurgents involves erudite and careful mobilization of every element of the society in which they are waged. These wars are won through a new and total kind of governance, one that emanates from the military but reaches to security and stability for civilian life, formal and informal economics, structures of authority, patron-client relationships, political participation, culture, law, identity, social structure, material needs, ethnic and linguistic subdivisions, and more.*[5]

Stathis Kalyvas put it as follows: "In short, this is a strategy of competitive state building combining targeted, selective violence and population control, on the one hand, with the dissemination of a credible mass ideology, the creation of modern state structures, the imposition of the rule of law, and the spurring of economic development."[6] General Stanley McChrystal's definition was more limited, but he still held that the United States must "promote good local governance, root out corruption, reform the justice sector, pursue narcotics traffickers, [and] increase reconstruction activities."[7]

It is often argued that the United States had no plan for postwar Iraq. In fact, prior to the 2003 invasion, the Department of State had prepared a massive 13-volume study known as *The Future of Iraq Project*.[8] The study provided plans for reconstruc-

tion projects for myriad institutions and sectors—water, agriculture and environment, public health and humanitarian needs, defense policy, economy and infrastructure, education, justice, democratic principles and procedures, local government, civil society capacity-building, free media, and oil and energy, among many others.

As a result of such a wide-ranging, scattershot approach, scores of projects were started, but few have been completed. Indeed, many were abandoned because there were not enough funds to complete them. The woes of development in Afghanistan have been so often told that they hardly need repeating. John Nagl captures the point exceedingly well in a book whose title says it all: it is akin to "learning to eat soup with a knife"—one might add, while fighting a war.

## Less Is More

All the preceding observations do not suggest that COIN cannot succeed in the kind of countries in which it is now applied, but rather that it must be greatly scaled back. Its commanders and societal engineers would be well served by daily recitation of the prayer familiar to recovering addicts: "God grant us the serenity to accept the things we cannot change, courage to change the things we can, and wisdom to know the difference."

I asked one of the highest ranking U.S. commanders in the Middle East what our sociological goal was in Afghanistan.[9] What was the nonmilitary "build" element of COIN trying to accomplish—to turn Afghanistan into a society like, for instance, Jamaica, Nigeria, or India—or Chicago, circa 1900? He responded, "We will turn them into Switzerland in 2 years."[10] Secretary of Defense Robert Gates stated that the United States is not trying to turn Afghanistan into a 21st-century society.[11]

These short quotations highlight the analytical and political difficulties in setting a realistic goal. Thus, if the general and Secretary Gates had stated that the United States would be quite content to turn Afghanistan into, say, an Egypt (or any comparable regime), they would invite voluminous criticisms from human rights advocates, champions of democracies, Afghan elites, and many in the Third World. At the same time, without setting a much more scaled-back and realistic goal than, in effect, a do-over of the social, economic, cultural, and political foundations of the society, one invites failure by setting goals that cannot be reached and by raising expectations that are bound to be disappointed, especially among the local people whose hearts and minds COIN is seeking to win.

Arguably the best way to proceed is to set what might be called "basic" goals, while leaving the door open to going beyond them once they are achieved. The goal is best set on a level that can be achieved in a reasonable amount of time (measured in years and not decades) and with the resources available—in plain English. Because this approach also calls for building largely on what is in place, the specific goals would differ from one COINed country to another, depending on its assets and foundations.

## A Question of Culture

On one hand, even a buck private knows that we ought to respect the local culture. On the other, much of the societal engineering the United States is involved in assumes that certain things can be changed—and in relatively short order. Take the way women are treated in Afghanistan. Our tendency is to promote equality for women. Thus, the United States pressured the Afghans to require that at least 25 percent of the seats in the Afghan parliament be set aside for women (a requirement it neither adheres to nor is the U.S. meeting in its own legislative bodies, from Congress to state assemblies). And American representatives proudly state that the United States built schools that accommodate more than 2 million girls in Afghanistan. However, such developments alienate significant segments of the population in many parts of that country, as well as in southern Iraq, critical parts of Pakistan, and most of Yemen, among others.

I am in favor of urging Afghan society to respect the rights of women and all others. But it does not necessarily follow that changing centuries-old sociological traditions, habits, and institutions—many rooted in the religious beliefs large segments of the population profoundly hold—can be part of these first-round, basic efforts.

Truth be told, it is difficult even to openly discuss the question: Which of its rights should the United States insist the locals respect, and which ought the United States let the local population fight for and gain on its own—or adapt to its own culture? Take the separation of state and religion, which U.S. representatives seek to promote in Muslim nations. One should recall that this precept is largely a French and American idea most other democracies, let alone the rest of the world, do not abide by. The United States would do well not to engage this issue, which happens to be especially important to the Taliban, whose number-one condition for peace is the introduction of sharia as the basis of law. One may argue that Muslim religious traditions and laws, like all others, are subject to both stricter and more permissive interpretations, and that the United States and its allies should hold out for some of the more moderate interpretations. As I see it,


ISAF (Joseph Swafford)

**At International AgFair in Kabul, representatives provide information on agriculture in Afghanistan, one of Central Asia's fastest growing markets**

one should leave it to the local population to decide which interpretation it is willing to live by, which, by the way, changes over time (as we see in Iran), rather than employ foreign troops to ensure that one version of a religion rather than another will prevail.

On the other hand, there are some human rights abuses so egregious that the United States should not tolerate their violation. An outstanding example is the practice of pedophilia, in which rich and powerful Afghans continue to engage.[12] Torture might well be another example. Indeed, several major religions draw such a line. Thus, Catholics differentiate between mortal and venial sins, and Jews have a list of 613 dos and don'ts, but only view 3 as cardinal rules for which one should die rather than transgress.

The strong inclination to Westernize or Americanize the local society and especially its security forces extends way beyond the promotion of rights. There are numerous reasons the training of the police in Afghanistan is such a prolonged, costly, and abysmal failure, and that the army, while doing much better, has such a long way to go. These include an insufficient number of trainers, lack of coordination among the various nations and agencies that are involved, and threats by the Taliban. One should not, though, overlook that another key retardant to creating a viable Afghan police and army is that the United States and its allies are seeking to Westernize them, rather than trying to piggyback some limited additions and improvements onto their way of conduct and fighting. Here is the way one reporter illustrates the point at issue:

*Their American trainers spoke of "upper body strength deficiency" and prescribed push-ups because their trainees buckle under the backpacks filled with 50 pounds of equipment and ammo they are expected to carry. All this material must seem absurd to men whose fathers and brothers, wearing only the old cotton shirts and baggy pants of everyday life and carrying battered Russian Kalashnikov rifles, defeated the Red Army two decades ago. American trainers marvel that, freed from heavy equipment and uniforms, Afghan soldiers can run through the mountains all day—as the Taliban guerrillas in fact do with great effect—but the U.S. military is determined to train them for another style of war.*[13]

Moreover, the recruits are coming from the poorer layers of a poor society. Many are short (5½ feet tall or under) and slightly built. There are not enough push-ups in the world to make them into American hulks.

Another example concerns the weapons themselves. The United States is introducing the M–16 rifle as a replacement for the venerable Kalashnikov. However, even U.S. trainers admit that in Afghanistan, the Kalashnikov is the superior weapon. Light and accurate, it requires no cleaning even in the dust of the high desert, and every man and boy already knows it well. The strange and sensitive M–16, on the other hand, may be more accurate at slightly greater distances, but only if a soldier can keep it clean, while managing to adjust and readjust its notoriously sensitive sights.[14]

I leave it for another day to ask what the proper balance for COIN is between conventional and irregular forces (or Special Forces), an issue of special interest to me as I fought in both capacities. I should, though, note in passing that to the extent that U.S. training takes irregular fighters and turns them into regular ones, this may not be the best way to counter an irregular force, which the insurgents invariably are.

The more COIN uses the local culture, habits, and instruments as the stock to which it grafts any necessary changes, the more successful it will be.

## Legitimacy and Politics

One of the key elements of COIN, arguably the most important nonmilitary one, is political development. In numerous discussions of this strategy, much weight is accorded to ensure that the government is legitimate and effective. This is correctly deemed necessary, as COIN requires that one win the hearts and minds of the population in order to get it to shift its allegiances from the insurgents to U.S. troops and/or the local partner. Also, politics are sought to absorb conflicts among various forces in society and allow the working out of differences in a peaceful manner, avoiding civil war or the kind of anarchy that favors the insurgency. In addition, it is considered essential to greatly reduce corruption and develop an effective civil service that serves the people rather than enriching the elites.

All this may be true, but the way the United States often proceeds points one more time to the need to recast COIN to both greatly scale back its scope and build on the culture in place. The United States tends to assume that a government gains legitimacy in one way: the democratic way—*our way.* Hence, the United States expends much effort in introducing new politics based on fair and open elections and elected bodies of representatives, and those who have a high level of integrity. And the United States exhibits an almost instinctive rejection of all other sources of legitimacy and forms of politicking. As a result, U.S. efforts face severe setbacks when it turns out that the elections are fraudulent and the political and civil servants are corrupt to the core.

The *Washington Post* examined the forms people fill out when they carry cash out of Afghanistan. There are no limits, but one has to declare. It turns out that the amount carried out on flights to Dubai alone (which does not include the amount carried by those who use the VIP section of the Kabul airport, who are almost never asked to fulfill this requirement) totaled $180 million over a 2-month period. Assuming that rate held constant for an entire year, the total amount would exceed Afghanistan's total annual domestic revenue.[15] Afghanistan is the world's second-most corrupt nation of 180 countries, as surveyed in 2009 by Transparency International.

There are, however, other ways in which legitimacy can be attained. And most people have distinct institutions and ways of selecting leaders and resolving conflicts: tribal councils, for instance, or community elders. Religious authorities also serve to guide, influence policies, and resolve differences. Moreover, many people often rely on what might be called "natural" leaders —those who rose to power due to their charisma, leadership they exhibited during wars, lineage (they come from what are considered "important" families), or religious status, but who were not elected in the Western way.

COIN would benefit if the United States worked with the institutions and leaders already in place. Thus, when Prime Minister Hamid Karzai assembled some 1,500 traditional leaders in May 2010 in a "Peace Jirga," seeking to reaffirm his legitimacy (and gain a mandate for negotiation with some elements of the Taliban),[16] the initial U.S. reaction was rather negative. However, such a jirga plays an important role in the politics of nations such as Afghanistan, although they are not based on elected representatives and *Robert's Rules of Order.*

To illustrate the role of natural leaders, it might serve to consider the case of Matiullah

Khan, a fairly typical account. In southern Afghanistan's Oruzgan Province, the private security company he leads has supplanted many of the weak Afghan government's functions. Matiullah's army is the primary provider of security in the region; U.S. and North Atlantic Treaty Organization forces pay Matiullah millions of dollars each month to secure roads for convoys. His militia also fights insurgents alongside U.S. Special Forces and gathers intelligence. Forces in the region view Matiullah and other warlords as lesser evils, people who can help establish security in areas where the government is not stable enough.

Like many leaders of private militias that have emerged over the past few years, Matiullah provides the province with more than just stability. He appoints public employees, endows scholarships, donates money for mosques, and holds weekly meetings with tribal leaders. It is estimated that he employs 15,000 people in the province.

Nowhere is the ambitious new building approach more visible—and more damaging—than in the U.S. support of a strong central national government, both in Iraq and in Afghanistan. In Afghanistan, the U.S.-backed government in Kabul appoints mayors and governors of provinces and districts, rather than holding elections for these posts. The approach is particularly odd coming from the United States—a nation that thrives on federalism—especially in states where there are strong local alliances based on ethnic and confessional groups, such as the Shia, Sunni, and Kurds in Iraq and the Pashtun, Tajiks, Uzbeks, and Hazaras in Afghanistan, and weak national loyalties. Moreover, it ignores the fact that the so-called tribal leaders command sizable armies and had formed an alliance (the Northern Alliance), which won the war against the Taliban in the first place. In large parts of northern Iraq, the United States and its allies had almost no casualties and few Iraqis were killed. This was due to the fact that the Kurds' own sizable army, the 200,000-member Peshmerga,[17] kept peace, law, and order. Attempts to truly integrate it into a national army failed, although nominally one can argue that it was deputized.

And Shia units, to the extent that they were let be, did rather well in controlling their turf, although, in several cases, Shia units clashed with each other. In Iraq, it was sheikhs who played the major role in the Sunni Awakening movement (and not the Sunnis' elected representatives in Baghdad), and they were the leaders that U.S. commanders turned to in the Anbar region (which includes Fallujah). These sheikhs were the leaders who decided to cooperate with the United States in taking on al Qaeda in Iraq, routing them from the region.

Instead, the United States sought to build professional national armies in which people dropped their group identities to represent their nation. Indeed, the United States initially sought to place Sunni units in Shia areas and vice versa in order to stress that they were serving their country and not their group. In Afghanistan, non-Pashtun police trainees of Hazara, Tajik, Uzbek, or other ethnic backgrounds were dispatched to maintain order in Pashtun territory.[18]

Clare Lockhart, an expert on Afghanistan, put it well when she testified before the Senate Foreign Relations Committee that what was needed is a "'light touch' form of governance . . . where formal structures . . . can 'mesh' with local and traditional networks and social organizations. . . . Networks of traditional birth attendants, *hawala* dealers, traders, *ulema*, and teachers can all be mobilized or partnered with for different tasks."[19] In a 2008 survey, the Asia Foundation found that local representative bodies (both traditional ones such as the shura and jirga and newer ones such as the Community Development Councils and Provincial Councils) enjoy the support of about two-thirds of the population. In addition, almost 70 percent stated that religious leaders should be involved in local government decisionmaking.

*the United States must also overcome its reluctance to work with religious leaders—but only those who reject violence*

When one raises these questions with commanders in the field, they respond that they deal with unelected local leaders and councils every day of the week. This is true. Indeed, since the middle of 2010—finally—attempts intensified to co-opt, win over, pay off, or otherwise work with local natural leaders. However, these efforts have run into intense opposition by the Karzai government, which sees such steps as undermining its authority and weakening its hold on power. Given that the United States continues to work with that central government as its main partner, local collaborations take at least one step backward for every two forward.

The tension between the strategic efforts that focus on the national versus the local level has been well captured by Stephen Biddle:

*These problems have led to some significant divergences between actual U.S. strategy in Iraq and the approach embodied in the manual. In particular, the rapid growth of local negotiated cease-fires between American commanders and Iraqi insurgent factions in the field has increasingly posed an alternative to reform of the Iraqi national government in Baghdad as a means to stabilizing the country.*[20]

Aside from negotiating with local political and militant leaders, the United States must also overcome its reluctance to work with religious leaders and instead embrace and even favor them—but only those who reject violence. This short aside is crucial. Rather than treating all those who are strongly devout, often called "fundamentalists," as adversaries, one must draw a line between those who reject violence (whether or not they also embrace the values of a liberal democracy) and those who legitimate violence.[21] Among Muslims, there are those (in fact, the majority) who characterize jihad as a journey of self-improvement and those who view it as a war to kill all the infidels.

A prime example is Grand Ayatollah Sayyid Ali al-Husayni al-Sistani, the most revered Shia cleric in Iraq. He is highly influential among the largest Iraqi confessional group (some 60 percent of Iraqis are Shia) and a strong advocate of nonviolence. Initially, the United States sought to marginalize him. The reasons are telling: He is not elected by voters and thus does not fit the democratic model. However, if one accepts the basic tenet that one must start from where people are, not from where we believe they ought to be, one cannot ignore that many of the most influential people in the countries in which terrorists thrive are religious authorities.

## Effective, Noncorrupt Government?

President Barack Obama was reported to have flown to Kabul at the end of March 2010 to convince the Karzai government

to pay more attention to "battling corruption." The same demand has been repeated in numerous countries by scores of advisors from the United States, allies, and the World Bank, among others. Many anticorruption drives have been initiated, and practically all have failed, often resulting in the jailing of those who led the drive. One ought to remember that corruption was rampant in our parts until quite late in the economic and educational development of the United States (and the United Kingdom), not to mention in southern European countries, where it is still endemic, as well as in Russia, India, China, and most other nations.

When one raises this point, a common response is that "all" we need to do is reduce corruption from high, debilitating levels, to a low, tolerable level, which might even be functional, as it allows a greasing of the wheels of highly bureaucratic countries. A "fee" of 10 percent or so is said to be acceptable, while corruption higher than 20 percent is truly damaging. This cocktail party sociology, like many other factoids, sounds quite plausible but is not based on robust evidence. Nor is there a reliable way to bring corruption down in a country in which it is endemic and "too" high.

What can be done? We should leave the local people to work out what they will tolerate and what they will balk at. *Local* is the key word: Think of "The Godfather," Tammany Hall, or the aldermen in Chicago. Local leaders tend to take care of their cadres, supporters, and cronies, but also their "base" community. They have a sense of affinity and loyalty to their people and find that sharing the bounty (for example, jobs) allows them to stay in power. In contrast, civil servants, who are appointed by the national government and draw their power from the center, are often much more exploitative because they have neither local ties nor commitments and do not expect to stay in place for long periods of time. Hence, keeping corruption within limits itself suggests that working with the local population, leaders, and institutions is much more realistic than seeking to build professional national civil services. True, there are exceptions to this rule: a particularly abusive warlord or a local regime that is corrupt well beyond the "norm" is best removed. Here too, however, helping the locals rather than making such calls from long distance is likely to be more effective.

This is not exactly the way attempts to curb corruption—considered essential for building an effective and legitimate government, a key COIN element—developed in 2010. At first the United States pressured the Karzai government to curb corruption. When two Afghan anti-corruption task forces closed in on major sources of corruption at the highest level, President Karzai fired the two main public officials who led the anti-corruption drive. The United States then initiated an American-based drive, which so distressed Karzai that he imposed restrictions on the roles "foreign" organizations could play in anti-corruption investigations. Hence the United States declared that it would cease to deal with high-level corruption and instead focus on the local level, because this is allegedly what concerns the people most. According to one American official, "Predatory corruption at local levels by local officials is the most important factor in turning people from supporting the Afghan government to opposing it."[22] Actually, for reasons already indicated, the opposite seems to be the case.

I leave it for another day to ask what can be done about corruption that is generated by foreign contractors, corporations, and individuals that try to make their way in this country. However, there is no denying, given the huge sums involved, that while Western nations call for curbing corruption, they also contribute to it and do rather little to curb this imported corruption. Maybe the best place to start reforming Afghanistan is closer to home.

In the longer run, more encompassing reforms may be introduced, and the national government may grow in scope and powers. However, these developments are best led by the locals and at a pace they dictate.

There is an inherent contradiction at the core of COIN. On the one hand, its main goal is to build a legitimate and effective native government so the United States can disengage and leave behind a stable and reliable partner. On the other hand, Field Manual 3–24 states that "COIN requires Soldiers and Marines to be ready both to fight and to build."[23] Of course, the two can be reconciled—but only as long as the Soldiers and Marines seek to turn over their duties as soon as possible to the locals and realize that the more they follow local norms and institutions rather than try to redo them, the sooner COIN will be advanced. Another tension exists between those who hold that COIN should be carried out by the military and those who think it ought to be carried out by U.S. civilians. The State Department has long argued that its personnel are better suited for the "build" part of COIN than the military, although it has had a hard time finding enough staffers who are willing or can be motivated to serve in that capacity. The facts point in the same direction as the previous observation. If the military has a trained incapacity to build because its core training and recruitment criteria are based on the ability to fight, and American (and allied) civilians are not available, there is still more reason to draw on locals as much as possible, even if they follow their own norms on most issues.

### Mission Creep

From the outset, COIN is a complicated vessel that must be carefully guided through challenging terrain. It is often burdened by adding missions to its core task to end the insurgency and leave behind a legitimate and effective government. Some of these missions may be fully justified; however, those who pile them on should realize that they further burden COIN, and that it might be overloaded to a breaking point. They had best restrain their ambition as much as possible, which is the subtext of this whole article.

One example will have to stand in for the many that could be provided. One of the major difficulties the United States faces in Afghanistan is that the Pashtun—the largest ethnic group in the country—feel left out (the way the Sunnis did in Iraq, only the Sunnis are the smallest among the three major groups in Iraq). The Pashtun are the primary source of supporters and recruits for the Afghan Taliban. The Pashtun also have close ties with the Pakistan Directorate for Inter-Services Intelligence (ISI). Thus, it would make sense for the United States to work harder with the ISI to encourage the Pashtun to cease their role as the mainstay of the insurgency. However, the United States decided that Afghanistan must remain largely neutral ground between India and Pakistan because India is opposed to a major Pakistani influence over Afghanistan, and the United States is courting India as a countervailing power or balancer to China. Thus, COIN is hindered by a mission creep that includes complicated and arguably dubious regional and even global geopolitical considerations.

One is reminded of the ways Americans tend to build numerous items, from biomedical identification cards to fighter airplanes. We tend to add ever more specifications in order to enable the instrument du jour to

carry out more missions, better. The result is typically an instrument that is costly, slow to complete, and prone to breakdowns. All this is true, only many times more so, when we are seeking to build nations in much less developed countries. Using local materials and restoring, rather than building de novo, are much more likely to succeed.

The problem is not that nationbuilding snuck in the back door after it was recognized as futile under many conditions. Initially, President Obama limited the goals in Afghanistan to eradicating al Qaeda. However, in the months that followed, the argument that this goal requires "building" won the day, which is a code word for nationbuilding. The problem is that the United States is engaged in the wrong kind of nationbuilding. It relies on a top-down approach rather than one that moves from the peripheries toward the center. This is a Western design, one that is much too ambitious and idealistic for the circumstances. **JFQ**

## NOTES

[1] Mike Drummond, "At U.S. Base, Iraqis Must Use Separate Latrine," McClatchy-Tribune News Service, August 3, 2007.

[2] Ann Jones, "Meet the Afghan Army," *The Nation*, October 5, 2009, available at <www.thenation.com/article/meet-afghan-army>.

[3] I assume that the reader is familiar with the basic concept and history of counterinsurgency. Those less initiated may wish to consult Bureau of Political-Military Affairs, *U.S. Government Counterinsurgency Guide* (Washington, DC: Department of State, 2009); U.S. Army Field Manual 3–24/Marine Corps Warfighting Publication 3–33.5, *Counterinsurgency* (Washington, DC: Headquarters Department of the Army/Headquarters Department of the Navy, 2006); John A. Nagl, *Learning to Eat Soup with a Knife* (Chicago: University of Chicago Press, 2002); and David Galula, *Counterinsurgency Warfare: Theory and Practice* (New York: Praeger, 1964).

[4] T.X. Hammes, William S. McCallister, and John M. Collins, "Afghanistan: Connecting Assumptions and Strategy," U.S. Naval Institute *Proceedings* 135, no. 11 (November 2009).

[5] FM 3–24, 81–99; Wendy Brown, "Review Symposium: The New U.S. Army/Marine Corps Counterinsurgency Field Manual as Political Science and Political Praxis," *Perspectives on Politics* 6, no. 2 (June 2008), 354–355.

[6] Stathis Kalyvas, "Review Symposium: The New U.S. Army/Marine Corps Counterinsurgency Field Manual as Political Science and Political Praxis," *Perspectives on Politics* 6, no. 2 (June 2008), 351.

[7] Rajiv Chandrasekaran and Karen DeYoung, "Changes in Afghanistan, Washington May Require Shift in U.S. War Strategy," *The Washington Post*, September 21, 2009.

[8] "New State Department Release on the 'Future of Iraq' Project," *The National Security Archive*, September 1, 2006, available at <www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB198/index.htm>.

[9] Personal conversation between author and U.S. commander.

[10] Ibid.

[11] "Media Roundtable with Secretary of Defense Robert Gates from London, United Kingdom," June 10, 2010, available at <www.defense.gov/transcripts/transcript.aspx?transcriptid=4639>.

[12] Joel Brinkley, "Afghanistan's Dirty Little Secret," *San Francisco Chronicle*, August 29, 2010.

[13] Ann Jones, "Meet the Afghan Army: Is It a Figment of Washington's Imagination?" *The Huffington Post*, September 20, 2009, available at <www.huffingtonpost.com/ann-jones/meet-the-afghan-army-is-i_b_292864.html>.

[14] C.J. Chivers, "How Reliable Is the M–16 Rifle?" *The New York Times* blog, no. 2, 2009, available at <http://atwar.blogs.nytimes.com/2009/11/02/how-reliable-is-the-m-16-rifle/>.

[15] Andrew Higgins, "Officials Puzzle over Millions of Dollars Leaving Afghanistan by Plane for Dubai," *The Washington Post*, February 25, 2010.

[16] Alissa J. Rubin and Rod Nordland, "Taliban Attacks Shake Afghan Peace Gathering," *The New York Times*, June 2, 2010.

[17] "Iraqi Security Forces Order of Battle 2010," *Defense Industry Daily*, March 3, 2010, available at <www.defenseindustrydaily.com/Iraqi-Security-Forces-Order-of-Battle-2010-0203-06217/>.

[18] Jones.

[19] Clare Lockhart, "Prepared Testimony: Senate Committee on Foreign Relations," September 17, 2009, available at <http://foreign.senate.gov/imo/media/doc/LockhartTestimony090917a1.pdf>.

[20] Stephen Biddle, "Review Symposium: The New U.S. Army/Marine Corps Counterinsurgency Field Manual as Political Science and Political Praxis," *Perspectives on Politics* 6, no. 2 (June 2008), 349.

[21] For extensive discussion of this point, see Amitai Etzioni, "The Global Importance of Illiberal Moderates," *Cambridge Review of International Affairs* 19, no. 3 (September 2006).

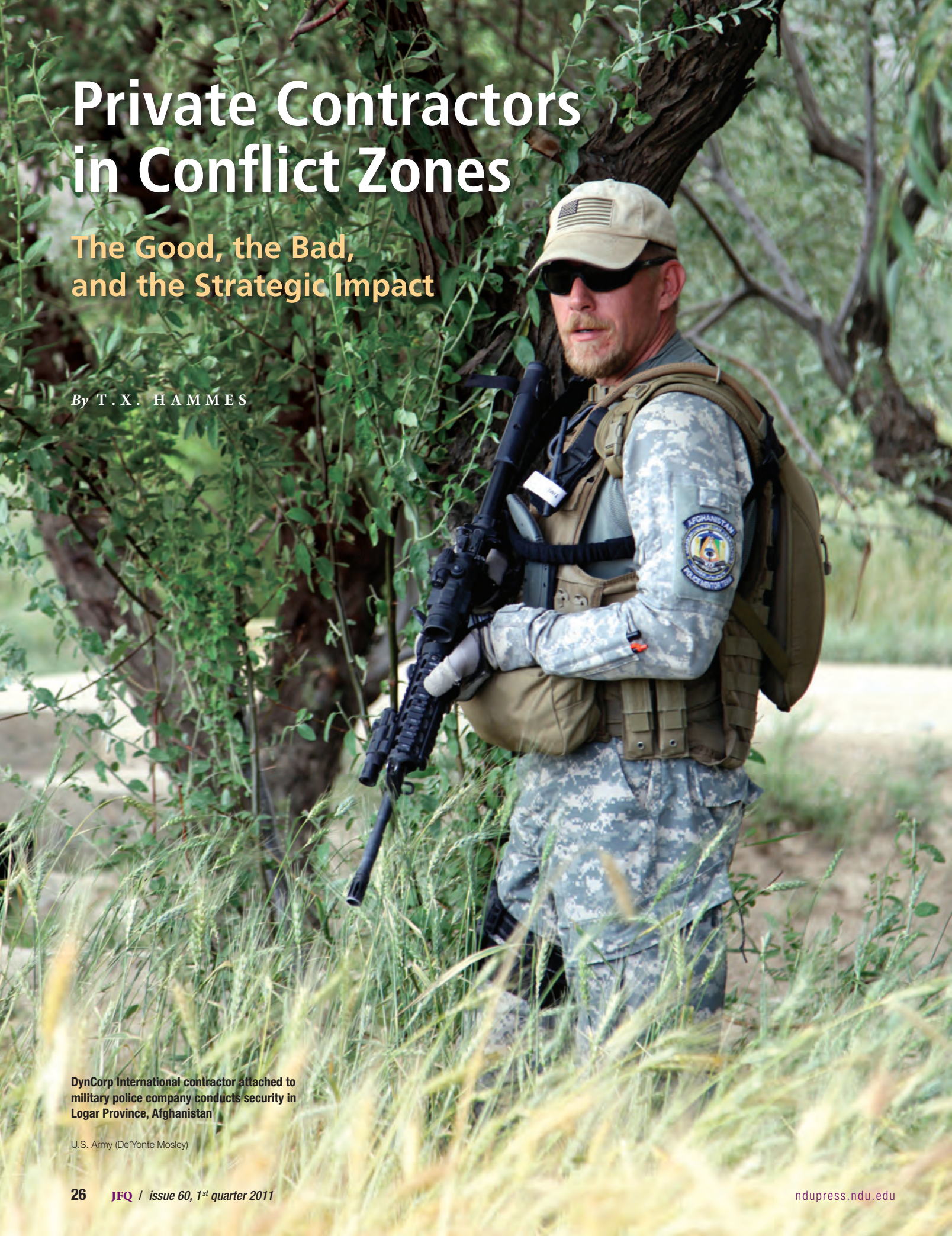
[22] Adam Entous, Julian E. Barnes, and Siobhan Gorman, "U.S. Shifts Afghan Grant Plan," *The Wall Street Journal*, September 20, 2010.

[23] FM 3–24, 34.

# Private Contractors in Conflict Zones

## The Good, the Bad, and the Strategic Impact

*By* T. X. HAMMES



DynCorp International contractor attached to military police company conducts security in Logar Province, Afghanistan

U.S. Army (De'Yonte Mosley)

In Iraq and Afghanistan, the use of contractors reached a level unprecedented in U.S. military operations. As of March 31, 2010, the United States deployed 175,000 troops and 207,000 contractors in the war zones. Contractors represented 50 percent of the Department of Defense (DOD) workforce in Iraq and 59 percent in Afghanistan.[1] These numbers include both armed and unarmed contractors. Thus, for the purposes of this article, the term *contractor* includes both armed and unarmed personnel unless otherwise specified. The presence of contractors on the battlefield is obviously not a new phenomenon but has dramatically increased from the ratio of 1 contractor to 55 military personnel in Vietnam to 1:1 in Iraq[2] and 1:43.1 in Afghanistan.[3]

This increase is the logical outcome of a series of decisions going back decades. Force structure reductions ranging from the post-Vietnam decisions that moved most Army logistics support elements to the Army Reserve and Guard[4] to the post–Cold War reduction that cut the Army from 18 to 10 divisions with corresponding cuts in support forces greatly reduced the Services' ability to support long-term operations. Next, a series of decisions in the 1990s led to the employment of contractors in the Balkans for tasks from traditional camp-building to the new concept of "force development" that saw MPRI training the Croatian army. Finally, the decision to invade Iraq with minimum forces left the United States with too few troops in-theater to deal with the disorder that resulted from the removal of Saddam. Thus, it is understandable that the immediate, unanticipated need for large numbers of logistics and security personnel, the shortage of such troops on Active duty, and the precedent for using contractors in the Balkans caused the Pentagon to turn to contractors to fill the immediate operational needs. However, the subsequent failure to conduct a careful analysis of the wisdom of using contractors is less understandable. The executive branch has conducted numerous investigations into fraud, waste, and corruption in the contracting process. Congress has held hearings and established the Commission on Wartime Contracting in Iraq and Afghanistan. Yet the U.S. Government has not systematically explored the essential question: Does using contractors in a conflict zone make *strategic* sense?

This article explores that question. It examines the good, the bad, and the strategic impact of using contractors in conflict zones. It concludes with policy recommendations for the future employment of contractors and outlines additional actions needed to understand and cope with the rapidly expanding use of armed contractors worldwide.

*does using contractors in a conflict zone make strategic sense?*

## The Good

Contractors provide a number of advantages over military personnel or civil servants—speed of deployment, continuity, reduction of troop requirements, reduction of military casualties, economic inputs to local economies, and, in some cases, executing tasks the military and civilian workforce simply cannot. This section examines each of these advantages in turn.

Speed of deployment—the ability to quickly mobilize and deploy large numbers of personnel—is particularly important when a plan fails to anticipate problems. Since the Pentagon had not planned to keep large numbers of troops in Afghanistan or Iraq for any period of time, it had not planned for the required logistics support. The Pentagon also failed to anticipate the requirement for large numbers of security personnel to protect all U.S. activities (including political and reconstruction activities) once the Afghan and Iraqi governments were toppled.

By tapping into databases, running job fairs in the United States, and contracting for labor from Third World companies, contractors were able to quickly recruit, process, and ship personnel to run base camps, drive trucks, and perform the hundreds of housekeeping chores required to maintain both combat forces and civil administrators spread across Iraq and Afghanistan. More challenging was finding qualified personnel to provide security for the rapidly growing U.S. presence in both nations. Private companies managed to find people, hire them, and move them into country—all without the political problems inherent in mobilizing additional U.S. military forces to execute the same tasks. The combination of speed and a low political profile made contractors an attractive choice to provide the resources for which the administration had failed to plan. In addition, the use of contractors aligned with previous decisions and the administration's faith in the efficiency and effectiveness of private business compared to governmental organization. Both inside and outside Iraq and Afghanistan, contractors replaced tens of thousands of soldiers normally required to move, stage, marshal, and transport personnel and supplies into conflict zones.[5]

Continuity is a second major advantage of contractors. While the U.S. military has a policy that ensures the vast majority of personnel rotate every 6 to 12 months, contractors are often willing to stay for longer periods. For key billets, companies can offer significant bonuses to personnel who stay. The companies know that they will reap commensurate savings due to the personnel continuity, and employees see an opportunity for significantly increased pay. Sometimes, moreover, longevity leads to a greater understanding of the situation. This can lead to more effective decisionmaking to include an understanding of the political impact of the contractor's decisions.

The most highly prized attribute of private contractors is that they reduce troop requirements by replacing military personnel. This reduces the military and political resources that must be dedicated to the war. At the height of the surge in April 2008, the Department of Defense (DOD) stated it had 163,900 contractors supporting 160,000 troops in Iraq.[6] Without the presence of contractors, the United States would have had to provide literally twice as many troops. The U.S. Armed Forces struggled to maintain 160,000 troops in Iraq; it is doubtful that they could have supported the 320,000 needed if contractors were not employed. While the vast majority of contractor personnel were involved in noncombatant logistics tasks, DOD estimated there were over 20,000 armed contractors in Iraq during 2007. Other organizations have much higher estimates.[7] Even using the Pentagon's lower estimate,

**Dr. T.X. Hammes, a retired U.S. Marine Corps officer, is a Senior Research Fellow in the Center for Strategic Research, Institute for National Strategic Studies, at the National Defense University. This article was originally published as Institute for National Strategic Studies Strategic Forum 260 (NDU Press, November 2010).**

U.S. Army (Christopher Nicholas)

**DOD contractor conducting 3-week training course for Afghan National Army soldiers demonstrates positioning when firing M–16**

contractors provided three times more armed troops than the British. It should also be noted that in Iraq and Afghanistan, many unarmed logistic support personnel functioned in what the military would define as a combat role. The drivers were subjected to both improvised explosive devices and direct fire attacks. This combination of drivers willing to run the gauntlet of ambushes and armed contractors replaced at least two full combat divisions. Given the very low support-to-operator ratio that contractors maintain, it is not unreasonable to estimate they actually replaced three divisions.

The contractors not only provided relief in terms of personnel tempo but also reduced military casualties. Contractors absorbed over 25 percent of the killed in action in Iraq, which reduced the political resources required to maintain support for the conflict. By the end of 2009, contractors reported almost 1,800 dead and 40,000 wounded in Iraq and Afghanistan.[8] As the fighting in Afghanistan gets worse, contractors are now suffering more deaths than U.S. forces: "In the first two quarters of 2010 alone, contractor deaths represented more than half—53 percent—of all fatalities. This point bears emphasis: since January 2010, more contractors have died in Iraq and Afghanistan than U.S. military soldiers."[9] For practical purposes, these casualties were "off the books" in that they had no real impact on the political discussions about the war. As Peter Singer noted:

*there was no outcry whenever contractors were called up and deployed, or even killed. If the gradual death toll among American troops threatened to slowly wear down public support, contractor casualties were not counted in official death tolls and had no impact on these ratings. . . . These figures mean that the private military industry has suffered more losses in Iraq than the rest of the coalition of allied nations combined. The losses are also far more than any single U.S. Army division has experienced.*[10]

Contractor casualties are not reported via the Pentagon, but only through the U.S. Department of Labor. Labor's Web site notes that these are not comprehensive statistics but only represent those injuries and deaths that resulted in insurance claims.[11] Thus, it is difficult if not impossible to determine how many additional casualties were suffered by other nations' contractors in either Iraq or Afghanistan.

Replacing these contractors, both armed and unarmed, would have required additional major mobilizations of Reserves or a dramatic increase in Army and Marine Corps end-strength. In effect, the mobilization of civilian contractors allowed the United States to engage in a protracted conflict in Iraq without convincing the U.S. public of the need for additional major mobilizations or major increases in the Active Armed Forces. The decision to hire contractors can be taken out of view of the public while decisions to increase troop strength are usually subject to intense debate. Opponents of contractors point out that this makes it easier for U.S. political leaders to commit forces to protracted conflicts precisely because it reduces uniformed casualties.[12] Whether the tendency of contractors to reduce the political cost of operations is a good thing depends upon one's view of the particular conflict.

Another advantage frequently cited by proponents of the use of contractors is

that of cost. According to their calculations, contractors are much cheaper to use than government employees. In fact, the actual costs remain a point of contention. The Congressional Research Service reported that the "relative cost advantage of the contractors can vary, and may diminish or disappear altogether, depending on the circumstances and contract."[13] Determining actual costs is extremely difficult due to the large number of variables involved—some of them currently impossible to document. For instance, with over 40,000 U.S. contractors wounded to date, we are unable to estimate potential long-term care costs to the U.S. Government. While contractors may claim their insurance covers those costs, the government, in fact, paid for that insurance through the contract, and if the coverage proves insufficient, the government may well end up paying for the continued care through various governmental medical programs. In short, long-term costs associated with employing contractors in a conflict environment are essentially unknowable.

*long-term costs associated with employing contractors in a conflict environment are essentially unknowable*

However, one cost benefit of contractors is indisputable. As soon as the need goes away, they can be let go when the contract expires. Thus, unlike military or government employees who continue on the payroll or return to Reserve status, contractors are simply paid off and sent home.

Another useful aspect of contracting is that it can provide economic inputs to local economies by hiring locals to provide services. Creating jobs and stimulating the economy are key aspects of population-centric counterinsurgency. In the Balkans and Afghanistan, the North Atlantic Treaty Organization (NATO) and International Security Assistance Force (ISAF) have hired large numbers of local personnel to conduct both armed and unarmed tasks. Carefully targeted contracts can be used to co-opt local power structures to support the government.

General David Petraeus, ISAF commander, specifically tasked his commanders to be aware of both the benefits and dangers of contracting in Afghanistan. He ordered them to monitor their contracts carefully to ensure they are contributing to the counterinsurgency campaign.[14]

A final, critical advantage is that contractors can execute tasks that U.S. military and civilian forces simply cannot. Some tasks, such as providing large numbers of interpreters, are obvious and widely applicable. Others are situation-specific. For instance, in Afghanistan, we lack the forces to secure our primary supply lines to Pakistan because they run through areas either controlled or heavily contested by the Taliban or bandits and police who charge for use of the road. Furthermore, if history is any guide, even a heavy presence of U.S. troops would not guarantee the delivery of supplies. Fortunately, Afghan contractors display the mix of force, personal connections, and negotiation skills to maintain our supply lines.

## The Bad

When serving within conflict zones, particularly during a counterinsurgency, contractors create a number of significant problems from tactical to strategic levels. Three inherent characteristics of contractors create problems for the government. First, the government does not control the quality of the personnel that the contractor hires. Second, unless it provides a government officer or noncommissioned officer for each construction project, convoy, personal security detail, or facilities-protection unit, the government does not control, or even know about, their daily interactions with the local population. Finally, the population holds the government responsible for everything that the contractors do or fail to do. Since insurgency is essentially a competition for legitimacy between the government and insurgents, this factor elevates the issue of quality and tactical control to the strategic level. In addition to these inherent characteristics, there are numerous other negative outcomes that flow from using contractors. Contractors compete directly with the host nation for a limited pool of educated, trained personnel. Their presence and actions can dramatically change local power structures. They fragment the chain of command. And when they fail to perform, contractors can be difficult to fire.

Quality control is a well publicized issue. Repeated reports of substandard construction, fraud, and theft highlight the problems associated with unarmed contractors. As noted above, these incidents are being investigated. In addition, the U.S. Government is working hard to refine contracting and oversight procedures to reduce these types of problems. Despite their best efforts, however, contracting officers cannot control how contractors treat their local employees. Poor treatment,

U.S. Army (Jeremiah Green)

**Iraqi construction supervisor guides U.S. contractors through hospital under construction in Basra**

lack of respect for local customs, skills, and methods—and even physical abuse to include sexual exploitation—have been recurrent problems with unarmed contractors.

Unfortunately, the problem is just as prevalent with armed contractors. While high-end personal security details generally are well trained, less visible armed contractors display less quality. When suicide bombers began striking Iraqi armed forces recruiting stations, the contractor responsible for recruiting the Iraqi forces subcontracted for a security force. The contractor was promised former Gurkhas. What showed up in Iraq a couple of weeks later were untrained, underequipped Nepalese villagers.[15] Not only did these contractors provide inadequate security, but also the United States armed them and authorized them to use deadly force in its name.


U.S. Army (Rob Summitt)

**Emergency personnel evacuate contractor injured by shrapnel near Ad Diwaniyah, Iraq**

Since the government neither recruits nor trains individual armed contractors, it essentially has to trust the contractor to provide quality personnel. In this case, the subcontractor took shortcuts despite the obvious risk to the personnel manning the recruiting stations. Even if the government hires enough contracting officers, how can it determine the combat qualifications of individuals and teams of armed personnel? The U.S. military dedicates large facilities, major exercises, expensive simulations, and combat-experienced staffs to determine if U.S. units are properly trained. Contractors do not. We need to acknowledge that contracting officers have no truly effective control over the quality of the personnel the contractors hire. The quality control problems are greatly exacerbated when the contractor uses subcontractors to provide services. These personnel are at least one layer removed from the contracting officer and thus subject to even less scrutiny.

*it is virtually impossible to determine the effectiveness of contractors until they begin to operate in theater*

In reality, it is virtually impossible to determine the actual effectiveness of any contractors—armed or unarmed—until they begin to operate in theater (and only then if a member of the U.S. Government can observe the contractors as they operate).

Compounding the problems created by lack of quality control, the government does not control the contractor's daily contact with the population. Despite continued efforts to increase government oversight of contractor operations, nothing short of having sufficient numbers of qualified U.S. Government personnel accompanying and commanding contractors will provide control. This lack of control usually means we may get poorly wired buildings, malfunctioning computer systems, and unfinished projects. However, too often, it includes incidents of bullying, abuse, intimidation, and even killing of local civilians such as the DynCorp employee who ran a child sex ring in the Balkans or the September 2007 Blackwater shootings in Nisour Square, Baghdad.

This lack of quality and tactical control greatly increases the impact of the third major problem: the United States is held responsible for everything the contractors do or fail to do. Despite the fact the United States has no effective quality or operational control over the contractors, the local population rightly holds it responsible for all contractor failures. Numerous personal conversations with Iraqis revealed a deep disgust with the failure of many contractors to provide promised services despite being well paid. There was even more anger with the actions of armed contractors. Iraqis noted the United States gave the armed contractors authority to use deadly force in its name. While Iraqis were not confident that American forces would be punished for killing Iraqis, they believed it was at least a possibility. However, the Iraqis were convinced that contractors were simply above any law. The Iraqi perception that it will be impossible to prosecute a contractor is reflected in a Congressional Research Service report that required 17 pages simply to outline the various legal structures under which a contractor might be prosecuted. The paper indicated that there was no clear legal precedent for prosecuting contractors, and it noted none had been prosecuted up through August 2008.[16]

These perceptions can seriously undercut the legitimacy of both the host nation and U. S. Government. A key measure of the legitimacy of a government is a monopoly on the use of force within its boundaries. The very act of hiring armed contractors dilutes that monopoly.[17] Legitimate governments are also responsible for the actions of their agents—particularly those actions taken against their own populations. Despite efforts to increase the accountability of contractors, the Congressional Research Service noted the widespread perception that contractors who commit crimes against host nation people are outside the legal reach of both the host country and the United States.[18] Contractors, armed or unarmed, could be quickly flown out of the country if their company believed they violated a law. And while the United States has laws criminalizing certain activities, the cost and difficulty of trying a contractor for crimes that occurred overseas in a conflict zone has so far deterred U.S. prosecutors. In over 7 years of activity in Iraq, no contractor has been con-

victed in a U.S. court of a crime against Iraqi citizens.

Exacerbating the legitimacy issue, contractors of all kinds are a serious irritant to the host nation population. Armed contractors irritate because they are an unaccountable group that can and does impose its will upon the population in many daily encounters: forcing locals off the road, using the wrong side of the road, and pointing weapons at civilians. Even unarmed contractors irritate the population when they take relatively well paying jobs that local people desperately need while at the same time driving up prices. Contractors, when they do hire locals, often treat them with a lack of respect and trust. Furthermore, the complete control over who works on projects combined with the disrespect shown those locals that are hired reinforces local perceptions of the United States as an occupying power.

In addition to undercutting government legitimacy, the use of contractors may actually undercut local government power. In Afghanistan, security and reconstruction contracts have resulted in significant shifts in relative power between competing Afghan *qawms*[19] as well as allegations of corruption. Dexter Filkins, writing in the *New York Times*, notes that the power structure in Orugzan Province, Afghanistan, has changed completely due to the U.S. Government's selecting Matiullah Khan to provide security for convoys from Kandahar to Tirin Kot:

*With his NATO millions, and the American backing, Mr. Matiullah has grown into the strongest political and economic force in the region. He estimates that his salaries support 15,000 people in this impoverished prov ince. . . . This has irritated some local leaders, who say that the line between Mr. Matiullah's business interest and the government has disappeared. . . . Both General* [Nick] *Carter* [commander of ISAF South] *and Hanif Atmar, the Afghan interior minister, said they hoped to disband Mr. Matiullah's militia soon—or at least to bring it under formal government control. . . . General Carter said that while he had no direct proof in Mr. Matiullah's case, he harbored more general worries that the legions of unregulated Afghan security companies had a financial interest in prolonging chaos.*[20]

Thus, an unacknowledged but serious strategic impact of using contractors is to directly undercut both the legitimacy and the authority of the host nation government. In this case, the shortage of ISAF troops and sheer difficulty of maintaining security along this route means that there is currently no feasible alternative. That makes it more important than ever that the U.S. Government take specific actions to minimize the negative strategic impacts of this operational necessity. Contracting actions must be seen as an integral part of the campaign rather than simply treated as a logistics function.

Contracting also has a direct and measureable impact on the local economy. When the U.S. Government passes its authority to a prime contractor, that contractor then controls a major source of new wealth and power in the community. However, the contractor is motivated by two factors: maximizing profit and making operations run smoothly. This means that even if he devotes resources to understanding the impact of his operations on society, his decisions on how to allocate those resources will differ from those of someone trying to govern the area. For instance, various contractors' policies of hiring South Asians rather than Iraqis angered Iraqis during the critical early phases of the insurgency. Desperate for jobs, the Iraqis saw third country nationals getting jobs that Iraqis were both qualified for and eager to do.[21] While there were clear business and security reasons for doing so, the decision was a slap in the face of Iraqis at a time of record unemployment. In Afghanistan, the contractor can literally shift the local power structure by picking one *qwam* over another to execute the contract. The winning *qwam* gains rich resources and access to both U.S. and Afghan officials.

In contrast, the U.S. Government in the form of a Provincial Reconstruction Team (PRT) commander or a unit commander writes contracts specifically to influence the political and security situation in the area. Commanders see the contracts themselves as a campaign tool. While its effect is limited by the cultural understanding of the commander and is often less efficient for the specific project, this system can be much more effective in the overall counterinsurgency campaign.

A related problem is the perception of the local population concerning how these contracts are managed. In Afghanistan, many Afghans are convinced that some contracts expend up to 80 percent of the funds on management. The Agency Coordinating Body for Afghan Relief states that 40 percent of nonmilitary aid goes straight to corporate profit and salaries. Profit margins run as high as 50 percent, and full-time expatriate consultants cost between $250,000 and $350,000 per year.[22] Many of the contracts run through multiple subcontracting companies before the aid reaches the Afghan people; each subcontractor takes a percentage for administrative overhead.[23] These confirmed cases of misuse of development funds further reduce the weak legitimacy of the Afghan government as well as ISAF efforts.

There are also a number of indirect consequences of employing armed contractors. First, this practice opens the door for local organizations to build militias under the cover of being a security company. It is difficult to object to other elements of a society hiring security when the government is doing so. This is particularly true when the government is hiring both locals and foreign nationals to provide security. If the government needs private contractors to feel safe, the citizens, local businesses, or even local political organizations can certainly argue that they do, too. This fact has created significant problems for ISAF in Afghanistan:

*Because PSCs* [private security companies] *are under the control of powerful individuals, rather than the Afghan National Security Forces, they compete with state security forces and interfere with a government monopoly on the use of force. There is growing pressure from ISAF and within the Afghan government to reform and regulate these companies. Major General Nick Carter, the commander of Regional Command–South, recently briefed that ISAF was developing a strategy to regulate PSCs as part of the Kandahar Operations unfolding in summer 2010.*[24]

In addition, private security companies can compete directly with host nation attempts to recruit and retain military and police personnel. In January 2010, Major General Michael Ward, Deputy Commander Police, NATO Training Mission Afghanistan, stated that Afghanistan's government was considering capping the pay of private security firms because Afghan police were deserting in large numbers for the better pay and working conditions associated with private companies.[25] This has created significant problems for ISAF. General Carter told reporters:

[P]*rivate security companies and militias are a serious problem . . . this is, of course, something that is of our own creation to a degree . . . where we contracted out everything to the civilian market, has created these private security companies. And of course they are paid a great deal more than our Afghan security forces, which in itself is counterproductive because, of course, the temptation for a soldier in the ANP* [Afghan National Police] *is to go across to a private security company because he might earn double in pay.*[26]

Contract hiring of unarmed personnel also competes directly with the host nation civil government. In both Iraq and Afghanistan, educated professionals took jobs as drivers or clerks with contractors and nongovernmental organizations (NGOs) simply because the jobs paid more than they could earn working for their own governments. In effect, ISAF and NGO hiring has created an internal "brain drain." This is of particular concern in Afghanistan where human capital is a major limitation on the ability of the government to function.

On August 16, 2010, President Hamid Karzai decreed that all private security contractors must cease operations in Afghanistan within 4 months.[27] Unfortunately, currently ISAF and most humanitarian agencies rely on armed contractors to provide security for essential operations, and neither ISAF nor the Afghan Security Forces are prepared to execute those missions.

At the time of this writing, it is too early to evaluate the impact of President Karzai's announcement, but it does highlight the political complications that such contractors inject into counterinsurgency campaigns.

Contractors, both armed and unarmed, also represent a serious military vulnerability. In the uprising in Iraq during the spring of 2004, both Sunni and Shia factions conducted major operations against coalition forces. The insurgents effectively cut Allied supply lines from Kuwait. U.S. forces faced significant logistics risks as a result. Despite the crisis, U.S. officials could not morally order unarmed logistics contractors to fight the opposition. The contractors lacked the training, equipment, and legal status to do so. Had the supply line been run by military forces, it would have been both moral and possible to order them to fight through. Despite this demonstrated operational vulnerability, the fact that unarmed contractors are specifically not obligated to fight has not been discussed as a significant risk in employing contractors rather than military logistics organizations. Furthermore, while military logistics units can provide their own security in low threat environments, unarmed contractors cannot. The government must either assign military forces or hire additional armed contractors to provide that security.

The substitution of unarmed contractors for Soldiers and Marines creates yet another vulnerability: lack of an emergency reserve. In the past, support troops have been repeatedly employed in critical situations to provide reinforcements for overwhelmed combat troops. Contractors are simply unable to fulfill this emergency role. This limitation, as well as the unarmed contractor's inability to fight, is even more significant in conventional conflicts than in irregular war.

Contracting also takes key elements of the counterinsurgency effort out of the hands of the commander. In the spring of 2010, ISAF determined that DynCorp had failed in its contract to train and mentor the Afghan police.[28] ISAF then put the contract out for competition. General Stanley McChrystal, then-commander of ISAF, stated that the police were one of the most critical elements of his campaign plan, so the contracting process was accelerated. Not surprisingly, DynCorp did not win the new contract. Since time is critical in Afghanistan, plans were made to rapidly transition the contract to a new provider to ensure that the Afghan police could play their part in the counterinsurgency campaign. However, DynCorp successfully protested the contract award.[29] Thus, it retains the training contract and will retain it until all legal processes are exhausted. In short, the commander lost control of one of the critical elements of his counterinsurgency campaign at a critical time—and there was nothing he could do about it. Despite DynCorp's documented failure, at the time of this writing, it remains in charge of police training and mentoring with the full knowledge that as soon as possible ISAF will get rid of DynCorp.

Contracts also fragment the chain of command. All military units in a theater are under the command of a military officer, but contractors are not. While both contractors and the government have worked hard to resolve coordination issues, the fact remains that contractors are not under military command. Complicating any attempt to create unity of effort is the fact that contractors are in direct competition with each other and treat a significant portion of the information concerning their operations as proprietary information, which they will not share with the government or their competitors.

### Strategic Impact

Despite the numerous problems articulated above, contractors will have an important and continuing role in U.S. operations—both domestic and overseas. There are currently numerous important functions that the U.S. Government is incapable of performing without contractor support. This is not a new phenomenon. DOD—particularly the Air Force and Navy—has long relied on contractors to fill niche requirements such as maintaining and, sometimes, even operating the newest high technology equipment. More recently, contractors have been hired to execute many of the routine housekeeping tasks at permanent U.S. military facilities.

However, despite conducting almost 9 years of combat operations supported by contractors, the United States still has not conducted a substantial examination of the strategic impact the use of contractors has in counterinsurgency. This does not mean contracts and contractors are not being studied. Congress formed the Commission on Wartime Contracting specifically "to assess a number of factors related to wartime contracting, including the extent of waste, fraud, abuse, and mismanagement of wartime contracts."[30] Focused on improving the efficiency of wartime contracting, the commission did not discuss the strategic impact of using contractors in its 2009 Interim Report.[31] This author hopes that the commission will include the strategic impact in its final report in 2011.

Within the executive branch, DOD and the Department of State are conducting studies on how to reduce fraud and increase the efficiency of contractors. The Joint Staff is running a major study to determine the level of dependency on contractor support in contingency operations. Various Department of Justice investigations are going over past contracts for everything from fraud to abuse of prisoners to inappropriate use of deadly force. Yet none of these studies is looking at the fundamental questions concerning the strategic impact of contractors in combat.

Contractors clearly can have a strategic impact on the success of counterinsurgency operations in a variety of ways. The most important include reducing the political capital

U.S. Army (Charles R. Brice)

**Plane from private contractor Blackwater Air closely follows lead element after supply drop to friendly forces in Sharana, Afghanistan**

necessary to commit U.S. forces to war; potentially reducing the legitimacy of a counterinsurgency effort; and damaging the perceived morality of the war effort. Rather than automatically defaulting to hiring contractors as a relatively quick, easy, and politically benign solution to an immediate problem, the United States should first answer several key strategic questions.

First, what is the impact of contractors on the initial decision to go to war as well as the will to sustain the conflict? Contractors provide the ability to initiate and sustain long-term conflicts without the political effort necessary to convince the American people a war is worth fighting. Thus, the United States can enter a war with less effort to build popular consensus. Most wars will not require full-scale national mobilization, but rather selective mobilization of both military and civilian assets. Both proponents and opponents admit that without contractors, the United States would have required much greater mobilization efforts to generate and support a force of 320,000 in Iraq (the combined troop and contractor count) or a force of over 210,000 in Afghanistan. The use of contractors allowed us to conduct both wars with much less domestic political debate.

But is this good? Should we seek methods that make it easier to take the Nation to war? That appears to be a bad idea when entering a protracted conflict. Insurgents understand that political will is the critical vulnerability of the United States in irregular warfare. They have discussed this factor openly in their online strategic forums for almost a decade.[32] Ensuring that the American public understands the difficulty of the impending conflict and is firmly behind the effort should be an essential element in committing forces to the 10 or more years that modern counterinsurgencies require for success. Thus, while the use of contractors lessens the extent of political mobilization needed, it may well hurt the effort in the long term.

Second, as discussed earlier in this article, contractors can undermine the legitimacy of both U.S. and host nation counterinsurgency efforts in a variety of ways. Field Manual 3–24, *Counterinsurgency*, states that the conflict is a competition for legitimacy between the counterinsurgent and the insurgent.[33] Widespread use of contractors can directly undercut a central theme of counterinsurgency doctrine. Under certain conditions, we may choose to use contractors in spite of the negative impact on legitimacy, but we should not do so in ignorance of that impact. Any decision to use contractors in a conflict zone should be carefully considered for its impact on the strategy that we have chosen and the campaign plan we are using to execute that strategy.

A third area that needs strategic consideration is the morality of using contractors. What are the moral implications of authorizing contractors, qualified or not, to use deadly force in the name of the United States? What about hiring poor Third World citizens to sustain casualties in support of U.S. policy? What is the U.S. responsibility for wounded and killed contractors—particularly those from the Third World? While these sound like theoretical questions, they are in fact practical ones. Maintaining long-term domestic popular support for conflict requires that U.S. actions be both legitimate and moral.

## Recommendations

Currently, the Commission for Wartime Contracting (www.wartimecontracting.gov)

is examining a broad range of issues concerning wartime contracting and will present its final report in 2011. Of particular interest will be the report's findings on "inherently governmental" functions that should not be done by contractors. Even as the commission continues its work, the manpower requirements of the current conflicts mean that, for the near term, the United States will continue to employ a large number of contractors in war zones. In fact, as our forces draw down in Iraq, the State Department has stated its requirement for security contractors will increase significantly.[34]

Near-term operational imperatives and the potential negative strategic impacts discussed above highlight the need for clear guidelines about when and how the U.S. Government should employ contractors. This question should be a central part of our post-Afghanistan force structure discussions. The size and type of force that we build for the future depend on a clear concept of how the United States plans to use contractors, both armed and unarmed, in present and future conflicts. This discussion cannot wait until the commission's report is finalized and approved. The Secretary of Defense is already pushing the Department to reduce its budget significantly. The debate about future force structure is well under way.

A number of factors are putting major pressure on force structure planners. The primary pressure will be the falling budgets that Secretary Robert Gates has clearly warned the Services to expect. In addition, as U.S. forces begin to withdraw from Afghanistan, force planners will have to decide how to allocate limited resources to position the Armed Forces to deal with future conflicts. There is an intense, ongoing debate about which types of conflicts should take priority and then how the forces should be structured, equipped, and trained to deal with those contingencies. A tempting way to avoid tough decisions will be to assume contractors will provide major services across the spectrum of conflict, thus dramatically reducing the force requirements for logistics and security. In the past, we have often sacrificed force structure to save weapons systems. Planning to use contractors in future conflict zones would reinforce this tendency.

Any force planning documents should clearly state what assumptions have been made concerning the functions of the contractors who will support the force. The following guidelines should be employed in considering when and how to use contractors in the future.

The U.S. Government's default position should be no contractors "outside the wire" in a conflict zone. Contractor presence outside secure facilities places them in direct contact with the population. Contractors can undercut the legitimacy of the host nation government, reduce the accountability of the U.S. Government for actions taken in its name, irritate the population, compete directly for the most competent local personnel, fragment the chain of command, provide an excuse for forming local militias, and are difficult to fire—even when ineffective. Given these issues, the United States should strive to keep contractors out of conflict zones. This will not always be possible but should be the standard. Most of the problems highlighted in this article occurred in conflict zones. The unique stresses on the contractors combined with the severe limitations on the government's ability to oversee their performance resulted in repeated actions that reduced operational effectiveness and undercut the U.S. strategic position. The cost savings of using contractors are uncertain at best. In contrast, the strategic and operational problems that arise from using them in a counterinsurgency are clear and documented.

The U.S. Government is unlikely to have enough government employees to perform the numerous housekeeping functions—mess, laundry, cleaning, and so forth—that are an integral part of any operation. Therefore, the default position should remain that we hire contractors only for those functions that take place within a secure facility and require minimum contact with host nation personnel. This means that DOD must be able to provide security for other U.S. Government organizations working in conflict zones until such time as they can hire and train sufficient

U.S. Air Force (Dayton Mitchell)


**Wounded Afghan security contractor is transported to aid station at Combat Outpost Rath, Afghanistan**

government security personnel. Exceptions to this rule should be closely examined. This position must be an explicit factor in force structure planning. The one consistent exception to this rule will be interpreters since the U.S. Government simply cannot maintain sufficient linguistic capability for the wide range of possible future commitments.

If U.S. Government capacity is exceeded, the default position should become using host nation organizations first and host nation contractors next with U.S. or foreign contractors being a choice of last resort. As noted, even with a default position of not hiring contractors in conflict zones, some elements of the government would most likely hire contractors, including armed contractors, in future conflicts. Some agencies could determine that they cannot achieve an assigned task without contractors and would be unable to get other U.S. Government partners to take the mission. To minimize the negative impact of contractors in irregular war, policy should give strong preference to the host nation providing the services—even if they have to be funded and supported by the United States.

Examples where local contractors should be first choice are inside secure facilities and as fixed point security. Many of the jobs contractors perform inside facilities—meal preparation, cleaning—can easily be done by local labor. Since local contractors would commute to and from work, hiring them would require more effort be dedicated to security than the current practice of importing South Asian laborers and keeping them on base. However, hiring local laborers provides economic stimulus. In addition, the fixed point security mission may well be appropriate for local personnel because these jobs require little training and, because they are in a fixed position, are easier to supervise. The primary effort should be to train local personnel to execute such jobs with those security personnel transitioning to the appropriate host nation government authority as soon as possible. Transitioning supervision of these personnel to local governments could be easier than doing so with regular army or police. However, caution must be exercised whenever considering armed contractors because the very act of the government hiring contractors legitimizes the private use of force. If a government needs to hire armed protection, then it is difficult to deny businesses, political parties, and other entities the right to hire armed contractors. In both

DOD (R.D. Ward)

**Under Secretary of Defense for Acquisition, Technology, and Logistics conducts news conference on DOD acquisition strategies to incentivize contractors to cut program costs**

Iraq and Afghanistan, this dynamic led to private militias that work for local strongmen rather than a local community. NGOs, who often have been forced to hire contractors as the security situation deteriorates, would continue to insist on protecting their people. Thus, a major focus of the initial effort must be to replace contract security with government-provided security.

In cases where the host nation lacks the necessary capacity, local companies and personnel should receive strong preference. In irregular war, it is important that these jobs be assigned to the local population both to stimulate economic growth and provide alternatives to insurgent employment for local males. While such contracts may be necessary, maximum effort should be made to ensure that responsibilities are transferred to the host nation government personnel as early as possible. Even as host nation government capacity grows, there may be some jobs that require local security contractors. In Afghanistan, escorting logistics convoys from Pakistan to Afghanistan falls into this category. The historical record indicates ISAF or the Afghan government would require massive forces to accomplish the mission. The Afghan "security companies" have succeeded at this task, but operate outside ISAF rules of engagement, upset local power structures, and can create additional enemies. Future use of local security companies for such missions must be carefully balanced against their negative side-effects and employed only when there is no other solution. If President Karzai enforces his order that contract security cease operations by December 2010, this may provide a valuable case study in how government forces can replace armed contractors or the negative impacts if they attempt to replace contractors but lack the capacity to do so.

The default position should be to hire contractors or U.S. Government civilian employees to fill those billets requiring deployment to locations *outside* the conflict zone. One of the greatest problems the U.S. military faces in protracted war is personnel tempo—the period Service personnel spend away from home. By hiring contractors to fill jobs overseas but outside the conflict zone, the United States can reduce the personnel tempo of the uniformed forces. Our current use of contractors in Kuwait is a good example of this approach. While deployments to Kuwait to support the effort in Iraq are not dangerous, they do increase the personnel tempo of the uniformed Services. Thus, DOD has filled

U.S. Navy (Michael D. Heckman)

**Contractor hired to supplement security stands watch at main entry point tower, Contingency Operating Base Speicher, Iraq**

most of these billets with contractors, who have compiled a very good record running the training, maintenance, and transit facilities in Kuwait. This type of well-defined, repetitive administrative task is ideal for contractors particularly in a forward-deployed, nonconflict location. Furthermore, the contractors, like all expatriates working in the country, are subject to Kuwait's legal system, and thus, the local population sees them as accountable to Kuwait authority.

Aggressive efforts should be made to use either DOD civilian employees or contractors to fill nondeploying military billets. As stated, personnel tempo is a major problem for the Services. Yet the Defense Business Board noted that, despite 9 years of conflict, fully 40 percent of Active-duty personnel have not deployed to a conflict zone, and an additional 30 percent have deployed only once.[35] While a significant number of these nondeployers are first-term personnel who have not yet received sufficient training to deploy, the number of career force personnel who have not deployed is still high. These personnel are filling nondeploying billets. Rather than hiring contractors to fill billets inside the conflict zone, we need to examine which of these nondeploying billets can be filled by contractors, freeing uniformed personnel to deploy.

If contractors are required, they must be under the direct supervision of a U.S. Government employee. While the government is making strenuous efforts to increase the number of contracting officers and to become more specific in writing contracts, the fact remains that the government cannot control contractor actions without direct supervision. Unless it has direct supervision, the government will remain unaware of contractors whose actions alienate the local population or fail to meet U.S. standards. The degree of supervision will vary with the type of work being done. Routine maintenance work in a secure facility would require only normal contracting oversight. Armed escorts or drivers who are in regular contact with civilian populations would require constant supervision in the form of a government employee riding with each vehicle and commanding each convoy. This would give rise to a number of problems such as having a government employee making less money but taking the same risks as a contractor or having a less experienced government employee supervising a more experienced and often older contractor. However, these are minor problems compared to those created by the population's perception of unsupervised contractors.

## Long-term Requirement

This article has focused on the current U.S. use of contractors in conflict zones, but the use of armed contractors is on the rise around the world. Led by the United States, many nations have reintroduced armed contractors to conflict zones. In addition, the lack of security in undergoverned areas has led NGOs, international organizations, private companies, and even nation-states to hire armed contractors to provide security

and unarmed contractors to deliver services. In some cases, it is difficult to tell if contractors are part of a private firm or are hired by a government that does not wish to send official government personnel. The most serious potential problems arise from the fact that large numbers of armed contractors are being injected into an international security arena that lacks recent experience in regulating them.

Armed contractors are having a global impact well beyond that of the two irregular wars America is fighting. Armed contractors introduce a new element into international relations. Current international law and international organizations such as the United Nations have developed protocols and procedures for dealing with the use of the armed forces of nation-states as well as insurgents. However, these same organizations have a paucity of experience in dealing with the introduction of armed contractors into a conflict zone whether those contractors are hired by a private firm or a nation-state. This leads to a final recommendation.

The United States must develop policies and procedures to deal with the presence of armed contractors in conflict zones. Because these armed entities are generally outside the experience and mandate of current international organizations and mechanisms, they will continue to have unforeseen impacts. Thus, the United States must work with other states, NGOs, and international organizations to develop policies, procedures, and institutions to deal with the presence of armed contractors in conflict zones. The Montreux Document is an example of such an effort and deserves the support of the United States.[36] However, it is only the first step in learning to manage these new players in the international arena. **JFQ**

## NOTES

[1] Moshe Schwartz, *Department of Defense Contractors in Iraq and Afghanistan: Background and Analysis* (Washington, DC: Congressional Research Service, July 2, 2010), 5.

[2] Congressional Budget Office, "Contractors Support of U.S. Operations in Iraq," table 2, available at <www.cbo.gov/ftpdocs/96xx/doc9688/MainText.3.1.shtml>.

[3] Schwartz, 5.

[4] Peter W. Singer, "The Dark Truth About Blackwater," October 2, 2007, available at <www.salon.com/news/feature/2007/10/02/blackwater/print.html>.

[5] Dan Baum, "Nation Builders for Hire," *The New York Times*, June 22, 2003, available at <www.informationclearinghouse.info/article3905.htm>.

[6] "Wising Up, Moving Out," *Jane's Defence Weekly*, July 1, 2009, 29.

[7] Steve Fainaru, "Private War: Convoy to Darkness," *The Washington Post*, July 29, 2007, 1.

[8] See <http://icasualties.org> and <www.propublica.org/series/disposable-army>.

[9] Steven L. Schooner and Colin D. Swan, "Contractors and the Ultimate Sacrifice," *Service Contractor*, September 2010, 17.

[10] Singer.

[11] Department of Labor, Office of Workers Compensation Programs, available at <www.dol.gov/owcp/dlhwc/lsaboutdbareports.htm>.

[12] David Isenberg, *Private Military Contractors and U.S. Grand Strategy* (Oslo, Norway: International Peace Research Institute, January 2009), 5.

[13] Jennifer K. Elsea, Moshe Schwartz, and Kennon H. Nakamura, *Private Security Contractors in Iraq: Background, Legal Status, and Other Issues* (Washington, DC: Congressional Research Service, updated August 25, 2008), 49.

[14] David H. Petraeus, "COMISAF's Counterinsurgency (COIN) Contracting Guidance," Kabul, Afghanistan, September 8, 2010.

[15] Author's experience while serving on Coalition Military Assistance Training Team in Iraq during early 2004.

[16] Elsea, Schwartz, and Nakamura, 15–31.

[17] There are a limited number of cases where armed contractor action can increase the legitimacy of a government—for instance, protecting a hospital or refugee camp. However, even in these benign cases, the presence of contractors shows the government cannot protect its people and opens the door for any business or association to hire its own armed guards—in essence a private militia.

[18] Elsea, Schwartz, and Nakamura, 13–14.

[19] Afghans identify themselves by *qawm*, rather than by tribe or nationality. A *qawm* identity is based on kinship, residence, and sometimes occupation. Although *qawm* is sometimes translated into English as *tribe*, the *qawm* relationship may cross tribal or even ethnic boundaries. The *qawm* is the basic unit of social community in Afghanistan, but the relationships involved can vary from ethnic group to ethnic group.

[20] Dexter Filkins, "With U.S. Aid, Warlord Builds Afghan Empire," *The New York Times*, June 6, 2010, available at <www.nytimes.com/2010/06/06/world/asia/06warlords.html>.

[21] Nicholas Pelham, "Contractors in Iraq Accused of Importing Labor and Exporting Profit," *The Financial Times*, October 14, 2003, available at <www.commondreams.org/headlines03/1014-01.htm>.

[22] Matt Waldman, "Falling Short: Aid Effectiveness in Afghanistan," available at <www.acbar.org/ACBAR%20Publications/ACBAR%20Aid%20Effectiveness%20(25%20Mar%2008).pdf>.

[23] Roya Wolverson, "Not So Helpful," *Newsweek*, November 24, 2007, available at <www.newsweek.com/id/72068>.

[24] Carl Forsberg and Kimberly Kagan, "Consolidating Private Security Companies in South Afghanistan," Institute for the Study of War, May 28, 2010, accessed at <www.understandingwar.org/files/BackgrounderPSC.pdf>.

[25] "Afghan-Cda Security Firms," The Canadian Press-Broadcast Wire, January 25, 2010, document BNW0000020100126e61p00011.

[26] Major General Nick Carter's Defense Department briefing via teleconference from Afghanistan, May 26, 2010.

[27] "Afghan Leader to Ban Security Contractors," August 16, 2010, available at <www.cbsnews.com/stories/2010/08/16/world/main6776999.shtml>.

[28] Pratap Chatterchee, "DynCorp Oversight in Afghanistan Faulted," available at <www.ipsnews.net/news.asp?idnews=50477>.

[29] Government Accountability Office Press Summary, "Decision on Bid Protest by DynCorp International Regarding U.S. Army Contracts in Afghanistan," available at <www.gao.gov/press/dyncorp_2010mar15.html>.

[30] The Commission on Wartime Contracting in Iraq and Afghanistan, available at <www.wartimecontracting.gov>.

[31] Ibid., "At What Cost? Contingency Contracting in Iraq and Afghanistan," June 2009, available at <www.wartimecontracting.gov/docs/CWC_Interim_Report_At_What_Cost_06-10-09.pdf>.

[32] Middle East Media Research Institute, "Bin Laden Lieutenant Admits to September 11 and Explains Al-Qa'ida's Combat Doctrine," February 20, 2002, available at <www.memri.org/report/en/0/0/0/0/0/0/607.htm>.

[33] Field Manual 3–24/Marine Corps Warfighting Publication 3.33–5, *Counterinsurgency* (Washington, DC: Headquarters Department of the Army, Headquarters Department of the Navy, December 2006), 1–1.

[34] William Matthews, "U.S. Contractor Use in Iraq Expected to Rise," *Defense News*, July 12, 2010, available at <www.defensenews.com/story.php?i=4704826>.

[35] Defense Business Board, "Reducing Overhead and Improving Business Operations: Initial Observations," accessed at <http://defensenewsstand.com/showdoc.asp?docid=5192010_may19a>.

[36] See *The Montreux Document* (Geneva, Switzerland: International Committee of the Red Cross, August 2009), available at <www.icrc.org/web/eng/siteeng0.nsf/htmlall/montreux-document-170908/$FILE/ICRC_002_0996.pdf>.

Afghan National Security Forces provide security during Key Leader Engagement in Khost Province

ISAF

# Silent Kingmaker

## The Need for a Unified Wartime Contracting Strategy

*By* JONATHAN PAN

*International support—financial, political, and military—is kingmaker in Afghanistan.*

—Carl Forsberg, *Politics and Power in Kandahar*

**Captain Jonathan Pan, USA, is an Economic Development Officer in the 5th Brigade/2d Infantry Stryker Brigade Combat Team.**

Wartime contracting in Afghanistan is broken, and the breakdown has led to a new breed of nouveau riche warlords, men who are too young to have fought the Soviets but who are more politically and economically savvy than their mujahideen predecessors. This new breed is called *commercial warlords*. In short, commercial warlordism is based on money and guns. Their money is not being reinvested into the local economy, but diverted to their Dubai slush funds; their hired guns are pointed not at the Taliban but rather at the citizenry and their political opponents. These commercial warlords have created an environment in which the North Atlantic Treaty Organization (NATO) International Security Assistance Force (ISAF) and the Quetta Shura Taliban are in a stalemate—a stalemate that these warlords want to perpetuate. If there is no more war, there is no more money.

For the Afghan populace, the revulsion against commercial warlords and greedy contractors is second only to the lack (or perceived lack) of security. For this war as well as future wars, it is time for NATO to realize that aid can be a problem and that every dollar or euro spent should be a dollar or euro leveraged. This article argues that the Alliance must create a unified wartime contracting strategy to combat commercial warlordism. This strategy must:

- limit price inflation on materials and services
- limit substandard performance through proper quality assurance and quality control by civil engineers
- increase access to contracts for local companies

- identify commercial warlords through financial forensics
- allow the Afghan National Security Forces (ANSF) to provide security instead of armed security groups
- ensure all national contracting commands are placed under the regional command
- rebalance the focus of tactical requirements versus governance goals.

## Price Inflation and Substandard Performance

The Tarnak Bridge in Kandahar Province, located on Highway 4 south of Kandahar City, was completed in 2005 at a cost of $247,000. Maintaining freedom of movement on this highway is important because of the imports and exports that come and go from Pakistan through the Wesh-Chaman border crossing point, which lies at the end of the highway. Aside from trade, the highway is important for military purposes. Nearly 90 percent of nonsensitive cargo supporting U.S. forces in Afghanistan passes through Pakistan. Before April 2009, 80 percent of all traffic went through Torkham Gate at the Khyber Pass, Afghanistan's busiest port of entry, and 20 percent went through the Wesh-Chaman Gate. As of November 2009, 40 percent went through the Wesh-Chaman Gate, and 60 percent through Torkham Gate.

A suicide attack on the Tarnak Bridge in February 2010 downgraded civilian, economic, and military traffic to one-way travel. Repairs on the bridge amounted to $527,000—more than double the cost of the original bridge. Part of the reason for this inflated price is the development and construction boom in Afghanistan that has companies charging from $33 to over $100 per cubic meter of gravel, with some contracting officials paying the higher end of this spectrum. Another reason is that the bridge was not properly constructed in the first place. The topping slab, which distributes the weight of the girders, was never placed on the bridge. This severely increased the wear and tear as certain girders received all the weight. Nevertheless, a letter dated January 9, 2006, from the United Nations Office for Project Services (UNOPS) says that the company "constructed this project to the satisfaction of UNOPS/PRT [Provincial Reconstruction Team] with the workmanship over the whole project being to a very high standard." A common problem among projects is the lack of engineers who can assess workmanship.

To prevent possible future degradation of freedom of movement, a causeway will be built around the bridge for $1.16 million because suicide attacks cannot be prevented unless every vehicle is searched at a checkpoint away from the bridge. However, this option is not feasible due to the volume of commercial, civilian, and military traffic. Without having a viable Afghan government solution, commercial warlords have an incentive to target projects just to have them repaired at a premium price. The Kandahar Department of Public Works, which is responsible for road maintenance, will not work outside a 10-kilometer radius of Kandahar City.

The solution to the price inflation is to create—and strictly adhere to—a price index of common construction materials or services. To prevent substandard performance, qualified engineers who can properly conduct quality assurance and quality control of projects must serve as project managers.

## Subcontracting Due to Lack of Access

The Tarnak Bridge project illustrates the large sums of money entering the Afghan economy. ISAF knows little about where the money is going.

Research of open source contract records and company profiles revealed that the company that built the Tarnak Bridge was Bilal Noori Construction Company (BNCC), which started out as Afghanistan Social Action Program (ASAP) in 1997. The Tarnak Bridge was completed as a joint venture between ASAP and the Attar Group of Construction and Trading Company. The owner of the Attar Group also owns the Afghanistan Rehabilitation Construction Company. At some point in time, Attar's owner was part of ASAP (he signed a contract on behalf of ASAP with the Kandahar Airfield Contracting Office on November 4, 2003). Afghan companies often change names and business owners frequently own multiple companies. Therefore, if a contracting office were to blacklist BNCC, the office probably would not know the names of the other companies the BNCC owner holds.

When companies do not have the capacity to do a whole project by themselves, they enter into a joint venture, such as BNCC and the Attar Group did for the Tarnak Bridge. On the other hand, subcontracting usually entails one company that has access to contracts subcontracting the whole project to another that did not. For example, there was a $40,000 per month service contract in a Kandahar district that was awarded to Revival Company, which is owned by a former subcommander of Ahmad Shah Massoud, the so-called Lion of Panjshir. A Kandahar company performed as a subcontractor for $35,000 per month. Basically, the contracting office paid a 12.5 percent markup only because the subcontrac-


Joint Task Force Afghanistan (Matthew McGregor)

**Canadian engineers repair bridge damaged by suicide car bomb in Kandahar, Afghanistan**

tor did not have access to the contracting office in Kandahar. While $5,000 might seem insignificant to NATO, the idea that a company from Kabul or the Panjshir Valley is winning contracts in Pashtun-majority Kandahar is hard for many contractors as well as ordinary citizens to accept. Of more than 100 companies whose representatives met with or were interviewed by the author, every single one was said to have received a subcontract for a project in Kandahar from a company in Kabul. It is not only the Kabul and Panjshir Valley companies that subcontract to Kandahar companies—some Kandahar companies profit from their access as well.

In July 2009, BNCC signed a $3.1 million contract for asphalt road construction and repair that the company had no capacity to do. Instead of entering into a joint venture with another company, BNCC subcontracted all the construction work to two companies: Esmat Arman Construction Road and Supplying Company (EACC) and Hafez Construction and Road Building Company (HCRC). When these companies were asked why they did not bid for the project themselves, their reply was that they did not know about it. Only the politically connected companies have access to NATO installations and therefore their respective contracting offices. For instance, many companies not owned by the Pashtun Popalzai and Barakzai tribes have informed me that they have had difficulty getting access to Kandahar Airfield.

## Financial Forensics

Researching projects costing over $200,000 and the companies that perform them inevitably results in the identification of commercial warlords. The Highway 4 project was supposed to be completed no later than October 21, 2009. The road was completed 16 weeks late with no penalty to the contractor. Part of the delay was caused when the provincial governor of Kandahar, Tooryalai Wesa, stopped the project for an unknown duration. Rumors generally diverge into two paths; the first was that the governor stopped the project because BNCC was a company from Herat that subcontracted the construction work; the second was that the governor wanted to award this contract to his own select group of companies. Although BNCC has an office in Herat, it appears to have its main headquarters in Kandahar. It is unknown how the governor actually stopped the project, and it is unknown what BNCC had to do to continue.

While a civilian official has a reason to be involved in development projects, the involvement of an ANSF commander in development projects beyond security is dubious. There are allegations that Colonel Abdul Razziq, an Afghan Border Police commander, placed the BNCC's owner in jail due to the delay of the project. The subcontractors believed that this happened because Razziq attended the Spin Boldak shura and promised that the road would be completed regardless of any difficulties. Razziq was also recommending contractors to NATO forces as well as threatening contractors that NATO would not pay them if they did not meet his demands.

*contracts and statements of work are so technical that even native English speakers find them difficult*

This threat was applied to EACC/HCRC when Razziq demanded what the company thought were modifications on the contract. Technically, this was all stipulated in the 40-page statement of work, but the company strongly believes that they made modifications out of their own pockets that totaled $586,000. This situation partly stems from the fact that contracts and statements of work are so technical that even native English speakers find them difficult. That makes it almost impossible for local Afghan contractors to comply, unless they choose the ones with Western consultants, which fuels the rage of the Afghan population.

The owner of BNCC alleges that Razziq and contracting officials promised him the second phase of the project, which was to pave the final 2.2 kilometers of Highway 4 to the Pakistan border. Due to financial forensics, BNCC was not sent solicitations for the second phase because it was assessed by the unit on the ground as well as the provincial government as doing a poor job. Also, the financial forensics process revealed a new layer of information that was previously unavailable to NATO forces.

## Private Security, Public Cost

According to the subcontractors, security costs amounted to 9 percent ($280,000) of the contract price. Instead of using private security, EACC/HCRC used local subcommanders. EACC claims that Razziq normally charges an overall fee for operating in the Spin Boldak district. However, due to the high visibility of this project, he waived this fee but continued to allow his subcommanders to provide laborers and security from the two dominant tribes in the district, the Noorzai and the Achekzai.

Some argue that ANSF commanders, usually the police, should not be involved in the private security business. Some contend that paying the police is the same as bribery. Counterintuitively, using the police as security for construction companies actually forces them to get outside instead of hunkering down in their checkpoints. The alternative to ANSF providing security is unacceptable:

*Forty members of a Karzai-affiliated unit, the Kandahar Strike Force, entered the office of the Kandahar City prosecutor and demanded the release of an associate being held for car theft and forgery. . . . The Kandahar City prosecutor refused to hand over the suspect, leading to an exchange of gunfire during which Kandahar Province Police Chief Matiullah Qateh was killed.*[1]

Furthermore, in the volatile south, new police recruits earn $240 a month while their rival armed security groups make upward of $600 a month, not including food and transportation to the work site. The private security company that EACC frequently uses is Asia Security Group, which is owned by Hashmat Karzai, cousin of President Hamid Karzai.

If NATO were to promote the usage of ANSF as security, perhaps recruitment and retention might increase. Although distasteful by Western standards, NATO's unified wartime contracting strategy should allow companies to utilize ANSF as security for the cost benefit as well as undermining the private security racket.

## Refocusing

Do substandard performances, extended delays, and usage of ANSF as security warrant a blacklist, a warning to the company, or just a warning to the contracting offices? If one nation's contracting office does one of the above, will its other NATO partners comply as well? These questions cannot be resolved until all national contracting commands answer to the regional commands. The regional

U.S. Army (Kristina Gupton)

**Afghan contractors mix concrete for soldier housing at Contingency Operating Base Pushtaysark, Parwan**

command cannot tell the national contracting commands what to spend money on, but it should be able to tell them who not to use based on historical data and evidence.

The lack of a standard contracting policy requires a joint NATO effort rather than individual national efforts. For the United States, the National Defense Authorization Act (P.L. 110–181) established the Special Inspector General for Afghanistan Reconstruction (SIGAR) in 2008 with the mission to "enhance oversight of programs for the reconstruction of Afghanistan . . . and [to keep] the Congress, as well as the Secretaries of State and Defense, currently informed of reconstruction progress and weaknesses."[2] The SIGAR produces quarterly reports to Congress, which include audit results. Usually, these results are bleak: "SIGAR—through its audits, inspections, investigations, and observations on the ground in Afghanistan—has identified four major oversight concerns: lack of accountability, insufficient attention to capacity building and sustainment, inadequate integration of projects, and corruption."[3]

There are usually remedial measures taken in the form of corrective training for contracting officials. However, the issue is the system, not the lack of training.

Contracting officials are judged on the speed and quality at which they fulfill requirements for the warfighter. Counterintuitively, choosing the lowest bidder can sometimes promote corruption; there are reasons why some contractors keep winning contracts. Furthermore, while contracting officials have some face-to-face interaction with prime contractors, the subcontractors doing the work at the district level are usually unknown at both the tactical warfighter level and the contracting official level.

To fix the system, it is time to establish a unified contracting command under NATO that is transparent, accountable, and responsive to both tactical and governance requirements. A unified wartime contracting strategy should establish varying levels of importance between fulfilling tactical requirements and limiting negative effects on governance, reconstruction, and development. The upcoming Kandahar operation is primarily focused on governance, and therefore the contracting strategy should accurately reflect that. For example, if one contractor has historically been the best for building checkpoints or repairing craters at the lowest price, but he does so through corruption, should contracting officials choose him? That depends on whether senior decisionmakers think that enhancing governance comes from the checkpoint itself or from making the rich richer. **JFQ**

## NOTES

[1] Carl Forsberg, *Politics and Power in Kandahar,* Afghanistan Report 5 (Washington, DC: The Institute for the Study of War, April 2010), available at <www.understandingwar.org/files/Politics_and_Power_in_Kandahar.pdf>.

[2] Public Law 110–181, "The National Defense Authorization Act for Fiscal Year 2008," January 28, 2008.

[3] Special Inspector General for Afghanistan Reconstruction (SIGAR), *Quarterly Report to the United States Congress* (Washington, DC: Office of the SIGAR, October 30, 2009), available at <www.sigar.mil/pdf/quarterlyreports/Oct09/pdf/SIGAROct2009Web.pdf>.

Atlas V is launched with Advanced Extremely High Frequency satellite onboard

U.S. Air Force (Larry E. Reid, Jr.)

# Spacepower and Warfare

*By* **M.V. SMITH**

**Colonel M.V. Smith, USAF, is Director of the Air Force Space and Cyber Center at Air University. This article is an excerpt from Colonel Smith's chapter in the forthcoming NDU Press book *Toward a Theory of Space Power: Selected Essays*, which is the outcome of the Institute for National Strategic Studies Spacepower Theory Project.**

A discussion of the nexus of spacepower and warfare is controversial because space has yet to be overtly weaponized or generally recognized as an arena of open combat. Many, if not most, nations want to keep space a weapons-free peaceful sanctuary, particularly the suprastate actors. Just because all other media are weaponized and used as arenas of combat does *not* mean that space will automatically follow suit.[1] Perhaps this generation will figure out how to keep the beast of war in chains short enough to prevent it from going to space. But the next (and each succeeding) generation must also keep the chains short. Unfortunately, the constant march of technology is making space more important to states at the same time it is making it easier to build space weapons.

In anticipating the future of spacepower for theoretical discussion, we can do little more than extract a roadmap from the history of human activity and extrapolate forward. The preponderance of evidence suggests that space will be no different from air, land, and sea regarding warfare. In the words of Colin Gray:

*It is a rule in strategy, one derived empirically from the evidence of two and a half millennia, that anything of great strategic importance to one belligerent, for that reason has to be worth attacking by others. And the greater the importance, the greater has to be the incentive to damage, disable, capture, or destroy it. In the bluntest of statements: space warfare is a certainty in the future because the use of space in war has become vital. . . . Regardless of public sentimental or environmentally shaped attitudes towards space as the pristine final frontier, space warfare is coming.*[2]

The strategic value of space to states is not in question. Advanced spacefaring states are already reliant—and moving toward dependence—on space-derived services for activities across every sector of their societies. Spacepower is becoming critical to their styles of warfighting. Likewise, the injury that can

be caused to such states by menacing their space systems can be considerable. Given these incentives, the beast of war will either break its chains all at once or stretch them slowly over time.[3]

Like war itself, space warfare, the decision to build space weapons, and whether or not to weaponize space are all matters of policy, not theory.[4] It is the job of theory to anticipate such developments given the template that history suggests. Land, air-, and seapower lend imperfect analogies to spacepower, but they are applicable enough to see that spacepower may have its own grammar, but not its own logic.[5] The logic of statecraft and warfare laid out in Sun Tzu's *The Art of War* and in Carl von Clausewitz's *On War* applies to spacepower as well as any other element of military power. A student of spacepower must become thoroughly familiar with both of these works.[6] War is a political activity and therefore a human activity with a long history that serves as a guide path. Spacepower is already part of the warfighting mix in the political and strategic unity of war, and this trend will continue.[7] Some predict that spacepower will make the greatest contributions to combat effectiveness in wars of the 21st century.[8]

## War Extended to Space

War is an instrument of policy, and spacepower, as an element of the military instrument of power, is part of the policy mix that makes war, whatever form it may take.[9] Space generally has been treated as a sanctuary since the Eisenhower administration, and the use of space systems in warfare is limited to supporting terrestrial forces. This is not likely to change if the security concerns of states remain low. However, if states are confronted with intense security concerns, such as their survival, the weaponization of space and its use as an arena of conflict become far more likely.

Spacepower is a player at every point along the spectrum of conflict.[10] Covert operations often use space services with the same degree of reliance as the large joint military forces of advanced spacefaring states engaged in a conflict. In addition, space systems often support multiple military operations with varying intensities in different parts of the world simultaneously.

Spacefaring prowess is a common attribute of the dominant powers in the world today. Special attention must be paid to so-called rogue states that have access to space-related technology and may even be spacefaring but do not have the conventional forces to achieve their policy aims. Those aims tend to be very intense, and these players may seek space weapons as an asymmetric hedge against spacefaring adversaries who may try to coerce them.

*if states are confronted with intense security concerns, the weaponization of space and its use as an arena of conflict become far more likely*

The dominant military powers in the world, some of whom are potential adversaries, also tend to be the dominant spacefaring states. Because of the economic benefits and exponential enhancements that spacepower delivers to terrestrial warfighting, those states are under increasing pressure to defend their space systems and to counter those of their potential adversaries. This may lead to a space weapons race and an immediate escalation of hostilities to "wipe the skies" of enemy satellites should war break out between two or more dominant military space powers.[11]

When assessing the interplay between the spectrum of conflict and the spectrum of belligerents, it may be the case that war between two weak actors will not likely extend into space. However, if the power is perceived to be disparate, a weak actor is far more likely to use space weapons against a powerful state as an asymmetric defensive move.[12] A powerful state may counter the space systems in use by a weaker adversary, but it is likely to do so by placing diplomatic pressure on commercial vendors, or executing attacks on their ground stations, or launching highly selective covert attacks on the satellites they use by employing temporary and reversible means.

Should two dominant spacefaring powers go directly to war with each other with intense motives, both will find it critical to preserve their space systems and will consider it a dangerous liability to allow their enemy to exploit them. Given the ability of spacepower to cut the fog and friction of war while connecting military forces at the tactical, operational, and strategic levels, it is likely that space systems will be primary targets that will be negated in the opening moves of war. The fight for space is likely to be intense and brief. Temporary means of negation will probably switch to permanent methods of destruction to remove doubt in the minds of commanders.

## Offense and Defense

Sun Tzu pointed out, "Invincibility lies in the defense; the possibility of victory in the attack. One defends when his strength is inadequate; he attacks when it is abundant."[13] All warfare depends on interplay between the offense and the defense. They are "neither mutually exclusive nor clearly distinct . . . each includes elements of the other."[14] Defense generally implies a negative aim of protection and of preserving the status quo in the face of an attack. Conversely, offense generally pursues a positive aim by inflicting damage on the adversary to coerce him into accepting terms. However, consider that there are defensive aspects resident in every attack. Warriors of old carried their shields into battle when they attacked with their swords to protect them from the thrusts of the defenders. The offense is also resident in every defense. Remember that the Royal Air Force won the great defensive Battle of Britain by attacking the invading German bombers.

The general goal of offense is to inflict such damage on the adversary that they are *defensively culminated*, meaning they can no longer resist the attack and must either accept terms or be annihilated. Conversely, the goal of defense is to resist the attack and inflict such costs on the adversary that they are *offensively culminated*, meaning they can no longer attack and can only defend themselves. These concepts will come into play when we discuss space control and space denial.

It is often said that defense is the stronger form of warfare.[15] This is not true in space—today. Defending satellites and their data links is a difficult proposition at best. Satellites are delicate, fragile devices that can easily fall prey to any number of space weapons that currently exist, such as lasers, radio frequency jamming, brute force weapons, and surface-to-space missiles with kinetic kill vehicles—many of which are relatively small, mobile systems. While satellites in low Earth orbit are the most vulnerable to lasers and lofted kinetic kill vehicles, satellites all the way out in the geostationary belt and in highly elliptical orbits share a universal vulnerability to radio frequency jamming and electromagnetic brute force attacks. Satellites do not need to be physically destroyed to be rendered ineffective. Satellites are commanded

(as applicable) and provide their services to ground stations and users via the electromagnetic spectrum. Hence, there is a rule: no spectrum means no spacepower. The rapid proliferation of jammers and electronic intrusion devices around the world in recent years occurred upon recognition of this rule.

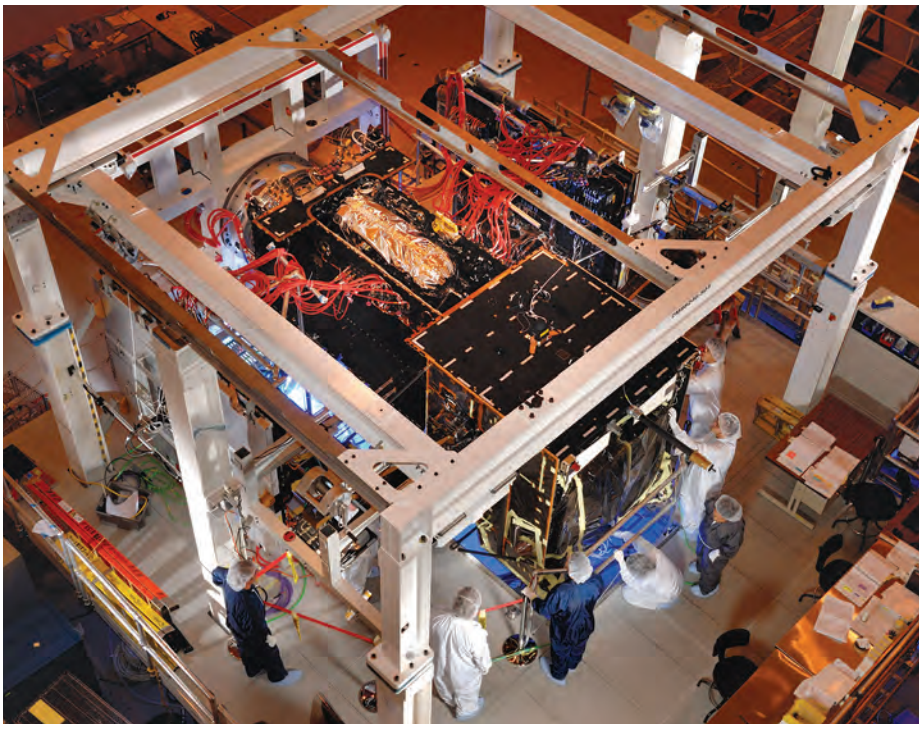
*today's space defense rests on the assurances in the Outer Space Treaty, which imperfectly implies that space is a peaceful sanctuary, although it only bans the basing of weapons of mass destruction in space*

Defenses to date are paltry at best. An adversary with robust space denial weapons may be able to negate all friendly space systems in a matter of hours; therefore, it is imperative for space powers to acquire the ability to find, fix, track, target, and destroy an adversary's space weapons very quickly. Such systems may reside on land, at sea, in the air, or in space. It will require close coordination with terrestrial forces to engage them against space weapons at the behest of the space commander.

In essence, today's space defense rests on the assurances in the Outer Space Treaty, which imperfectly implies that space is a peaceful sanctuary, although it only bans the basing of weapons of mass destruction in space. Does this mean all lesser threats are allowed? This is a hotly debated point. No one contests the language in article 51 of the United Nations charter that gives states the inherent right of self-defense. Presumably, this includes self-defense from space weapons and space-based weapons. It can be argued that space weapons are a matter of the inherent right of self-defense. The slope to space warfare is slippery indeed.

Although offense is the dominant form of war in space today, this will not always be the case. Defense is possible. Three principles will likely guide the development of future space defenses.

First, *if you can't see it, you can't hit it.* Satellites are already getting smaller—too small for most space surveillance networks to detect and track. This trend will likely continue not only as a matter of cost savings, but also as a matter of stealthy defense. Avoiding detection includes maneuvering satellites to undisclosed wartime orbits.



Lockheed Martin Space Systems

**Baseline integrated system testing of Space-based Infrared System geosynchronous orbit spacecraft**

Second, *all warfare is based on deception.*[16] Potential adversaries collect intelligence on each other's space systems and make their estimates based on their intelligence assessments. Action must be taken to deceive potential adversaries into underestimating the value of critical systems and overestimating the value of inconsequential systems. In addition, the use of wartime-only modes of operation, frequencies, and other unanticipated behaviors will further complicate an adversary's problems.

Third, *there is strength in numbers. The age of the capital satellites is over.* Employing only one or two large, very expensive satellites to fulfill a critical mission area, such as reconnaissance, is foolish. Future space systems must be large constellations of smaller, cheaper, and, in many cases, lower fidelity systems swarming in various orbits that exploit ground processing to derive high-fidelity solutions. In addition, swarms improve global access and presence.

The best defense for a space system in the 21st century may be the dual-use system that is owned, operated, and used by broad international partners. A hostile foe may be deterred from attacking a satellite if doing so comes with the likelihood of expanding the war against their cause. This is also dependent on the hostile foe's policy aim. If it is intense, such as national survival or radical ideology, they may attack anyway.

The term *attack* is practically synonymous with *offense*, but it must be understood in a much more nuanced way regarding spacepower than is generally ascribed among those who hype the threat of direct kinetic kill antisatellite weapons that may smash satellites to bits. It must be remembered that space systems are comprised of space, ground, and user segments integrated through data links. Any of these segments or links can be targeted by an attack to gain the desired effect. A specific target within a space system is selected and a weapon is chosen to attack that target in a certain way to achieve the desired *level of negation*. The first includes temporary and reversible effects such as deception, disruption, and denial. The second includes permanent physical effects such as degradation and destruction. They can be described this way:

- *Deception* employs manipulation, distortion, or falsification of information to induce adversaries to react in a manner contrary to their interests.
- *Disruption* is the temporary impairment of some or all of a space system's capability to produce effects, usually without physical damage.

Lockheed Martin

**Modernization of U.S. Air Force Integrated Space Command and Control program will result in "virtual command center"**

■ *Denial* is the temporary elimination of some or all of a space system's capability to produce effects, usually without physical damage.

■ *Degradation* is the permanent impairment of some or all of a space system's capability to produce effects, usually with physical damage.

■ *Destruction* is the permanent elimination of all of a space system's capabilities to produce effects, usually with physical damage (called *hard kill* or, without physical damage, *soft kill*).[17]

Ultimately, the level of negation is chosen to achieve the desired effect that serves the objectives given to space forces in support of the overall strategy and operational plans of the war. A very low-intensity war is likely to involve covert use of the temporary and reversible levels of negation. Conversely, more intense wars will probably tend toward the permanent levels.

There is a drawback to temporary levels of negation. It is exceptionally difficult to determine if the application of the weapon is achieving the desired effect. Permanent levels of negation may deliver more easily observable confirmation of effects. This is somewhat analogous to the problems of determining a tank kill in Operation *Desert Storm*. Some commanders considered a tank killed if its unit was attacked and the tank was no longer moving. Others did not agree with this. But all agreed that it was a kill if the tank had its turret blown off.

It must be kept in mind that a small number of powerful directed energy space weapons can quickly cause permanent levels of negation to dozens of satellites. On the other hand, it would take several dozen space weapons such as jammers that only cause temporary effects to negate the constellations of the larger spacefaring states. Since noise jammers are only effective when broadcasting, and broadcasting jammers are relatively easy to find and target, there are incentives to develop space weapons that cause permanent effects.

If history serves as a template for the future in space, then space will become a warfighting medium. It is already heavily militarized, with powerful spacefaring states using the medium to enable their surveillance and reconnaissance strike complexes in ways that accelerate the scale, timing, and tempo of combat operations exponentially beyond non-spacefaring actors' ability to cope. Weak actors are likely to employ space weapons in an attempt to counter the advantage space confers on powerful states. The most dangerous situation, however, will occur if two powerful spacefaring states go to war with each other. If the motives are intense, it is likely that they will be forced to counter each other's space systems in the very early stages. At present, there are inadequate defenses for space systems, but defense is possible. Space denial strategies of warfare are likely to evolve, wherein a belligerent merely attacks an adversary's space systems to inflict costs or to induce strategic paralysis on the enemy before offering terms. Finally, space is very much part of the military mix of all actors, state and nonstate, and it must be recognized that spacepower is not a replacement for terrestrial forces, but an additional set of tools that delivers unique capabilities. **JFQ**

## NOTES

[1] Karl Mueller, "Totem and Taboo," *Astropolitics* 1, no. 1 (September 2003), 26–28.

[2] Colin S. Gray, *Another Bloody Century: Future Warfare* (London: Phoenix, 2006), 307.

[3] It has been postulated that the weaponization of space will occur in one of two ways, based on either a single trigger event or a slippery slope. See Barry D. Watts, *The Military Uses of Space: A Diagnostic Assessment* (Washington, DC: Center for Strategic and Budgetary Assessments, February 2001), 98.

[4] Carl von Clausewitz, *On War*, ed. and trans. Michael Howard and Peter Paret (Princeton: Princeton University Press, 1989), 87. Clausewitz's famous dictum that "war, therefore, is an act of policy" serves as a central proposition for *On War*.

[5] Extrapolated from Clausewitz, 605.

[6] Sun Tzu, *The Art of War*, trans. Ralph D. Sawyer (Boulder, CO: Westview Press, 1994); Clausewitz, previously cited.

[7] Clausewitz, 605–607.

[8] Colin S. Gray, *Modern Strategy* (Oxford: Oxford University Press, 1999), 256–257.

[9] Clausewitz, 87.

[10] Brian E. Fredriksson, "Space Power in Joint Operations: Evolving Concepts," *Air and Space Power Journal* (Summer 2004), available at <www.airpower.maxwell.af.mil/airchronicles/apj/apj04/sum04/fredriksson.html>.

[11] The urgency felt by powerful spacefaring states to "wipe the skies" is the thesis of a book by William B. Scott et al., *Space Wars: The First Six Hours of World War III* (New York: Forge, 2007), 7–16.

[12] Ibid.

[13] Sun Tzu, *The Art of War*, trans. S.B. Griffith (New York: Oxford University Press, 1982), 85.

[14] John Schmitt, *Warfighting: The U.S. Marine Corps Book of Strategy* (New York: Currency-Doubleday, 1995), 30.

[15] Clausewitz, 84; Schmitt, 30.

[16] Sun Tzu, *The Art of War*, ed. James Clavell, trans. Lionel Giles (New York: Delacorte Press, 1983), 11.

[17] Air Force Doctrine Document 2–2, *Space Operations*, November 27, 2001, 13.

# Airpower, Spacepower, and Cyberpower

*By* BENJAMIN S. LAMBETH

Image of Baghdad showing smoke plumes from previous night's bombardment, acquired by IKONOS–2 satellite April 2003

NASA

When American airpower played a central role in driving Iraq's occupying forces from Kuwait in early 1991, many doubters tended to dismiss that remarkable performance as a one-of-a-kind force employment anomaly. It was, the doubters said, the clear and open desert environment, or the unusual vulnerability of Iraq's concentrated armored formations to precision air attacks, or any number of other unique geographic and operational circumstances that somehow made the Persian Gulf War an exception to the general rule that it takes "boots on the ground" in large numbers, and ultimately in head-to-head combat, to defeat well-endowed enemy forces in high-intensity warfare.

To many, that line of argument had a reasonable ring of plausibility when airpower's almost singular contribution to the defeat of Saddam Hussein's forces was an unprecedented historical achievement. During the 12 years that ensued in the wake of Operation *Desert Storm*, however, the world again saw American airpower prevail in broadly comparable fashion in four dissimilar subsequent cases, starting with the North Atlantic Treaty Organization's two air-centric contests over the Balkans in Operations *Deliberate Force* in 1995 and *Allied Force* in 1999, and followed soon thereafter by Operation *Enduring Freedom* against terrorist elements in Afghanistan in 2001–2002 and by the 3-week period of major combat in Operation *Iraqi Freedom* that ended Saddam's rule in 2003. Granted, in none of those five instances did the air weapon produce the ultimate outcome all by itself. However, one can argue that in each case, successful aerial combat and support operations were the pivotal enablers of all else that followed in producing the sought-after results at a relatively low cost in friendly and noncombatant enemy lives lost.

In light of those collective achievements, what was demonstrated by American air assets between 1991 and 2003 was arguably *not* a succession of anomalies, but rather the bow wave of a fundamentally new American approach to force employment in which the air weapon consistently turned in a radically improved level of performance compared to what it had previously delivered to joint force commanders. Indeed, that newly emergent pattern has now become so pronounced and persistent as to suggest that American airpower has finally reached the brink of maturity and become the tool of first resort by combatant commanders, at least with respect to defeating large enemy force concentrations in high-intensity warfare.

Yet in each of the five instances noted above, what figured so importantly in determining the course and outcome of events was not *airpower* narrowly defined, but rather operations conducted in, through, and from the Earth's atmosphere, backstopped and enabled, in some cases decisively, by the Nation's diverse additional assets in space and by operations conducted within cyberspace (that is, the electromagnetic spectrum).

Accordingly, any effort to understand the evolving essence of American *airpower* must take into account not only our aerial warfare assets, but also those vitally important space and cyberspace adjuncts that, taken together, have made possible the new American way of war. By the same token, any successful effort to build a theoretical framework for better charting the future direction and use of American air, space, and cyberspace

**Benjamin S. Lambeth is a Senior Research Associate at the RAND Corporation. This article is an excerpt from his chapter in the forthcoming NDU Press book *Toward a Theory of Space Power: Selected Essays*, which is the outcome of the Institute for National Strategic Studies Spacepower Theory Project.**

warfare capability must first take due measure of the Nation's current state of advancement in each domain. Toward that end, the discussion that follows offers a brief overview of where the United States stands today in each of the three operating mediums. It then considers some pertinent lessons from the airpower experience that bear on the development of spacepower and cyberpower theory, along with the sorts of cross-domain synergies that should be pursued in the many areas where the air, space, and cyberspace arenas overlap. Finally, it considers some essential steps that need to be taken toward that end before a holistic theory of warfare in all three domains, let alone any separate and distinct theory of spacepower, can realistically be developed.

## Recent Air Achievements

By any measure, the role of airpower in shaping the course and outcome of the 1991 Persian Gulf War reflected a major breakthrough in the effectiveness of the Nation's air arm after a promising start in World War II and more than 3 years of misuse in the *Rolling Thunder* bombing campaign against North Vietnam from 1965 to 1968. At bottom, the *Desert Storm* experience confirmed that since Vietnam, American airpower had undergone a nonlinear growth in its ability to contribute to the outcome of joint campaigns at the operational and strategic levels thanks to a convergence of low observability to enemy sensors in the F–117 stealth attack aircraft, the ability to attack fixed targets consistently with high accuracy from relatively safe standoff distances using precision-guided munitions, and the expanded battlespace awareness that had been made possible by recent developments in command, control, communications, and computers, and intelligence, surveillance, and reconnaissance (ISR).[1]

As a result of those developments, American airpower had finally acquired the capabilities needed to fulfill the longstanding promise of its pioneers of being able to set the conditions for winning in joint warfare—yet *not* through the classic imposition of brute force, as had been the case throughout most of airpower's history, but rather through the *functional* effects now achievable by targeting an enemy's vulnerabilities and taking away his capacity for organized action. The combination of real-time surveillance and precision target–attack capability that was exercised to such telling effect by airpower against Iraq's fielded ground forces in particular heralded a new relationship between air- and surface-delivered firepower, in which friendly ground forces did the fixing and friendly airpower, now the predominant maneuver element, did the killing of enemy troops rather than the other way around.

During the years immediately after the 1991 Gulf War, further qualitative improvements rendered the Nation's air weapon even more capable. For one thing, almost every American combat aircraft now possessed the ability to deliver precision-guided weapons. For another, the advent of stealth, as was first demonstrated on a significant scale by the F–117 during the Gulf War, was further advanced by the subsequent deployment of the Air Force's second-generation B–2 stealth bomber that entered operational service in 1993. Finally, the advent of the satellite-aided GBU–31 Joint Direct Attack Munition (JDAM) gave joint force commanders the ability to conduct accurate target attacks with near impunity, around the clock and in any weather, against an opponent's core concentrations of power, whether deployed forces or infrastructure assets.

In the three subsequent major wars that saw American combat involvement (Operations *Allied Force*, *Enduring Freedom*, and the major combat phase of *Iraqi Freedom*), the dominant features of allied air operations were persistence of pressure on the enemy and rapidity of execution, thanks to the improved data fusion that had been enabled by linking the inputs of various air- and space-based sensor platforms around the clock. Greater communications connectivity and substantially increased available bandwidth enabled constant surveillance of enemy activity and contributed significantly to shortening the sensor-to-shooter data cycle time. Throughout each campaign, persistent ISR and growing use of precision munitions gave the United States the ability to deny the enemy a sanctuary. More important, they reflected an ongoing paradigm shift in American combat style that promised at the time to be of greater moment than was the introduction of the tank at the beginning of the 20th century.[2]

Since then, to be sure, mastering the sorts of lower intensity counterinsurgency challenges that have dominated more recent headlines has highlighted modern airpower's limitations as well as strengths. Although today's instruments of air warfare have thoroughly transformed the Nation's ability to excel in conventional warfare, those instruments and their associated concepts of operations have yet to have shown comparable potential in irregular warfare, since irregular opponents, given their composition and tactics, are less vulnerable than conventional opponents to airpower as currently configured and employed. Conversely, however, the recent rise of irregular warfare as our preeminent security concern today has been substantially a result of airpower's proven effectiveness in conventional warfare, a fact that attests to modern airpower's unprecedented leverage at the same time that it illuminates the continuing challenges that airpower faces.

*friendly ground forces did the fixing and friendly airpower, now the predominant maneuver element, did the killing of enemy troops rather than the other way around*

## Space Contributions

The medium of space and its associated mission areas have also figured prominently in the steady maturation of American airpower since Vietnam. If there is a single fundamental and distinctive advantage that mature airpower has conferred upon theater commanders in recent years, it has been an increasingly pronounced degree of freedom *from* attack and freedom *to* attack for all force elements, both in the air and on the ground, in major combat operations. The contributions of the Nation's space systems with respect to both ISR and precision attack have played a central role in making those two force-employment virtues possible. Although still in its adolescence compared to our more developed air warfare posture, the Nation's ever-improving space capability has nonetheless become the enabler that has made possible the new strategy of precision engagement.

Despite that and other contributions from the multitude of military assets now on orbit, however, the Nation's air warfare repertoire still has a way to go before its post-Vietnam maturation can be considered

U.S. Army (Aaron D. Allmon II)

Airborne weapons officers monitor consoles aboard E–8C JSTARS aircraft

complete. Advances in space-based capabilities on the ISR front lie at the heart of the full and final transformation of American airpower. It is now almost a cliche to say that airpower can kill essentially anything it can see, identify, and engage. To note one of the few persistent and unrectified shortfalls in airpower's leverage, however, it can kill *only* what it can see, identify, and engage. Airpower and actionable real-time target intelligence are thus opposite sides of the same coin. If the latter is unavailing in circumstances in which having it is essential for mission success, the former will likely be unavailing also. For that reason, accurate, timely, and comprehensive information about an enemy and his military assets is not only a crucial enabler for airpower to produce pivotal results in joint warfare, but it is also an indispensable precondition for ensuring such results. In this regard, it will be in substantial measure through near-term improvements in space-based capabilities that the Air Force's long-sought ability to find, fix, track, target, engage, and assess any target of interest on the face of the Earth will become an established reality rather than merely a catchy vision statement with great promise.[3]

The spectrum of military space missions starts with *space support*, which essentially entails the launching of satellites and the day-to-day management of on-orbit assets that underpin all military space operations. It next includes *force enhancement*, a broader category of operations involving all space-based activities aimed at increasing the effectiveness of terrestrial military operations. This second mission area embraces the range of space-related enabling services that the Nation's various on-orbit assets now provide to U.S. joint force commanders worldwide. Activities in this second area include missile attack warning and characterization, navigation, weather forecasting, communication, ISR, and around-the-clock Global Positioning System (GPS) operations. A particularly notable aspect of space force enhancement in recent years has been the growing use of space-based systems for directly enabling, rather than merely enhancing, terrestrial military operations, as attested by the increasing reliance by all four Services on GPS signals for accurate, all-weather delivery of satellite-aided JDAMs.

To date, the American defense establishment has largely limited its space operations to these two rather basic and purely enabling mission areas. Once the third mission area, *space control*, develops into a routine operational practice, it will involve the direct imposition of kinetic and nonkinetic effects both within and through space. Conceptually, space control is analogous to the familiar notions of sea and air control, both of which likewise involve ensuring friendly access and denying enemy access to those mediums. Viewed purely from a tactical and technical perspective, there is no difference in principle between defensive and offensive space control operations and similar operations conducted in any other medium of warfare. It is simply a matter of desirability, technical feasibility, and cost-effectiveness for the payoff being sought.

Unlike the related cases of sea and air control, however, serious investment in space control has been slow to take place in the United States, in part due to a persistent lack of governmental and public consensus as to whether actual combat, as opposed to merely passive surveillance and other terrestrial enabling functions, should be allowed to migrate into space and thus violate its presumed status as a weapons-free sanctuary. The delay also has had to do with the fact that the United States has not, at least until recently, faced direct threats to its on-orbit assets that have needed to be met by determined investment in active space control measures, all the more so in light of more immediate and pressing research and development and systems procurement priorities. For both reasons, the space control mission area remains almost completely undeveloped. About all the United States can do today to deny enemy access to the data stream from space is through electronic jamming or by physically destroying satellite uplinks and downlinks on the ground.

Finally, the *force application* mission, which thus far remains completely undeveloped due to both widespread international disapprobation and a general absence of political and popular domestic support, will eventually entail the direct defensive and offensive imposition of kinetic and non kinetic measures from space in pursuit of joint terrestrial combat objectives. In its ultimate hardware manifestations, it could include the development, deployment, and use of space-

based nonnuclear, hyperkinetic weapons against such terrestrial aim points as fixed high-value targets (hardened bunkers, munitions storage depots, underground command posts, and other heavily defended objectives), as well as against surface naval vessels, armored vehicles, and such other targets of interest as enemy leadership. How many years or decades into the future it may be before such capabilities are developed and fielded by the United States has been a topic of debate among military space professionals for many years. For the time being, it seems safe to conclude that any such developments will be heavily threat-determined and will not occur, if only from a cost-effectiveness viewpoint, as long as effective air-breathing or other terrestrial alternatives for performing the same missions are available.

Fortunately, as the Nation's defense community looks toward further developing these mission areas in an orderly sequence, it can claim the benefit of a substantial foundation on which to build. In February 2000, the Defense Science Board (DSB) concluded that the United States enjoyed undisputed space dominance, thanks in large part to what the Air Force had done in the space support and force enhancement mission areas over the preceding four decades to build a thriving military space infrastructure. Air Force contributions expressly cited by the DSB included a robust space launch and support infrastructure, effective indications and warning and attack-assessment capability, unique ground-based space surveillance capability, global near-real-time surveillance of denied areas, ability to disseminate the products of that capability rapidly, and strong command, control, and communications infrastructure for exploiting space systems.[4]

In looking to build on these existing capabilities with the goal of extracting greater leverage from the military promise of space, the Air Force now faces an urgent need to prioritize its investment alternatives in an orderly and manageable way. It cannot pursue every appealing investment opportunity concurrently, since some capability upgrade needs are more pressing than others. These appropriately rank-ordered priorities, moreover, must be embraced squarely and unsentimentally by the Nation's leadership. If the experience with the successful transformation of American *airpower* since Vietnam is ever to become a prologue to the next steps in the expansion of the Nation's military space repertoire, then it follows that the Air Force, as the lead Service in space operations, will need to get its hierarchy of operational requirements in space right if near-Earth space is to be exploited for the greatest gains per cost in the service of theater commanders. Because an early working template for an overarching theory of spacepower might help impose a rational discipline on the determination of that hierarchy, perhaps the pursuit of such a focusing device should be undertaken as one of the first building blocks for such a theory.

Furthermore, a case can reasonably be made that the Nation's next moves with respect to military space exploitation should first seek to ensure the further integration of space with the needs of terrestrial warfighters, however much that might appear, at least for the near term, to shortchange the interests of those who are ready *now* to make space the fourth medium of warfare. More to the point, one can reasonably suggest that if the Nation's leadership deems a current space-based capability to be particularly important to the effective conduct of joint warfare and that it is either facing block obsolescence or otherwise is at the threshold of failing, then it should be replaced as a first order of business before any other major space investment programs are pursued. Once those most pressing recapitalization needs are attended to, then all else by way of investment opportunities can be approached in appropriate sequence, including such space-based multispectral ISR assets as electro-optical, infrared, and signals intelligence satellites, followed by space-based radar once the requisite technology has proven itself ready for major resources to be committed to it.

Moreover, in considering an orderly transfer of such ISR functions from the atmosphere to space, planners should exercise special caution not to try to change too much too quickly. For example, such legacy air-breathing systems as the E–3 Airborne Warning and Control System (AWACS) and E–8 Joint Surveillance Target Attack Radar System (JSTARS), which have been acquired through billions of dollars of investment, cannot be summarily written off with substantial service life remaining, however well intended the various arguments for mission migration to space may be. Thus, it may make greater sense to think of space not as a venue within which to replace existing surveillance functions wholesale, but rather as a medium offering the potential for expanding the Nation's existing ISR capability by more fully exploiting both the air *and* space environments. It also may help to think in terms of windows of time in which to commence the migration of ISR missions to space. A challenge that the Air Force faces now in this respect is to determine how to divest itself of existing legacy programs in a measured way so as to generate the funds needed for taking on tomorrow's challenges one manageable step at a time. That will require careful tradeoff assessments to determine the most appropriate technology and medium—air or space—toward which its resources should be vectored for any mission at any given time.

*the Air Force will need to get its hierarchy of operational requirements in space right if near-Earth space is to be exploited for the greatest gains per cost*

Finally, it will be essential that the survivability of any new ISR assets migrated to space be assured by appropriate protective measures developed and put into place first. American investment in appropriate first-generation space control measures has become increasingly essential in order for the Nation to remain secure in the space enabling game. Having been active in space operations for more than four decades, the United States is more heavily invested in space and more dependent on its on-orbit assets than ever before, and both real and potential adversaries are closing in on the ability to threaten our space-based assets by means ranging from harassment to neutralization to outright destruction, as attested by China's demonstration in January 2007 of a direct-ascent antisatellite kinetic kill capability against one of its own obsolete weather satellites 500 miles above the Earth's surface.[5] As the Nation places more satellites on orbit and comes to rely more on them for military applications, it is only a matter of time until our enemies become tempted to challenge our freedom of operations in space by attempting to undermine them.

In light of that fact, it would make no sense to migrate the JSTARS and AWACS

functions to space should the resultant on-orbit assets prove to be any less survivable than JSTARS and AWACS are today. It follows that getting more serious about space control is not an issue apart from force-enhancement migration, but rather represents a sine qua non for such migration. Otherwise, in transferring our asymmetric technological advantages to space, we will also run the risk of burdening ourselves with new asymmetric vulnerabilities.

## Exploiting Cyberspace

If the case for proceeding with timely initiatives to ensure the continued enabling functions of the Nation's space-based assets sounds reasonable enough in principle, then the argument for pursuing similar measures by way of vouchsafing our continued freedom of movement in cyberspace can be said to be downright compelling. The latter arena, far more than today's military space environment, is one in which the Nation faces clear and present threats that could be completely debilitating when it comes to conducting effective military operations. Not only that, opponents who would exploit opportunities in cyberspace with hostile intent have every possibility for adversely affecting the very livelihood of the Nation, since that arena has increasingly become not just the global connective tissue, but also the Nation's central nervous system and center of gravity.

Just a few generations ago, any American loss of unimpeded access to cyberspace would have been mainly an inconvenience. Today, however, given the Nation's ever-expanding dependence on that medium, the isolation, corruption, or elimination of electrical power supply, financial transactions, key communications links, and other essential Web-based functions could bring life as we know it to a halt. Furthermore, given the unprecedented reliance of the United States today on computers and the Internet, cyberspace has arguably become the Nation's center of gravity not just for military operations, but for *all* aspects of national activity, to include economic, financial, diplomatic, and other transactions. Our heightened vulnerability in this arena stems from the fact that we have moved beyond the era of physical information and financial exchanges through paper and hard currency and rely instead on the movement of digital representations of information and wealth. By one informed account, more than 90 percent of American business in all sectors, to say nothing of key institutions of governance and national defense, connects and conducts essential communications within the cyberspace arena.[6] Accordingly, that arena has become an American Achilles' heel to a greater extent than for any of our current opponents.

The term *cyberspace* derives from the Greek word *kubernetes*, or "steersman." Reduced to basics, it is the proverbial ether within and through which electromagnetic radiation is propagated in connection with the operation and control of mechanical and electronic transmission systems. Properly understood, cyberspace is not a "mission," but rather an operating domain just like the atmosphere and space, and it embraces all systems that incorporate software as a key element. It is a medium, moreover, in which information can be created and acted on at any time, anywhere, and by essentially anyone. It is qualitatively different from the land, sea, air, and space domains, yet it both overlaps and continuously operates within all four. It also is the only domain in which all instruments of national power (diplomatic, informational, military, and economic) can be concurrently exercised through the manipulation of data and gateways. Cyberspace can be thought of as a "digital commons" analogous to the more familiar maritime, aerial, and exoatmospheric commons. Moreover, just like the other three commons, it is one in which our continued uninhibited access can never be taken for granted as a natural and assured right. Yet uniquely among the other three, it is a domain in which the classic constraints of distance, space, time, and investment are reduced, in some cases dramatically, both for ourselves and for potential enemies.

There is nothing new in principle about cyberspace as a military operating domain. On the contrary, it has existed for as long as radio frequency emanations have been a routine part of military operations. As far back as the late 1970s, the commander in chief of the Soviet navy, Admiral Sergei Gorshkov, declared famously that "the next war will be won by the country that is able to exploit the electromagnetic spectrum to the fullest."[7] Furthermore, the Soviets for decades expounded repeatedly, and with considerable sophistication and seriousness, on a mission area that they referred to as *REB* (for *radioelektronaya bor'ba*, or radio-electronic combat). However, only more recently has it been explicitly recognized as an operating arena on a par with the atmosphere and space and begun to be systematically explored as a medium of combat in and of itself.

At present, theorizing about airpower and its uses and limitations has the most deeply rooted tradition in the United States, with conceptualizing about military space occupying second place in that regard. In contrast, focused thinking about operations in cyberspace remains in its infancy. Yet cyberspace-related threats to American interests are currently at hand to a degree that potentially catastrophic air and space threats are not—at least yet. Accordingly, the U.S. defense establishment should have every incentive to get serious about this domain now, when new terrorist, fourth-generation warfare, and information operations challengers have increasingly moved to the forefront alongside traditional peer-adversary threats.[8]

In light of that emergent reality, it is essential to include cyberspace in any consideration of air and space capabilities. Like the air and space domains, cyberspace is part and parcel of the third dimension (the first two being the land and maritime environments). Also like those other two domains, it is a setting in which organized attacks on critical infrastructure and other targets of interest can be conducted from a distance, on a wide variety of "fronts," and on a global scale—except, in this case, at the speed of light. Moreover, it is the principal domain in which the Nation's air services exercise their command, control, communications, and ISR capabilities that enable global mobility and rapid long-range strike.

In thinking about cyberspace as a military operating arena, a number of the medium's distinguishing characteristics are worth noting. First and foremost, control of cyberspace is a sine qua non for operating effectively in the other two domains. Were unimpeded access to the electromagnetic spectrum denied to us through hostile actions, satellite-aided munitions would become useless, command and control mechanisms would be disrupted, and the ensuing effects could be paralyzing. Accordingly, cyberspace has become an emergent theater of operations that will almost surely be contested in any future fight. Successful exploitation of this domain through network warfare operations can allow an opponent to dominate or hold at risk any or all of the global commons. For that reason, not only American superiority but also American dominance must be assured.

B–2 Spirit stealth bomber lands at Nellis Air Force Base, Nevada, after completing mission during exercise Red Flag

U.S. Air Force (Thomas P. Dougherty)

One reason for the imminent and broad-based nature of the cyberspace challenge is the low buy-in cost compared to the vastly more complex and expensive appurtenances of air and space warfare, along with the growing ability of present and prospective Lilliputian adversaries to generate what one expert called "catastrophic cascading effects" through asymmetric operations against the American Gulliver.[9] Because the price of entry is fairly minimal compared to the massive investments that would be required for any competitor to prevail in the air and space domains, the cyberspace warfare arena naturally favors the offense. It does so, moreover, not only for us, but also for any opponents who might use the medium for conducting organized attacks on critical nodes of the Nation's infrastructure. Such attacks can be conducted both instantaneously and from a safe haven anywhere in the world, with every possibility of achieving high impact and a low likelihood of attribution and, accordingly, of timely and effective U.S. retribution.

Indeed, America's vulnerabilities in cyberspace are open to the entire world and are accessible to anyone with the wherewithal and determination to exploit them. Without appropriate defensive firewalls and countermeasures in place, anything we might do to exploit cyberspace can be done to us as well, and relatively inexpensively. Worse yet, threat trends and possibilities in the cyberspace domain put in immediate jeopardy much, if not all, of what the Nation has accomplished in the other two domains in recent decades. Our continued prevalence in cyberspace can help ensure our prevalence in combat operations both within and beyond the atmosphere, which, in turn, will enable our prevalence in overall joint and combined battlespace. On the other side of the coin, any loss of cyberspace dominance on our part can negate our most cherished gains in air and space in virtually an instant. Technologies that can enable offensive cyberspace operations, moreover, are evolving not only within the most well-endowed military establishments around the world, but even more in the various innovative activities now under way in other government, private sector, and academic settings. The United States commands no natural advantage in this domain, and our leaders cannot assume that the next breakthrough will always be ours. All of this has rendered offensive cyberspace operations an attractive asymmetric option not only for mainstream opponents and other potential exploiters of the medium in ways inimical to the Nation's interests, but also for state and nonstate rogue actors with sufficient resources to cause us real harm.

Moreover, unlike the air and space environments, cyberspace is the *only* military operating area in which the United States already has peer competitors in place and hard at work. As for specific challengers, U.S. officials have recently suggested that the most sophisticated threat may come from China, which unquestionably is already a peer competitor with ample financial resources and technological expertise. There is more than tangential evidence to suggest that cyberwar specialists in China's People's Liberation Army have already focused hostile efforts against nonsecure U.S. transmissions.[10] Such evidence bears strong witness to the fact that state-sponsored cyberspace intrusion is now an established fact and that accurate and timely attack characterization has come to present a major challenge.

In light of its relative newness as a recognized and well-understood medium of combat, detailed and validated concepts of operations for offensive and defensive counter–cyber warfare and cyberspace interdiction have most likely yet to be worked out and formally incorporated into the Nation's combat repertoire. Interestingly, some of the most promising initial tactical insights toward that end may come from accessible sources in the nonmilitary domain, including from the business world, the intelligence world, the high-end amateur hacker world, and even perhaps segments of the underworld that have already pioneered the malicious exploitation of cyberspace. Ultimately, such efforts can help inform the development of a full-fledged theory of cyberspace power, which, at bottom, "is about dominating the electromagnetic spectrum—from wired and unwired networks to radio waves, microwaves, infrared, x-rays, and directed energy."[11]

With a full-court press of creative thought toward the development of new capabilities, the possibility of what a future cyberspace weapons array might include is almost limitless. Cyber weapons can be both surgical and mass-based in their intended effects,

ranging from what one Air Force cyber warrior recently portrayed as "the ultimate precision weapon—the electron," all the way to measures aimed at causing mass disruption and full system breakdowns by means of both enabling and direct attacks.[12] The first and most important step toward dealing effectively with the cyberspace warfare challenge in both threat categories will be erecting impenetrable firewalls for ourselves and taking down those of the enemy. Of course, with respect to plausible techniques and procedures for tomorrow's cyberspace world, it will be essential never to lose sight of the timeless rule among airmen that a tactic tried twice is no longer a tactic but a procedure.

*cyberspace warfare professionals will need to learn that any "cyberspace culture" must not be isolated from mainstream combat forces in all Services*

As the newly emerging cyberspace warfare community increasingly sets its sights on such goals, it would do well to consider taking a page from the recent experience of the military space community in charting next steps by way of organizational and implementation measures. For example, just as the military space community eventually emulated to good effect many conventions of the air warfare community, so might the cyberspace community usefully study the proven best practices of the space community in gaining increased relevance in the joint warfare world. Some possible first steps toward that end might include a systematic stocktaking of the Nation's cyberspace warfare posture with a view toward identifying gaps, shortfalls, and redundancies in existing offensive and defensive capabilities.

Similarly, those now tasked with developing and validating cyberspace concepts of operations might find great value in reflecting on the many parallels between space and cyberspace as domains of offensive and defensive activity. For example, both domains, at least today, are principally about collecting and transmitting information. Both play pivotal roles in enabling and facilitating lethal combat operations by other force elements. Both, again at least today, have more to do with the pursuit of functional effects than with the physical destruction of enemy equities, even though both can materially aid in the accomplishment of the latter. Moreover, in both domains, operations are conducted remotely by warfighters sitting before consoles and keyboards, not only outside the medium itself, but also in almost every case out of harm's way. Both domains are global rather than regional in their breadth of coverage and operational impact. And both domains overlap—for example, the jamming of a GPS signal to a satellite-aided munition guiding to a target is both a counterspace and a cyberwar operation insofar as the desired effect is sought simultaneously in both combat arenas.[13] To that extent, it seems reasonable to suggest that at least some tactics, techniques, procedures, and rules of thumb that have been found useful by military space professionals might also offer promising points of departure from which to explore comparable ways of exploiting the cyberspace medium.

Finally, as cyberspace professionals become more conversant with the operational imperatives of joint warfighting, they also will have a collective obligation to rise above the fragmented subcultures that unfortunately still persist within their *own* community and become a more coherent and interconnected center of cyberspace excellence able to speak credibly about what the exploitation of that medium brings to joint force employment. Moreover, cyberspace warfare professionals will need to learn and accept as gospel that any "cyberspace culture" that may ultimately emerge from such efforts must not be isolated from mainstream combat forces in all Services, as the Air Force's space sector was when it was in the clutches of the systems and acquisition communities, but instead must be rooted from the start in an unerring focus on the art and conduct of war.

## Toward Synthesis

As long as military space activity remains limited to enabling rather than actually conducting combat operations, as will continue to be the case for at least the near-term future, it will arguably remain premature even to *think* of the notion of space "power," strictly speaking, let alone suggest that the time has come to begin crafting a self-standing theory of spacepower comparable in ambitiousness and scope to the competing (and still-evolving) theories of land, sea-, and airpower that were developed over the course of the 20th century. Only when desired operational effects can be achieved by means of imposition options exercised directly through and from space to space-based, air-breathing, and terrestrial targets of interest (or, more to the point, when we can directly inflict harm on our adversaries from space) will it become defensible to entertain thoughts about space "power" as a fact of life rather than as merely a prospective and desirable goal.

To be sure, it scarcely follows from this observation that today's space professionals have no choice but to wait patiently for the day when they become force appliers on a par with their air, land, and maritime power contemporaries before they can legitimately claim that they are true warfighters. On the contrary, the Nation's space capabilities have long since matured to a point where they have become just as important a contributor to the overall *national* power equation as has what one might call mobility power, information power, and all other such adjuncts of the Nation's military strength that are indispensable to joint force commanders for achieving desired effects at all levels of warfare. To that extent, insisting that it remains premature to speak of spacepower solely because our space assets cannot yet deliver such combat effects directly may, in the end, be little more than an exercise in word play when one considers what space already has done toward transforming the Nation's airpower into something vastly more capable than it ever was before U.S. on-orbit equities had attained their current breadth of enabling potential.

Until the day comes when military space activity is more than "merely" about enabling terrestrial combat operations, however, a more useful exercise in theory-building in the service of combat operators at all levels might be to move beyond the *air*-power theorizing that has taken place to date in pursuit of something akin to a working "unified field theory" that explicates the connections, interactions, and overlaps among the air, space, and cyberspace domains in quest of synergies between and among them in the interest of achieving a joint force commander's objectives more efficiently and effectively. A major pitfall to be avoided in this regard is the pursuit of separate theory sets for each medium. To borrow from Clausewitz on this point, space, like the Earth's atmosphere and electromagnetic spectrum, may have its own grammar, but it does not have its own logic. Each of the three environments explored in the preceding

pages has distinctive physical features and operating rules that demand respect. By one characterization in this regard, "air permits freedom of movement not possible on land or sea.... Space yields an overarching capability to view globally and attack with precision from the orbital perspective. Cyberspace provides the capability to conduct combat on a global scale simultaneously on a virtually infinite number of 'fronts.'"[14] Yet while the air, space, and cyberspace mediums are all separate and unique physical environments, taken together, they present a common warfighting challenge in that operations in each are mutually supportive of those in the other two. For example, the pursuit of air supremacy does not simply entail combat operations in the atmosphere, but also hinges critically on ISR functions and on GPS targeting from both air-breathing and space-based platforms that transmit through cyberspace.

In light of the foregoing, the most immediate task for those seeking to build a better theory for leveraging capabilities in the third dimension may be to develop a point of departure for thinking systematically and holistically about synergies and best uses of the Nation's capabilities and prospects in all three domains, since all are key to the Nation's transforming joint strike warfare repertoire. Furthermore, it would be helpful to have a seamless body of applied and actionable theory that encompasses all three domains and that focuses more on functions and effects than on the physical locations of the instruments of power, with a view toward rank-ordering the many priorities in each and across all three, with the goal of charting a course for achieving cross-domain dominance. Another useful step toward managing the existing seams between and among the air, space, and cyberspace communities within the American defense establishment would be a perspective focused on *operational integration* accompanied by *organizational differentiation*. Through such a bifurcated approach, each medium can be harnessed to serve the needs of all components in the joint arena while, at the same time, being treated rightly as its own domain when it comes to program and infrastructure management, funding, cadre building, and career development.[15] Such organizational differentiation will be essential for the orderly growth of core competencies, discrete career fields, and mature professionalism in each medium. However, operational integration should be the abiding concern and goal for all three mediums, since it is only from synergies among the three that each can work to its best and highest use.

This is *not* a call for the Air Force, as the Nation's main repository of air, space, and cyberspace warfare capabilities today, to make the same mistake in a new guise that it made in 1959 when it conjured up the false artifice of "aerospace" to suggest that the air and space mediums were somehow undifferentiated just because they happened to be coextensive. Nothing could be further from the truth. It is, rather, to spotlight the unifying purpose of operations in all three mediums working in harmony, namely, to deliver desired combat effects in, through, and from the third dimension as quickly as possible and at the least possible cost in friendly lives lost and unintended damage incurred. Only after that crucial transitional stage of conceptualization has passed and when military space operations have come into their own as an independent producer, rather than just an enabler, of combat effects will it be possible to start giving serious thought to coming to grips with the prerequisites for a self-standing theory of spacepower. **JFQ**

## NOTES

[1] For an overview of the Air Force's pivotal contribution to this transformation, see Benjamin S. Lambeth, "The Air Force Renaissance," in *The Air Force*, ed. James P. McCarthy and Drue L. DeBerry (Andrews Air Force Base, MD: The Air Force Historical Foundation, 2002), 190–217. A fuller assessment of post-Vietnam developments in fixed-wing air warfare capability in all of the Services may be found in Benjamin S. Lambeth, *The Transformation of American Airpower* (Ithaca, NY: Cornell University Press, 2000).

[2] These major air operations are examined in detail in Benjamin S. Lambeth, *NATO's Air War for Kosovo: A Strategic and Operational Assessment* (Santa Monica, CA: RAND Corporation, 2001); *Airpower Against Terror: America's Conduct of Operation* Enduring Freedom (Santa Monica, CA: RAND Corporation, 2005); and *The Unseen War: Airpower in the Major Combat Phase of Operation Iraqi Freedom* (Santa Monica, CA: RAND Corporation, forthcoming).

[3] Of course, space plays a larger role in the "fixing" of targets than just providing space-based ISR. Space-based communications and the Global Positioning System are both essential enablers of unmanned aerial vehicle operations, which are also a critical contributor to the "find, fix, track, target, engage, assess" equation.

[4] Cited in E.C. Aldridge, Jr., "Thoughts on the Management of National Security Space Activities of the Department of Defense," unpublished paper, July 6, 2000, 3.

[5] For the essential known details of the test, see Craig Covault, "Space Control: Chinese Antisatellite Weapon Test Will Intensify Funding and Global Policy Debate on the Military Uses of Space," *Aviation Week and Space Technology*, January 22, 2007, 24–25.

[6] General James Cartwright, USMC, Commander, U.S. Strategic Command, remarks at the Air Force Association's Warfare Symposium, Orlando, Florida, February 8, 2007.

[7] Sergei G. Gorshkov, *The Sea Power of the State* (Annapolis, MD: Naval Institute Press, 1979).

[8] Among the classic articles in the airpower theory literature are Edward Warner, "Douhet, Mitchell, Seversky: Theories of Air Warfare," in *Makers of Modern Strategy*, ed. Edward Mead Earle (Princeton: Princeton University Press, 1943), and David MacIsaac, "Voices from the Central Blue: The Airpower Theorists," in *Makers of Modern Strategy: From Machiavelli to the Nuclear Age*, ed. Peter Paret (Princeton: Princeton University Press, 1986). See also the collection of essays in Phillip S. Meilinger, ed., *The Paths of Heaven: The Evolution of Airpower Theory* (Maxwell Air Force Base, AL: Air University Press, 1997). One of the better synopses of spacepower thinking to date is presented in Peter L. Hays et al., *Spacepower for a New Millennium: Space and U.S. National Security* (New York: McGraw Hill, 2000). For the most serious and thorough treatise thus far to have expounded about the cyberspace domain, its boundaries, and its potential, see George J. Rattray, *Strategic Warfare in Cyberspace* (Cambridge: MIT Press, 2001). The book is the doctoral dissertation of an Air Force lieutenant colonel who commanded the 23d Information Operations Squadron in the Air Force Information Warfare Center.

[9] Colonel Glenn Zimmerman, USAF, "The United States Air Force and Cyberspace: Ultimate Warfighting Domain and the USAF's Destiny," unpublished paper.

[10] See Carlo Munoz, "Air Force Official Sees China as Biggest U.S. Threat in Cyberspace," *Inside the Air Force*, November 17, 2006.

[11] "Ten Propositions Regarding Cyber Power," Air Force Cyberspace Task Force, unpublished briefing chart, no date.

[12] Zimmerman.

[13] I am grateful to my RAND colleague Karl Mueller for suggesting these and other thought-provoking parallels between the two media.

[14] Zimmerman.

[15] For an earlier development of this line of argument with respect to the Air Force's space community, see Benjamin S. Lambeth, *Mastering the Ultimate High Ground: Next Steps in the Military Uses of Space* (Santa Monica, CA: RAND Corporation, 2003).


U.S. Air Force (Duncan Wood)

**Commander, Air Force Space Command, meets with Government officials to discuss GPS needs of civil and military communities**

# An Allard Commission Postmortem and the Need for a National Space Council

*By* JOAN JOHNSON-FREESE

The unclassified Department of Defense (DOD) space budget is over double that of the combined expenditures of all other countries with military space programs, and in excess of $20 billion annually. Of the over 850 satellites in orbit in 2010, more than half belong to the United States. While a significant portion of those satellites is not owned by the military, DOD uses, even relies on, commercial satellites for military use. What conclusions can be drawn from these facts and statistics? It is clear that the United States has more space capabilities than any other country, but are those capabilities, regardless of their ownership, well integrated into and within the military?

That question can be answered in one of two ways: either from the perspective of the warfighter, or as an organizational issue. The good news is that from the perspective of the warfighter, space has come a long way toward becoming a well-integrated tool. Though the first Gulf War is sometimes referred to as the "first space war" due to the high utilization of space assets, Service integration, let alone the integration of space capabilities into Service operations, was a significant challenge. The Navy, for example, had to fly the daily air tasking orders out to the aircraft carriers by helicopter, a system known in Navy vernacular as Pigeon Post, because its communications systems were not compatible with the lengthy Riyadh-generated document.[1] In terms of space, an after-action assessment report stated: "The ground forces who initially deployed had only minimal access to the United States' most effective means of navigation, the Global Positioning System (GPS) and remained so until the U.S. Army used the delay in the war's start to procure and distribute thousand [sic] of commercial receivers."[2] Since then, however, significant efforts have been made toward Service integration and integration of information from space assets into operations. According to Lieutenant General Edward Anderson, USA (Ret.), for example, "Operation *Enduring Freedom* and Operation *Iraqi Freedom* are just tremendous examples of how our military has really become quite comfortable with using those [space] capabilities."[3]

Organizationally, however, requirements for space capabilities are not somewhere in the military, but they are everywhere as a function of space hardware providing force enhancement potential. They are also expensive, potentially drawing otherwise available funding away from other more traditional Service capabilities, such as tanks, ships, and planes, and from traditional command, control, intelligence, surveillance, and reconnaissance capabilities. Subsequently, while all the Services want input into decisions regarding how and where funding is spent, and full access to its use, there is less enthusiasm for bill-paying. That, added to entrenched bureaucratic acquisition practices and normal organizational politics, has resulted in decades of attempts at various arrangements to add more coherence to military space planning and organizational integration, toward optimizing funds and meeting ever-increasing needs and demands. But, as reflected over a decade ago, "organizational reform can

**Dr. Joan Johnson-Freese is a Professor of National Security Studies at the Naval War College.**

represent a major attempt to introduce change or a mechanism for deflecting real change."[4] Most efforts to date have served as the latter. In 2008, the Allard Commission—a panel named for sponsor Senator Wayne Allard (R–CO) and chaired by retired aerospace executive Tom Young—issued a report entitled *Leadership, Organization and Management for National Security Space*.[5] It found organizational military space integration fundamentally lacking, and offered a roadmap for change. However, more than 2 years after the Allard Commission Report was issued, military space integration is still limited by organizational gridlock and resistance, with few indications of positive change on the horizon. The answer for how to change that dim future outlook remains within the Allard Report.

## Still Searching

As the result of a 1993 congressional mandate borne from frustration over repeatedly asking the military "who's in charge" of military space policy and programs and getting no good answer, the positions of Deputy Under Secretary of Defense for Space and DOD Space Architect were chartered in 1995. Creation of those positions, especially the Space Architect, and multiple subsequent, mostly marginal reorganization efforts have been akin to rearranging the deck chairs on the Titanic, as evidenced by fast-forwarding to the findings of the 2008 congressionally mandated Allard Commission Report. It is peppered with concerns regarding a lack of a true authority for military and intelligence space assets—that no one is "in charge." Subsequent to the findings being released, commission chair Tom Young was quoted as saying there had been "no adult supervision" in national security space.[6] Having chaired what was known as the Space Commission in 2001[7] and having been in the rare position of being able to implement several of his own recommendations while in the top job at the Pentagon, Young was especially critical of Donald Rumsfeld's leadership in the area: "You could not give a grade other than F. You couldn't even give it a gentleman's D. It boggles my mind."[8]

One of the relatively few changes made regarding management of space programs as a result of Rumsfeld's Space Commission report was the Air Force assuming the role as the executive agent for space, with specific responsibility going to Air Force Space Command. That meant that the Air Force would own most space assets, though the other Services were the primary users, especially in Iraq and Afghanistan. The Air Force's performance as executive agent has been tenuous at best. Part of the problem, again, has been organizational.

*the Allard Commission Report is peppered with concerns regarding a lack of a true authority for military and intelligence space assets—that no one is "in charge"*

Air Force Space Command (AFSPC) was activated in September 1982. Realistically, it is a stepchild in a family that focuses first and foremost on airplanes. Additionally, U.S. Space Command was created in 1985 as a new functional unified command, both in acknowledgment of the increasingly recognized value of space assets, and to help institutionalize the use of space in U.S. deterrence efforts. AFSPC acted as a Service component of U.S. Space Command. In 1992, U.S. Strategic Command was created, incorporating U.S. Space Command in 2002, with AFSPC still a Service component. After the deactivation of Strategic Air Command, nuclear forces belonged to Air Combat Command from June 1992 to July 1993. Then, responsibility for both space and nuclear operations fell within Air Force Space Command for a while. Nuclear forces were merged into AFSPC in 1993, and that was never a fully comfortable marriage, with the cultural gap between space and missile operations much wider than many wanted to admit. Air Force Global Strike Command was created in 2008 and activated in 2009, taking over the missions of nuclear deterrence and global strike operations—the latter still not fully defined. If all these jurisdictional responsibility lines seem somewhat fuzzy and fungible, it is because they are. One of the (several) negative results of blurred lines of responsibility is multiple organizations fighting over the same pots of money.

To the Air Force's credit, as Major General James Armor, Jr. (Ret.), pointed out in his 2008 article subsequent to the Air Force nuclear debacles, "the Air Force has done nothing short of a spectacular job of bringing the U.S. to its current pre-eminence in space."[9] But, as he also pointed out, issues including too much emphasis on air superiority, prioritizing the future rather than the present, power grabs for new missions such as unmanned aerial vehicles and cyberspace, relations with Congress outside the DOD chain of command, and "shenanigans" in shorting the space budget—knowing Congress will restore the needed money and therefore increase the Air Force total budget—indicate problems.

Organizational issues were exacerbated when the Air Force procurement budget fell victim to the demands of urgent war bills, lowering the priority of already challenged space acquisitions programs. Congressional testimony in 2009 by Christina Chaplain from the Government Accountability Office (GAO) imparted the problems. She stated:

*estimated costs for major space acquisition programs have increased by about $10.9 billion from initial estimates for fiscal years 2008–2013. . . . Several causes consistently stand out. First, DOD starts more weapons programs than it can afford, creating competition for funding that, in part, encourages low cost estimating and optimistic scheduling. Second, DOD has tended to start its space programs before it has the assurance that the capabilities it is pursuing can be achieved within available resources. . . . Moreover, along with the cost increases, many programs are experiencing significant schedule delays—at least 7 years.*[10]

Attention to space issues suffered further after the Air Force was rocked by a series of events questioning its stewardship of nuclear weapons in 2008, resulting in the resignations of Air Force Secretary Michael Wynne and Air Force Chief General T. Michael Moseley, drawing more attention away from space issues. All in all, muddling along became the standard operating procedure. Allard Commission member General Anderson succinctly stated the problem as "no one's in charge, so everyone thinks they are in charge." He specifically cited Space Radar as an example of the consequent negative impact of that organizational model: "The intelligence and military space communities could not come to an agreement, so nothing ever got done."[11]

It has been over 2 years since the Allard Report was issued, and it is the second year

of a new administration in office. Both allow for real change to have occurred—or, alternatively, for the recommendations to be dismissed as "OBE" (overtaken by events) because there has been a change of administrations. Not surprisingly, the Allard Report drew "some support from younger military persons and outsiders when it was released, but encounter[ed] 'concern' and resistance from older, higher ranking personnel" with entrenched interests,[12] most often and likely to be those wanting to wave the recommendations away as OBE. The problems have not gone away, though. Thus, the Allard Report recommendations remain a valid topic for further consideration. In fact, because the problems have not gone away and the United States is now 2 years further into an increasing quagmire of space-related issues, the issues the recommendations address are more critical than ever.

## The Recommendations

The Allard Commission made four specific recommendations.[13]

■ The President should establish and lead the execution of a National Space Strategy that assures U.S. space preeminence, integrates the various participants, establishes lines of authority and accountability, and delineates priorities. To implement the strategy, the President should reestablish the National Space Council, chaired by the National Security Advisor, with the authority to assign roles and responsibilities, and to adjudicate disputes over requirements and resources.

■ Establish a National Security Space Authority (NSSA). The director of NSSA should be assigned the rank of Under Secretary of Defense for Space and also serve as Deputy Director of National Intelligence (DNI) for Space, reporting to the Secretary of Defense and DNI. The NSSA director will be the Executive Agent for Space with the sole authority, responsibility, and accountability for the planning and execution of the National Security Strategy (NSS) program, including acquisition. Key functions will be defining and formulating the Major Force Program–12 budget and serving as the focal point for interagency coordination on NSS matters. Analytical and technical support from a National Security Space Office–like organization augmented with Intelligence Community expertise will be required to effectively execute this responsibility.

■ Create a National Security Space Organization (NSSO). Assign to it the functions of the following entities: National Reconnaissance Office (NRO), Air Force Space and Missile Systems Center, Air Force Research Laboratories Space Vehicles Directorate, operational functions of the Air Force Space Command, and Army and Navy organizations now providing space capability. The merged organization will report to NSSA for policy, requirements, and acquisition and to AFSPC for organization, training, and equipping responsibilities. Spacecraft command, control, and data acquisition operations as well as launch operations will be NSSO responsibilities.

■ Change Air Force and Intelligence Community human resource management policies for space acquisition professionals in order to emphasize technical competence, experience, and continuity. Establish a career education, training, and experience path for the development of engineers and managers who are steeped in space. Establish as the norm that space project management personnel be in a given position for sufficient time to maximize project success—4 years or more—without adverse effect on an individual's career. Support should be given to the current Space Cadre management and training program being implemented by the Services, as exemplified by the Air Force through AFSPC and Air Education and Training Command.

Together, these recommendations were intended to represent a plan for a major overhaul of the processes used in conjunction with military space policy decisionmaking and implementation. These would not tweak the system; they would break it and start over. Implementation would represent an overall equivalent to those imposed on the Defense Department by the Reorganization Act of 1958 or the Goldwater-Nichols Defense Reorganization Act of 1986—both of which faced internal resistance and took years to implement and where implementation is still, some would argue, a work in progress. Individually, the recommendations addressed problems that had plagued space programs for years, but in doing so attacked the stovepipes and standard operating procedures by which bureaucracies had not just existed, but thrived, and individuals had built their careers. Change represents challenges to power.

The valid point also has been made that fixing problems by creating another layer of bureaucracy—which, it can be argued, the Allard recommendations do—rarely fixes problems. Even some close to the commission, including General Anderson, suggested there were "alternatives" to the organizational structure offered in the report.[14] Everyone, however, agreed that something had to be done, and the Allard Commission recommendations represented a way out of the inertia that had perpetuated the status quo for too long.

There are many reasons for "resistance," which is different from "friction." Friction occurs when implementing change—even if everyone is fully supportive of the planned change. It arises simply because details of implementation are inherently worked out as changes unfold, and sometimes not easily. If sources of the friction are dealt with promptly and effectively, serious problems can be avoided. Resistance, on the other hand, is intentional and aimed at stopping, altering, delaying, or otherwise adversely impacting attempts at change. It implements the adage of 19th-century British Prime Minister Lord Robert Salisbury: "Whatever happens will be for the worse and therefore it is in our interest that as little should happen as possible." There are many different forms of resistance, some most common and effective in preventing change, some in implementing change, and some utilized in both cases. These include "slow rolling" change, citing failures of the past as reasons not to change, spotlighting failure, exaggerating the costs of change, and minimizing the predicted benefits. All have been employed in avoiding implementation of the Allard Commission recommendations.

***Recommendation One.*** The recommendations begin with a plea for high-level leadership and a comprehensive strategy for the way forward that considers all elements of the various space communities—the stovepipes or fiefdoms—that have dominated programs. They have not been the only ones to do so. At the same time the Allard Commission was at work, a report was being prepared for the House Permanent Select Committee on Intelligence on challenges and recommendations for U.S. overhead architecture (spy satellites). In their findings, they begin by stating: "First, there is no comprehensive space architecture or strategic plan that accommodates current and future capability requirements."[15] And the National Research Council, in its 2009 report "America's Future in Space: Aligning the Civil Space Program with National Needs," included as one of its foundational elements for realizing critical

national objectives: "Coordinated national strategies—implementing national space policy coherently across all civilian agencies in support of national needs and priorities and aligning attention to shared interests of civil and national security space activities."[16]

Perhaps not surprisingly, no comprehensive space strategy—or even an effort to produce one—has yet emerged. Resistance has been largely unnecessary, as the recommendation was for the most part ignored. When addressed, slow-rolling in the form of "we're supportive, but it's just too hard" attitudes triumph. That was the prevailing attitude at a February 2010 workshop entitled *Towards a National Space Strategy*, for example, especially those currently in positions having a vested interest in maintaining the status quo. The workshop report that followed concluded: "An overarching approach to strategy, i.e., grand strategy, though desirable, is not feasible given political realities."[17] So there is no plan or even the intent to try to develop one, even though often the process of bringing the right people together to prioritize problems and talk about viable solutions is as worthwhile as a product that might or might not consequently follow.

Every plan must have an implementer for effective execution. Having everyone in charge and no one accountable has been cited as problematic dating back to the creation of the Space Architect position in 1995. So the reestablishment of the National Space Council with the National Security Advisor as Chair, to implement the strategy, was also recommended. But without a plan, the need for an executor can be, and has been, argued as moot. Alternatively, however, it can be argued that the existence of such an organization directly correlates with the potential for such a plan to be created and executed.

The National Space Council was created by President Dwight Eisenhower in 1958 as the National Aeronautics and Space Council (NASC), abolished in 1973 by President Richard Nixon, and reestablished as the National Space Council (NSC) during the administration of George H.W. Bush. Although it was originally intended to be headed by the President, Eisenhower generally ignored the NASC. John F. Kennedy utilized it, especially in the formation of the Comsat Corporation, but abrogated leadership of the organization to Vice President Lyndon Johnson, as did George H.W. Bush to his Vice President, Dan Quayle. The intent of the National Space Council has always been to provide a bridge between interagency space policies and programs toward national coordination. If the NSC is limited to coordination, however, it has little power or value, as it can simply be ignored. If it has authority to force its will on the multiple space players, however, it is a threat to their bureaucratic autonomy. Hence, while there have been multiple attempts to revive the organization over the years, and most recently the Obama administration has pledged its intent to do so, the status quo powers have managed to stifle those efforts.

Minotaur IV rocket launches Space-based Space Surveillance satellite to detect and track objects orbiting Earth

U.S. Air Force (Andrew Lee)

The Allard Commission recommendation to reestablish the National Space Council, with the authority to assign roles and to adjudicate disputes is viewed either as a threat, or as a bureaucratic solution to a policy issue, or both. While having someone in charge is clearly necessary for real change to occur, real change is not necessarily what bureaucracies, with a primary goal of self-perpetuation, in point of fact want. On the other hand, more bureaucracy can create as many problems as it can potentially solve, especially in terms of time required to deal with every issue and people involved (many of whom are uninformed and will have no role or responsibility for decision implementation). Also, centralizing personnel often sounds like a good idea, but when organizations badly want people reassigned to them, they often get exactly that: those people purged from other organizations. All that said, there is one clear, unambiguous aspect in recommendation one. Having the NSC chaired by the National Security Advisor rather than the Vice President unambiguously signals an attempt to move space policy closer to the inner circle of Presidential advisors and to someone with a strong position in the security communities. Until that happens, space issues will be considered as subsets of multiple other policy areas, rising to, falling from, and most often never reaching beyond the level of bureaucratic, staff importance. Until somebody close to the President is in charge, we will continue to rearrange deck chairs.

***Recommendation Two.*** Like any good plan of attack, the Allard Commission recommendations begin at the strategic level, and then move to the operational. That, however, is the level where most people work. Thus, immediate impact could be anticipated as a result of change. So it is not surprising that this recommendation generated the most immediate discussion, resistance, and pushback. In effect, recommendation two sought to combine the organizations that control classified and unclassified military satellites—the black and white worlds. Creation of a National Security Space Authority would give acquisition as well as requirements authority for both programs to one entity and one person, thereby stripping that authority from those currently holding it—the Air Force Space and Missile Systems Center (SMC), operated by AFSPC (for unclassified programs), and the NRO for classified programs, each with its own director.

For 3 years, between December 2001 and March 2005, Peter B. Teets was dual-hatted as both the Under Secretary of the Air Force and Director of the NRO, thus unifying the management of national security space activities. After 9/11, however, and focused attention on mechanisms for responding to global terrorism, establishment of the DNI created a powerful intelligence bureaucracy, which then

U.S. Air Force (Andrew Lee)

**Launch team members conduct preflight operations to test operational effectiveness, readiness, and accuracy of Minuteman III ICBM**

reclaimed the NRO as its own. When Teets left in 2005, responsibilities for space were again bifurcated, and organizational turf lines were again staked out.

Asked to comment on the Allard Commission report recommendations in 2008, Lieutenant General John Sheridan, SMC Commander, was judiciously noncommittal:

*I understand the results of that study are now being made public. Also, of course, it is just that at this point in time—the results of a study. There are no actions that have been taken by the government to lay in the plans that have been suggested by the results of the study. . . . They made one suggestion upfront in the report, which talks about coming up with a national strategy for space based on our national space policy. I don't think anyone would argue with the fact that having a strategy in place that lays out how we should build programs and apportion budgets would be a good way to organize things from the top down as far as the national commitment to space across the board, whether it is civil space or commercial space or national security space.*[18]

There was no need to be protective or negative, as it was already clear that the George W. Bush administration was not going to undertake any major reforms before leaving office, and equally likely that the Obama administration would have other priorities, which has proven true.

The GAO study of May 2009 on space acquisitions reiterated the concerns of the Allard Commission and others:

*The Allard Commission reported that responsibilities for military space and intelligence programs are scattered across the staffs of the DOD and the Intelligence Community and that it appears that "no one is in charge" of national-security space. The* [House Permanent Select Committee on Intelligence] *expressed similar concerns in its report, focusing specifically on difficulties in bringing together decisions that would involve both the Director of National Intelligence and the Secretary of Defense. Prior studies, including those conducted by the Defense Science Board and the Commission to Assess United States National Security Space Management and Organization (Space Commission) have identified similar problems, both for space as a whole and for specific programs. While these studies have made recommendations for strengthening leadership on space acquisitions, no major changes to the leadership structure have been made in recent years.*[19]

In fact, the "executive agent" position within the Air Force that was designated in 2001 in response to a Space Commission recommendation went vacant after Ronald Sega resigned in 2007, and then went into limbo, where it remains.

Pentagon acquisition czar John Young was happy to fill the void left by the resignation of Sega. In July 2008, he told lawmakers that he intended to retain oversight authority for military space programs: "I fundamentally disagree that a single service should have the total acquisition decision authority and milestone authority for a set of programs, as was done with space, and I would intend to retain acquisition authority over space programs."[20] Young did retain that authority. Soon thereafter, Air Force Chief of Staff General Norton Schwartz indicated that he wanted space acquisition authority to "migrate back"[21] to the Air Force, but that did not happen. During Senate confirmation hearings for Erin Conaton as Under Secretary of the Air Force in 2009, she stated: "The organization and management of space issues within the Air Force headquarters is under internal review, as well as through the Quadrennial Defense Review and the Space Posture Review process. These reviews and studies will inform and assist the Air Force in developing a way ahead."[22] The Quadrennial Defense Review was silent on the issue; the Space Posture Review is still under way. So turf battles continue.

***Recommendations Three and Four.*** Part of the impetus for recommending the creation of the NSSA was the commission finding that there are "insufficient numbers of space acquisition personnel to execute the responsibilities" of the SMC and NRO: "Both organizations suffer from the long-term ill effects of the reductions in government technical personnel made during the 1990s and neither has instituted necessary career development and management practices. Strengthened management focus is needed to identify, develop, assign, and promote acquisition personnel who are 'steeped in space.'"[23] Simply stated, there are not enough people who know what they are doing in the highly complex and technical space acquisition field.

The 2009 GAO report addresses both the quantity and quality aspects of the problem:

*More actions may be needed to address shortages of personnel in program offices for major space programs. We recently reported that personnel shortages at the EELV* [Evolved Expendable Launch Vehicle] *program office have occurred, particularly in highly specialized areas, such as avionics and launch vehicle groups. Program officials stated that 7 of the 12 positions in the engineering branch for the Atlas group were vacant. These engineers work on issues such as reviewing components responsible for navigation and control of the*

*rocket. Moreover, only half of the government jobs in some key areas were projected to be filled. These and other shortages in the EELV program office heightened concerns about DOD's ability to use a cost-reimbursement contract acquisition strategy for EELV since that strategy requires greater government attention to the contractor's technical, cost, and schedule performance information.*[24]

As a result of both cost-cutting measures that reduced the size of the acquisition workforce and an Air Force culture that favors pilots and technology specialists and consequently inhibits quality, experienced personnel from staying in key acquisition positions, hardware costs are rising, schedules are delayed, and U.S. capabilities are suffering. Ultimately, U.S. space superiority is being jeopardized by an unworkable organizational matrix of responsibilities that largely are underpopulated, and, when they are filled, it is often with the wrong people.

During the 1990s, as part of the post–Cold War downsizing efforts, the government made deep cuts into the technical workforce. The Air Force provides approximately 90 percent of space personnel to fulfill the DOD space mission. In 2006, the GAO pointed out the difficulties it had with fulfilling that role.

The Air Force has a shortage of midgrade and senior officers, who play vital management and oversight roles in space acquisition. At the Space and Missile Systems Center, 37 percent of the critical acquisition positions were vacant as of April 2006 and about 50 percent of the center's workload was being done by contractors. Also, the NRO depends on Air Force personnel to fill many of its key space acquisition positions. Continuing shortages may hamper the SMC and NRO ability to meet mission needs and highlight the Air Force's need to strategically manage its space acquisition workforce. The technical proficiency of the Air Force's space acquisition workforce also may not be adequate to meet national security needs. At SMC, the percentage of space acquisition officers with the highest acquisition certification level dropped from 28 percent in 1996 to 15 percent in 2005. Reasons for the lower certification levels include NRO priority in selecting personnel, the lack of a space acquisition specialty, limited training, and the decline in the number of personnel coming into the Air Force with technical degrees. Although required by law, the Air Force has not developed a career field for officers to develop space systems. Without a specialty to identify these personnel and increased space acquisition–related education and training, the Air Force may not be able to strategically manage its workforce and ensure personnel can effectively develop space systems.[25]

The Air Force recognizes that there is a problem. In fact, improving space acquisition is a specific objective in the Air Force Space Command 2009–2010 Strategic Plan. And while well intended and likely to render improvements, the degree of improvements possible is limited by cultural issues, and culture is always the hardest thing to change in an organization, which reaches back to the Air Force prioritization and stewardship issues discussed earlier.

## Moving Forward

In June 2010, the Obama administration released its National Space Policy (NSP). The language of the National Security Space Guidelines includes such directives as "develop, acquire, and operate space systems and supporting information systems and networks to support U.S. national security and enable defense and intelligence operations during times of peace, crisis, and conflict," "ensure cost-effective survivability of space capabilities," and "develop and implement plans, procedures, techniques, and capabilities necessary to assure critical national security space-enabled missions."[26] While responsibilities for taskings are allocated between the Secretary of Defense and Director of National Intelligence, nowhere does it say how these directives are to be carried out in anything other than a business-as-usual manner.

*the technical proficiency of the Air Force's space acquisition workforce may not be adequate to meet national security needs*

While Allard Commission recommendation one dealt with space at a strategic level, and recommendation two at an operational level, recommendations three and four get down to the tactical level, clearly indicating that space security management is "broken" at all levels.

When organizations and organizational structures are broken, as the Allard Report and others unequivocally say military space is, personnel is often an issue, and that has been clearly demonstrated in this case. But as is also often the case, a complex organizational structure can have many stress points, some self-reinforcing. Regarding the insufficient number of acquisition personnel to work on the highly technical and complex issues related to space hardware, it is a chicken-or-egg problem. The Federal Acquisition Regulations is a 600-plus-page manual that rivals the tax code for complexity—hence the need for an army of individuals to execute its provisions. Pile on top of those provisions a loss of credibility before Congress as to its ability to execute those provisions and programs, for reasons ranging from ethical violations to inaccurate cost estimates, and the military space community is saddled with checkers for the checkers and monitors for the monitors to a point of near gridlock. Clearly, tweaking the system is ineffective; a complete overhaul to address the myriad issues—self-imposed and otherwise—is required.

In all fairness, national security strategies, national space policies, and similar documents are all words on a page, ultimately judged by their implementation rather than their verbiage. While the overall intent of the NSP seems to be one of changing paradigms, in the area of military space integration it appears that the administration largely heeded the advice of the status quo advocates.

Though theoretically the long-awaited Space Posture Review could address these issues, largely the same folks have input into that process as did into the NSP. Bureaucracies do not by their nature champion change that threatens their established ways of doing business. Change is usually generated either by crises or by external forces anticipating crises and initiating change to avoid them. If left to internal forces, the day of reckoning is never seen to be imminent because efforts are focused on pushing it back rather than on fixing the problem. Though we can wait for a crisis to occur, the better option seems to be having change initiated and guided by an external force or body with enough clout to make it happen. That returns us to the first recommendation of the Allard Commission: reinvigoration of the National Space Council.

Presidential candidate Obama promised to bring back the National Space Council. Obama Science Advisor John Holdren stated that discussions were already under way to

revive the organization during his Senate confirmation hearings in February 2009. Senate Space Subcommittee Chair Senator Bill Nelson (D–FL) stated that reviving the National Space Council would take space policy out of the hands of "some green-eyeshade person at the Office of Management and Budget."[27] A 2009 report by the Aerospace Industries Association entitled "The Role of Space in Addressing America's National Priorities" states as its first recommendation, "Our space capabilities should be coordinated, at the highest level, as a singular enterprise."[28] And yet there was no mention of a National Space Council in the 2010 National Space Policy. The ability to stifle such a promised action is a tribute to the power of bureaucratic and organizational politics.

Former IBM chief executive Lou Gerstner, considered an authority on organizational change, clearly differentiated between reorganization and transformation: "Reorganization to me is shuffling boxes, moving boxes around. Transformation means that you're really fundamentally changing the way the organization thinks, the way it responds, the way it leads. It's a lot more than just playing with boxes."[29] For too long, the United States has been toying with reorganization of vital military space activities. Issues identified by the Allard Commission in 2008 made it clear that transformation is needed, and their recommendations toward that end remain sound.

While the presence of a National Space Council does not assure that transformation will occur, its absence almost certainly does assure that it will not. Until such an entity exists, headed by the National Security Advisor so as to have the access and ability to raise issues to the Presidential level, national security will suffer under the onus of organizational gridlock. **JFQ**

The author thanks Major General James Armor, Jr., USAF (Ret.), Colonel Dana Struckman, USAF, and Colonel Victor Budura, USAF (Ret.), for their comments.

## NOTES

[1] Edward J. Merola, Senior Historian, U.S. Naval Historical Center, available at <www.history.navy.mil/Wars/dstrorm/sword-shield.htm>.

[2] United States Space Command, United States Space Command Operations *Desert Shield* and *Desert Storm* Assessment, January 1992, 3, available at <www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB39/document10.pdf>.

[3] Sharon L. Hartman, "An Inside Look at the Allard Commission . . . And That's the Way It Was," *Army Space Journal* 8, no. 2 (Summer 2009), 20.

[4] Joan Johnson-Freese and Roger Handberg, "Searching for Policy Coherence: The DOD Space Architect as an Experiment," *Joint Force Quarterly* 16 (Summer 1997), 92.

[5] Report to Congress of the Independent Assessment Panel on the Organization and Management of National Security Space, July 2008, available at <www.smdc-armyforces.army.mil/ASJ/Images/National_Security_Space_Study_Final_Sept_16.pdf>.

[6] Amy Butler, "Adrift in Space," *Aviation Week & Space Technology*, October 13, 2008, 34.

[7] There were actually three commissions looking into space issues in 2001, evidencing it being viewed as perpetually broken: the Commission to Assess U.S. National Security Space Management and Organization (Rumsfeld's Space Commission), the National Commission for the Review of the National Reconnaissance Office, and the Independent Commission on the National Imagery and Mapping Agency.

[8] John M. Doyle, "Failing Grade," *Aviation Week & Space Technology*, October 13, 2008, 23.

[9] James B. Armor, Jr., "The Air Force's Other Blind Spot," *The Space Review*, September 15, 2008, available at <www.thespacereview.com/article/1213/1>.

[10] Christina T. Chaplain, Director, Acquisition and Sourcing Management, "Space Acquisition: DOD Faces Substantial Challenges in Developing New Space Systems," Testimony before the Subcommittee on Strategic Forces, Committee on Armed Services, U.S. Senate, GAO–09–705T, May 20, 2009, summary and 1.

[11] Turner Briton, "Plan to Join Classified, Unclassified Space Functions Faces Opposition," *Defense News*, September 1, 2008, 24.

[12] "Younger Military, Outsiders, Receptive to Reforming Space Security Procurement, Leadership, but Older and Higher-Ranking Officials Resistant," *Space & Missile Report*, October 20, 2008.

[13] A. Thomas Young et al., *Leadership, Management and Organization for National Security Space: Report to Congress of the Independent Assessment Panel on the Organization and Management of National Security Space* (Alexandria, VA: Institute for Defense Analyses, 2008), ES-4–ES-6.

[14] John Liang, "New Space Commission Report Recommends Abolishing NRO, SMC," *Inside the Air Force*, August 27, 2008.

[15] "Report on Challenges and Recommendations for United States Overhead Architecture," 110th Congress, 2d Session, Report 110–914, available at <www.fas.org/irp/congress/2008_rpt/hrpt110-914.html>.

[16] National Research Council, Committee on the Rationale and Goals of the U.S. Civil Space Program, *America's Future in Space: Aligning the Civil Space Program with National Needs* (Washington, DC: National Academies Press, 2009), 49.

[17] *Towards a National Space Strategy* (Superior, CO: Secure World Foundation, April 12, 2010), 9, available at <www.astroconsultinginternational.com/library/documents/Towards%20a%20National%20Space%20Strategy%20Report.pdf>.

[18] Tony Skinner, "Interview: Lieutenant General John R. Sheridan, Commander, U.S. Air Force Space and Missile Center," *Jane's Defence Weekly*, October 9, 2008.

[19] Chaplain, 13–14. Emphasis added.

[20] "No More Executive Agent for Space," July 14, 2008, available at <www.airforce-magazine.com/DRArchive/Pages/2008/July%202008/July%2014%202008/NoMoreExecutiveAgentforSpace.aspx>.

[21] "USAF Chief Wants Space Acquisition Authority to 'Migrate Back' to the Service," *Defense Daily*, February 24, 2009.

[22] Marcia Smith, "Will the Under Secretary of the Air Force Still Be DOD Executive Agent for Space?" November 20, 2009, available at <www.spacepolicyonline.com/pages/index.php?option=com_content&view=article&id=552:will-the-under-secretary-of-the-air-force-still-be-dod-executive-agent-for-space&catid=75:news&Itemid=68>.

[23] Young et al., ES-5.

[24] Chaplain, 14.

[25] Government Accountability Office (GAO), *Defense Space Activities: Management Actions Are Needed to Better Identify, Track, and Train Air Force Space Personnel*, GAO-06-908 (Washington, DC: GAO, September 21, 2006), summary, available at <www.gao.gov/products/GAO-06-908>.

[26] *National Space Policy of the United States of America* (Washington, DC: The White House, June 28, 2010), 13–14, available at <www.whitehouse.gov/sites/default/files/national_space_policy_6-28-10.pdf>.

[27] Frank Morring, Jr., "National Space Council to Return, Obama Science Advisor Pick Says," *Aerospace Daily*, February 27, 2009.

[28] Aerospace Industries Association (AIA), *The Role of Space in Addressing America's National Priorities* (Arlington, VA: AIA, January 2009), available at <www.aia-aerospace.org/assets/report_space_0109.pdf>.

[29] "In Focus: Lou Gerstner," available at <http://edition.cnn.com/2004/BUSINESS/07/02/gerstner.interview/index.html>.

Aircraft formation flies over USS *George Washington* during combined U.S. and South Korean maritime and air readiness exercise

U.S. Navy (Charles Oki)

# Defense Planning Paradigms and the Global Commons

*By* MARK E. REDDEN *and* MICHAEL P. HUGHES

Over the last several years, examination of U.S. national security interests within the context of the global commons has emerged as a major policy issue in the defense community.[1] At the highest levels of the Department of Defense (DOD), there is now an awareness that the U.S. military will be confronted by a host of challenges "to stability throughout the global commons."[2] Furthermore, the Nation can "expect to be increasingly challenged in securing and maintaining access to the global commons and must also be prepared for operations in unfamiliar conditions and environments."[3] In response, the 2010 *Quadrennial Defense Review Report* has now assigned "assured access" to the commons as a top priority for U.S. military forces.[4]

As defined by DOD, the global commons comprise the geographic and virtual realms of "space, international waters and airspace, and cyberspace."[5] They are a subset of the broader maritime, aerospace, and cyber domains, deriving their existence from the notion of areas that are accessible to all but owned by none. The commons are seen as the essential conduits of U.S. national power in a rapidly globalizing and increasingly interconnected world. The heritage of the commons' strategic importance can be traced back at least as far as Alfred Thayer Mahan, who highlighted the relationship between maritime power and the ability to maintain the sea lines of communications with economic expansion and the impact on overall national power.[6] Attainment of U.S. strategic, economic, informational, and military objectives is contingent upon assured access to, and freedom of action within, the commons. Accordingly, global commons access must remain at the forefront of U.S. national security imperatives.

Successful application of military power in and through the global commons in

**Captain Mark E. Redden, USN, and Colonel Michael P. Hughes, USAF, are Senior Military Fellows in the Center for Strategic Research, Institute for National Strategic Studies, at the National Defense University.** **This article is based on *Global Commons and Domain Interrelationships: Time for a New Conceptual Framework?* Institute for National Strategic Studies Strategic Forum 259 (NDU Press, November 2010).**

U.S. Air Force (Jim Varhegyi)

**Air Force Vice Chief of Staff testifies before House Armed Services Subcommittee on Readiness about Air Force cyber security measures**

support of overarching U.S. national objectives is likewise dependent upon the ability of military forces to access and maneuver within and across the commons—to deliver power in and through the various geographies. While the required extent and duration of the U.S. military's access to and freedom of action in the commons will be determined by larger strategic factors, the fundamental ability to achieve them is becoming more problematic. New complexities in the global commons potentially lessen military effectiveness, diminishing the military's ability to support national interests. Arguably, the least recognized and least understood of these complexities is the notion of domain interrelationships: the idea that *intradomain* military operations are increasingly dependent on *interdomain* dependencies.[7] Barring a fundamental shift in U.S. strategic objectives, the military must retain the ability to operate throughout the global commons to achieve the requisite level of local control and superiority for mission success in support of national objectives. To accomplish this, the U.S. defense establishment must reassess the fundamental ideas and concepts regarding military power employment within the global commons in light of expanding domain interrelationships.

## New Challenges

Responsibility for the maintenance of the global commons and guarantee of free access for both international trade and commerce and the projection of military power has for more than 60 years fallen to the U.S. military.[8] However, over the last two decades, a confluence of events and emerging issues has begun to impact the U.S. military's ability to gain access to the global commons, as well as its freedom of action within it. The continuing evolution of the commons presents the U.S. military with a host of new challenges and demands.

First among these challenges is the incorporation of new geographies into the commons. In addition to dealing with growing complexities in the more "mature" maritime and air components, the U.S. military is confronting the issue of integrating the newer domains, space and cyber, into its fundamental concepts of operation. The cyber domain arguably provides the most acute challenge; its complex and at times seemingly anarchic nature and the difficulty in detecting and attributing actions complicate military planning. Despite its breadth of use within both the civilian and defense sectors, the U.S. defense community's understanding of the full impact of cyberspace on military capabilities and operations is modest at best.

Compounding the issue of the expanded scope of the global commons is their increasingly congested and contested nature. Driven in large part by economic and technological advances, barriers to commons access have been significantly lowered, with an attendant rise in the number and types of actors able to exploit the commons. For example, space—the almost exclusive purview of the superpowers during the Cold War due to high financial and technical barriers—is now routinely accessed by several dozen companies and consortia from various states, as well as individual entrepreneurs and commercial entities. Similarly, the oft-quoted price of access to the cyber domain can be as low as the cost of a laptop computer.

The dynamics making the commons more contested are varied and complex. At the high end, a number of state actors are rapidly approaching the level of a peer or near-peer military competitor in specific geographic areas. Although unable to challenge U.S. military access to all of the commons on a global scale and for extended periods of time, robust investment in conventional and asymmetric antiaccess and area-denial capabilities is positioning some countries to be able to challenge U.S. military access and freedom of action in bounded regions and for set periods of time. This is a significant issue given U.S. global interests and the military resources and efforts required to guarantee security of those interests at long distances.

Exacerbating the challenges from traditional or rising peer and near-peer military competitors is the increasing influence exerted by nonstate actors in the global commons. State actors typically have substantial incentives to keep general access to the commons unrestricted. Nonstate actors can have drastically different motives. Driven by such factors as economics and political ideology, nonstate actors are more likely to deny, restrict, or disrupt commons access and usage in pursuit of their objectives. Even a modestly sized nonstate actor can exert a disproportionate effect within the commons. As evidenced in the cyber domain, at little cost in resources and effort, small groups (or even individuals) can disrupt and degrade Internet access and functionality for civilian, commercial, and government users, yielding effects that are of far greater value than the costs of producing them.

The precipitous decline in U.S. conventional air and naval platforms used to address these challenges aggravates the situation. The global commons are expansive in nature, with time, speed, and distance factors that at times can only be addressed through employment of large numbers of military assets. In the air

and maritime domains, current U.S. aircraft and ship quantities are a fraction of the levels that existed at the conclusion of the Cold War. In 2009, U.S. Navy ship numbers alone were over 50 percent lower than they were in 1990 in the waning days of the Cold War.[9] While technological advances help offset the negative aspects of force reductions, they are insufficient to address the growing challenges inherent in a more complex and dynamic global commons. In the cyber domain, resource challenges are exacerbated by the complex balance between offense and defense and the difficulty of attempting to innovate in a military field while simultaneously responding to the advancements of others. Unlike the maritime, air, and space domains, where the United States has traditionally been at the forefront of military development and has compelled potential adversaries to respond to its military initiatives, the Nation has no such advantage in the cyber domain.

External and internal fiscal pressures will limit the near- to mid-term potential for significant growth in the defense procurement budget. Furthermore, the short-term requirement to balance current counterinsurgency and counterterrorism operations against other mission requirements makes the prospects for a resource-intensive solution to the challenges posed within the global commons unlikely. The U.S. military will not be able to apply overwhelming quantitative and qualitative resource advantages to solve global commons problems.

The last and least recognized military challenge in the global commons involves the rapidly developing interrelationships among and between the different domains and the platforms and systems operating in and through the related parts of the global commons. The phenomenon is a manifestation of how military capabilities and operations have evolved, particularly over the last two decades. Domain interrelationships start at the most fundamental levels of military operations and capabilities and yield effects throughout the whole spectrum of military power as the totality of the interrelationships is integrated across each level of warfare. Now more than ever, effective and efficient application of military power in any specific part of the global commons rests upon a foundation of simultaneous access and freedom of action throughout the remainder of the commons. The idea of domain interrelationships is not new. These interrelationships have been, to a certain degree, part of military planning for as long as the potential for multidomain military operations has existed. Rather, it is the breadth of the various domain interrelationships and the pace at which they have developed that are now the critical issues.

Domain interrelationships cover a wide spectrum of dependencies between platforms and systems and, ultimately, operations. At the low end of the interdependence scale are interrelationships that enhance capabilities and provide force multipliers. This degree of interrelationship does not preclude employment of military power in a particular domain, but helps increase the effectiveness of platforms and systems. At the other end of the spectrum stand true interdependencies: interrelationships that can preclude operations in one domain if access to other domains is denied. Defense leaders have provided illustrative discussion on these evolving interrelationships and the global commons, particularly with respect to the space and cyber domains. However, taxonomies matter a great deal when distinguishing relationships that are interconnected (and therefore enabling) from those that are mutually dependent (and therefore require access to other domains).

Despite the increasing importance of domain interrelationships, development of military strategy and fundamental concepts of operations for the employment of military power within the commons has not kept pace. The increasingly congested and contested nature of the commons and the problem of declining U.S. conventional force levels do not necessarily lend themselves to quick fixes and will continue to stress the military's ability to ensure continued access to the commons. To prevent any further reduction in the margins of its military superiority, the United States must seek to optimize its military capabilities in the global commons despite these constraints. The U.S. defense establishment must revisit the fundamental ideas and concepts regarding the employment of military power within the global commons in light of growing domain interrelationships.

## The New Reality of Domain Interrelationships

Historical perspectives on military use of the global commons from the industrial age detail a long period of modest advances in capability and domain interactions. Military exploitation of each new geography, along with its integration with the others in the context of military operations, was modest in scope and relatively linear in nature, occurring over extended timeframes. Despite the work of General Billy Mitchell and others in the interwar period of the 1920s and 1930s, the full appreciation of airpower's utility in maritime operations arguably was not realized until World War II, some 30 years after the initial exploitation of the air domain for military purposes. The advent of the information age induced a marked shift in this dynamic. The technology that drove the information age significantly increased the range of militarily useful tools and resources, enhanced intradomain capabilities, and, more importantly, yielded a range of previously unavailable interdomain military options.

At the tactical level, advocates of platforms specific to each individual domain have continued their relentless pursuit of intradomain dominance, while exploiting technology-based capabilities that require access to other domains. As an example, the F–22 represents the premier air superiority aircraft, with its unequalled radar-evading technologies, engine performance, and advanced avionics; it also provides additional force multipliers such as unique connectivity and electronic attack capabilities. However, the latter capabilities are wholly dependent upon the ability of the aircraft to access the space and cyber domains. As the DOD aircraft investment plan for fiscal years 2011–2040 points out, "When considering aviation investment plans, the Department must increasingly consider the potential complementary capabilities resident in the cyber and space domains, as well as across other aircraft types."[10] The F–22 highlights how military operations within the global commons are now multidomain in nature, with interrelationships that can simultaneously span all domains and blur the distinction between supported and supporting efforts. Adding to this complexity is the growing overlap between the military and civilian realms, with military capabilities becoming increasingly reliant on commercial satellite communication systems, space-based surveillance, and cyber infrastructure for mission success.

With space and cyberspace serving as the bond between a range of military capabilities that require access to the commons, domain interrelationships have become more pervasive and complex. These interrelationships alter basic notions of force-on-force analysis. Drawing a parallel from cyber and

telecommunications network theory, the intrinsic value of military platforms and systems can conceivably increase at a nonlinear rate with the linear addition of each new platform and system, in large part due to the multitude of interrelationships.[11] A logical and corollary lesson is that vulnerabilities may expand at a nonlinear rate as well, with the associated risk to U.S. military operations increasing rapidly. Further proof of the importance of domain interrelationships exists in capabilities derived from exploitation of the space domain. Loss of space systems, whether involving the global positioning system constellation, communications systems, or intelligence, surveillance, and reconnaissance assets, would have negative effects that would cascade across military platforms and systems in other domains. This example illustrates how a limited number of key tactical level interdomain relationships can yield operational level effects.

*the growing reliance of military systems and operations on commercial enterprises is but one possible insidious relationship that puts U.S. military capabilities at risk and that is largely unseen without a macro view of the complex, interactive system that is the global commons*

The manner in which space and cyberspace now provide a means for the transmission of military power distorts traditional industrial age notions of supporting and supported domains. The increasing capacity for space and cyber to become the primary focus of effort within a military operation can lead to role reversals. For example, with a significant portion of the cyber domain relying on seabed transmission cables, efforts to disrupt military operations in cyberspace could employ maritime and air domain operations as supporting elements. The multiorganizational Operation *Burnt Frost* in 2008, which led to the destruction of a malfunctioning U.S. reconnaissance satellite, provides a real-world example: maritime domain operations (primarily) were conducted in support of operations in space, traditionally considered an enabling or supporting domain.

## The Traditional Approach

Throughout history, the emergence of human activity within each of the sea, air, space, and cyberspace domains has produced a fundamental transformation in the nature of warfare and military operations. It is this geographic aspect of warfare, albeit on a domain-by-domain basis, that has remained a cornerstone for the U.S. military approach to development of military power theory and operating concepts. This reductionist, bottom-up methodology arguably propagated a degree of stovepiping in strategy and concept development within the commons. Development tends to proceed in a linear and highly dogmatic fashion, with a focus on single domain exploitation preceding efforts to address the implications of domain overlaps and interdependencies. Much as was the case for air and maritime doctrine, development of concepts for military operations within the space domain (and more recently in cyberspace) appears to be following a similar pattern, with intradomain analysis and concept development preceding interdomain considerations. The U.S. Air Force and Navy have only just begun efforts to better understand the implications of cyber warfare for air and maritime operations; these nascent efforts are perhaps less well developed than the modest understanding of military operations exclusive to the cyber domain itself.[12] Bi-domain theoretical initiatives have typically been marked by a hierarchical conceptual approach in which one domain is dominant and the other exists in a subordinate or supporting role. While the military operating environment in and through the commons shows ever-increasing degrees of complexity, the theoretical methodologies used to address this environment have not kept pace.

## Why a New Approach?

The traditional approach to conceptual development that begins with intradomain work followed by measured bi-domain expansion lags the transformational nature of current opportunities and challenges in the global commons. The implications of these growing challenges are not insignificant. The growth of cross-domain interrelationships brings a concomitant increase in the number of seams between the domains—seams that offer large numbers of both vulnerabilities and opportunities. Approaching conceptual development for the commons with a stovepiped, single domain–centric mindset heightens the risk that domain dependencies and the resulting seams will be inadequately addressed. Given integrated and highly interdependent domain relationships, degrading one system in one domain has the potential to exponentially increase degradation in all other systems. Serious analytical attention has not been devoted to cross-domain issues such as these, partly because a traditional stovepiped planning methodology is insufficient to identify and analyze the full scope and relevance of these issues.

Shortcomings in applying the traditional planning methodology to the global commons are not limited to the military realm. The growing reliance of military systems and operations on commercial enterprises (such as satellite communications and imagery) is but one possible insidious relationship that puts U.S. military capabilities at risk and that is largely unseen without a macro view of the complex, interactive system that is the global commons. The importance of operating from the global commons, and the increasingly complex relationships of platforms operating within the various domains, clearly requires a theoretical construct that accounts for these factors.

There appears to be a growing recognition within the U.S. military that the evolving nature of the global commons and the rapidly expanding set of domain interrelationships mean that traditional approaches to strategy and concept development may be ineffective. As pointed out by General Michael Moseley, former Chief of Staff of the U.S. Air Force, "Since the air, space and cyber domains are increasingly interdependent, loss of dominance in any one could lead to loss of control in all. . . . No future war will be won without air, space and cyberspace superiority."[13] The very fact that DOD has now unified the disparate geographies into the more encompassing term *global commons* and is pursuing a new multidomain theoretical initiative called AirSea Battle hint at the prospect that the notion of the global commons may be more than just a new, more convenient taxonomy scheme and may in fact be an initial attempt to recraft the strategy and concept development process. The critical issue for security planners thus becomes finding an appropriate methodology for development of a military

U.S. Navy (Joshua J. Wahl)

**Navy Cyber Defense Operations Command Sailors monitor Navy information systems and computer networks for unauthorized activity**

concept of operations for the global commons that goes beyond the domain-by-domain approach and fully considers the rich interactions between domains that characterize military operations in the commons.

## Requirements of a New Planning Paradigm

Strategic thought has historically demanded consideration of a problem or issue in totality in order to grasp the full magnitude of the situation at hand. Whether for grand strategy development or military operational planning, a holistic perspective is required. Historically speaking, conceptual strategy development has always warned of the need for consideration of the whole in order to comprehend the overall nature of a particular military endeavor.[14] The same holds true for military planning when considering the need for operations conducted in any of the domains.[15]

Joint operating concepts in use today are designed to "identify future military problems and propose solutions for innovative ways to conduct operations. They are an articulation of potential future operations and describe how a commander, using military art and science, might employ capabilities necessary to meet future challenges."[16] Yet development of such concepts requires analysis that is not restricted to limited avenues of consideration (such as the air and sea domains as in the case of AirSea Battle). An analysis that envisions one or possibly two domains and considers others as enablers ignores the need to consider the totality of the global commons and the domains' evolving interdependent nature. As such, we should consider the global commons from a broader perspective.

While the body of intradomain research and concept development continues to evolve, parallel efforts that give full consideration to interdomain issues must also be conducted. An updated planning paradigm must fully quantify domain interrelationships, properly articulate the nature of the supported/supporting relationship for multidomain evolutions, seek synergies and leverage in military operations through the exploitation of domain overlaps, and ensure combat effectiveness by mitigating risks associated with seam vulnerabilities.[17] Strategists and defense planners must depart from the domain-centric mindset and take a broader perspective when viewing the commons. They must employ a holistic approach that breaks down domain stovepipes and treats the global commons not as a set of distinct geographies, but rather as a complex, interactive system.[18] It must not be merely an exercise in enhancing "jointness" within the force, but rather must be an issue of formulating a conceptual framework that allows us to think about, and plan for, military operations in this dynamic arena.

A paradigm shift to a macro perspective on a complex, interactive system that would provide the proper framework from which to address security and stability within the commons is needed to consider the global commons writ large. A Global Commons Operational Concept construct properly detailing the effective employment of military power to ensure commons access would serve not only military interests, but also broader national priorities within the diplomatic, economic, and informational realms as well. While at first appearing anathema to current doctrinal thinking, the intellectual exercise provides many benefits:

- it elevates thinking beyond the specific domains and forces a broader perspective that better accounts for the current reality of multidomain operations in the commons
- it forces consideration of the applicability of military missions (such as presence and power projection) into the newer domains of space and cyber
- it provides a framework to identify interrelated military-civilian-commercial connections that can affect military success.

## The Way Forward

The United States must decide whether an increasingly congested, contested, and competitive global commons allows for a military strategy as straightforward as one that exploits a command of the commons. The answer is not self-evident. There is a clear need for a more detailed analysis of the global commons, along with a systematic determination of domain interdependencies, identifying the resultant risks and rewards and the appropriate means of incorporating them into military strategy, concepts, and doctrine.

Given current and evolving globalization and technological trends, we need a holistic paradigm to advance our understanding of military operations in and employing the global commons. This new perspective should better frame the nature of domain interdependencies and their potential impact on military power employment options. At a minimum, a holistic concept development methodology should quantify the nature of domain interdependencies, identify military vulnerabilities and opportunities associated with the domain seams, and illuminate fundamental principles of military power employment that will mitigate the risks associated with seam vulnerabilities and exploit inherent seam opportunities.

This interdependent nature is becoming clearer and much more pronounced. Yet the ability to operate freely in a secure and stable

global commons is largely being analyzed using domain-specific constructs. Overarching questions must also be considered. What further research must be conducted to explore the interdependent relationships and maturing integration of the global commons? How do we define and comprehend the truly interdependent relationships that provide critical capabilities in a globalized world? Which dependencies are crucial to success when operating in the commons, and which linkages are merely enabling support? Have a common lexicon and taxonomy been clearly defined in order to consider the critical nature of the systems?

Multidomain interdependencies result in more complex challenges for military planners with regard to time, space (geography), and force issues given a particular objective or purpose. Joint operational planning emphasizes the importance of time and space and the need to comprehend these characteristics in and across particular domains. There is an increasingly critical need to more fully understand and exploit these cross-domain interdependencies, especially with respect to time disparities between the cyber domain and the other traditional domains. For example, the nearly instantaneous speed of movement in the cyber domain is very different from the time and space considerations that govern force employment in other domains. The implications for force planners used to focusing on maritime or air domains lie in the potential to exploit the speed of the cyber domain and ability to employ cyber assets at great geographic distances to increase the tempo of operations faster than ships can sail or aircraft can fly. However, this also implies that naval and air assets are now vulnerable to cyber attack from locations far removed from the battlespace. Air, space, or maritime forces reaching across their domains to influence or affect a force in another domain or multiple domains must now consider cyberspace's unique characteristics of speed, rapid pace of change, and influence on multiple domains in addition to the more traditional domains and their interrelationships.

From a military perspective, further consideration of a holistic global commons paradigm would inform strategy issues in a broader sense. What further analysis must be undertaken that informs or affects other aspects of military strategy, such as deterrence theory? Consideration should also be given to exploring the development of a military power theory for the global commons writ large. In addition, there should be analysis of an integration of a global commons military strategy into a global commons security strategy, and the resultant integration with other elements of national power and grand strategy, to ensure a synergistic approach to global commons research.

A paradigm shift must occur in order to fully comprehend the emerging systems nature of the global commons, and a military strategy and concept of operations are needed that fully consider the increasingly interrelated character of the various domains. Rapid technological advancements and improvements in military capabilities will continue to increase domain interdependencies within and across the global commons. As the United States and international community become more reliant on the global commons, a clear understanding of how to conduct multidomain military operations is needed if the United States is to have an effective strategy for maintaining military and commercial access to the global commons. **JFQ**

## NOTES

[1] Michèle A. Flournoy and Shawn Brimley, "The Contested Commons," U.S. Naval Institute *Proceedings* 135/7/1,277 (July 2009), 1.

[2] Department of Defense (DOD), *Quadrennial Defense Review Report* (Washington, DC: DOD, February 2010), 8.

[3] Ibid., 103.

[4] Ibid.

[5] *National Defense Strategy of the United States of America* (Washington, DC: Office of the Secretary of Defense, 2008), 13.

[6] Alfred Thayer Mahan, *The Influence of Sea Power Upon History, 1660–1783* (New York: Dover Publications, 1987), 25.

[7] Throughout this article, no distinction is made between the broader notion of domain interrelationships and, as a subset of that, commons interrelationships. The important conceptual point is based upon the fact that military operation interrelationships across the geographies of space, air, maritime, and cyber are growing in scope and complexity. Utilization of the full physical extent of space, air, maritime, and cyber as opposed to the more bounded areas encapsulated in the notion of the global commons has little bearing on the central tenets of this paper. The terms *domain interrelationships* and *commons interrelationships* may be used interchangeably.

[8] *National Defense Strategy*, 16.

[9] "U.S. Navy Active Ship Force Levels," Naval Historical Center Web page, available at <www.history.navy.mil/branches/org9-4htm#1993>.

[10] Aircraft Investment Plan Fiscal Years (FY) 2011–2040, submitted with the FY 2011 Budget, February 2010, 3.

[11] Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz, eds., *Cyberpower and National Security* (Washington, DC: NDU Press and Potomac Books, Inc., 2009), 149.

[12] Chief of Naval Operations Strategic Studies Group XXVII, "Collaborate & Compel: Maritime Force Operations in the Interconnected Age," December 2008.

[13] General T. Michael Moseley, USAF, "The Nation's Guardians: America's 21st Century Air Force," Chief of Staff of the Air Force White Paper, Washington, DC, December 29, 2007, 2.

[14] Colin S. Gray, *Modern Strategy* (New York: Oxford University Press, 1999), 23.

[15] Joint Publication (JP) 5–0, *Joint Operation Planning* (Washington, DC: The Joint Staff, December 26, 2006), III–17.

[16] Deterrence Operations Joint Operating Concept, Version 2.0, December 2006, 1.

[17] At the operational level of war, the concepts of leverage and synergy are defined and placed as critical concepts in warfighting capabilities. In accordance with JP 5–0, *leverage* seeks, "in the context of joint operation planning, a relative advantage in combat power and/or other circumstances against the adversary across one or more domains (air, land, sea, and space) and/or the information environment sufficient to exploit that advantage." *Synergy*, "achieved by integrating and synchronizing the actions of conventional and unconventional forces and capabilities in joint operations and in multiple domains[,] enables Joint Force Commanders . . . to maximize available capabilities and minimize potential seams or vulnerabilities."

[18] "Simply defined, a *system* is a complex whole, the functioning of which depends on its parts- and the interaction between those parts. Simple systems can be characterized as having a few subsystems that are involved in only a small number of highly structured interactions. They tend not to change much over time, being relatively unaffected by the independent actions of their parts or by environmental influences. Extremely complex systems, at the other end of the spectrum, can be characterized as having a large number of subsystems that are involved in many more loosely structured interactions, the outcome of which is not predetermined. Such systems adapt and evolve over time as they are affected by their own purposeful parts and by the turbulent environments in which they exist." See Michael C. Jackson, *Systems Thinking: Creative Holism for Managers* (New York: Wiley, 2003), 3, 19.

North Koreans bow in respect at statue of late leader Kim Il-sung

AP Images (David Guttenfelder)

# A Philosophical Case for OPCON Transition on the Korean Peninsula

*By* JOHN W. BAUER

The problem of North Korea confounds America today as much as it did 60 years ago. A rogue regime holds sway over a population of 23 million that is poised for war and intensely skeptical of the "Yankee" puppet government to the south. Negotiations, ongoing for decades, have come to seem hopelessly fruitless. The world has watched helplessly as the Democratic People's Republic of Korea (DPRK) has perpetuated diplomatic misdirection, disingenuous bargaining, and nuclear brinkmanship. Meanwhile, the Republic of Korea (ROK) has continued to reap the full financial and military benefits of the *Miracle on the Han River*—a phrase used to describe the astonishing export-fueled economic progress throughout the 1980s and 1990s. In recognition of the South's progress, the United States and South Korea are poised to deliver a debilitating strategic communications message to North Korea. On April 17, 2012, wartime command of ROK military forces is set to be transferred from the U.S.

**Major John W. Bauer, USA, was a Strategist in Special Operations Command Korea. He is currently pursuing a Ph.D. in Philosophy at the University of South Carolina.**

Kyodo via AP Images

**Kim Jong-un, left, heir apparent to his father Kim Jong-il as leader of North Korea, marks 65th anniversary of Workers' Party of Korea**

military to the South Korean government, ending 60 years of American control.

Yet recent statements have put this project in serious jeopardy. Since last year, a number of influential retired ROK generals have questioned the wisdom of such a move. These objections have been followed by recent statements coming from senior ROK government officials, claiming that the transfer is occurring at the "worst possible time."[1] Various American academics and policy advisors have recently joined the chorus of protestations.[2] The strongest arguments against operational control (OPCON) transition revolve around the lack of readiness within the ROK military command structure. Critics suggest that the most logical and prudent move is to delay. However, the reason for this recommendation is based almost entirely on subjective judgments about the ability to defend against North Korean attack. Who better to make that assessment than the current Allied Force Commander, General Walter Sharp? Recent statements by General Sharp have directly refuted these critics. He has stated that OPCON transition "will not lead to a reduction of [U.S.] forces or weaken the U.S. commitment to provide reinforcement to the Korean Peninsula."[3] In his expert opinion, OPCON transition can occur as planned without any degradation in American military capabilities.

*the OPCON transition has the potential to alter the entire calculus of North Korean regime control*

Rather than entering the debate over military readiness, this article seeks to highlight the deeper ideological rationale behind the transfer. Wartime control presents itself as an important symbol of ROK sovereignty and directly counters the North's accusations of American puppeteering. Such accusations are never merely gratuitous. They in fact provide the basis for the two messages that underlie the regime's grip over its people: first, the claim that the Americans, rather than the South Koreans, are really calling the shots; and second, the claim, playing on popular fears, that an unprovoked, imperialistically motivated American attack could happen at any moment. These claims form the explicit justification behind North Korea's "Military First" policy, which has been in effect since 1994. Convinced that the South is under American imperial control and an existential threat is imminent, it is no wonder the North Korean people have been able to endure famine and oppression for so long. They have become victims of a confused survival reflex based on a belief that their future as an unblemished, autonomous Korean nation is at stake and that the fragile liberty they possess is but a dream for their brothers to the south. To the contrary, the OPCON transition concretizes the handing over of responsibility for its own defense to a sovereign South Korea. This transfer has the potential to alter the entire calculus of North Korean regime control.

## Legacy of Occupation

The ideology that both grips the North Korean people and is so carefully protected by the regime finds its origins in the Japanese occupation of Korea from 1910 to 1945. Japan had previously spent 50 years assimilating Western ideas, including a period of unprecedented openness that reached its peak during the Meiji era. During that time, Europe found itself caught in a philosophical whirlwind, with popular thinking becoming radicalized to justify communism on the extreme left to ultranationalism on the extreme right. Japanese intellectuals, educated in Europe, took many of those ideas home and thrust them into the mainstream.

As Japan evolved into an ultranationalist, imperialist state, it found that such ideas provided convenient grounds for its far-reaching design for state control. These ideas directly influenced Japanese occupation policies following its annexation of Korea in 1910. In a clever attempt to pacify the Korean people, Japanese authorities went to great lengths to woo them into thinking that they too were chosen members of a greater Japanese state. Those who refused to cooperate were subjected to harsh measures deemed justified as a pragmatic necessity. While the oppression experienced by Koreans cannot be taken lightly, they did not entirely reject the Japanese project. By the 1920s, the upper and middle classes in Seoul were speaking Japanese voluntarily in their own homes.[4] Evidence suggests that in the waning days of imperial rule, Koreans found themselves to some degree accustomed to the Japanese style of governance.

The occupiers were finally expelled by the Allies in 1945, leaving the Koreans to deal with other forms of foreign influence. When Kim Il-sung came to power as the handpicked revolutionary of the Soviets, communism and North Korea were paired in a partnership of convenience. Reaping the ancillary benefits of the communist name, the DPRK received substantial military and economic resources from China and the Soviet Union throughout the 1950s and 1960s, assistance that helped it rise to a pride of place over its poorer brothers to the south. During the same period, the term *Juche* was born, the seemingly Marxist-communist, uniquely Korean ideology that has since both captivated and mystified the West. Often described as self-reliance, *Juche* was billed as the impressive pseudo-Marxist ideological creation of the elder Kim Il-sung.

But the connection between *Juche* and communism is weak at best. From North Korea's inception, virtually none of its

UN Command Security Battalion–Joint Security Area commander and deputy discuss joint evacuation exercise near demilitarized zone

U.S. Army (Christophe Paul)

intellectual elite received formal training in Marxism.[5] The philosophy was adjusted in 1970 at the behest of the Great Leader, who commissioned his close advisor Hwang Chang-up to devise an expanded *Juche* philosophy that would further baffle the outside world. Brian Myers, a professor in South Korea who has carefully researched primary source North Korean domestic propaganda, calls Hwang's creation an "ideological smokescreen." Hwang's *Juche* gave the impression that North Korea continued as a firmly entrenched, ideologically Marxist-communist state, assuaging outside observers while the regime worked toward its real goal, the continued loyalty and dependency of its citizens. Myers claims that Hwang, after defecting to the South in 1997, admitted that the main function of *Juche* was *externally* oriented.[6] The showcased ideology, which was intended to impress the world while offering a philosophical glimpse into the elusive North, had in reality nothing to do with the regime's true domestic ideology. To prove once and for all that the link between *Juche* and Marxism was nonexistent, the word *communism* was recently dropped from the North Korean constitution.

## A Philosophical Explanation

If the *Juche* philosophy is essentially meaningless and if the Marxism connection is absent, then what is the real ideology at work within North Korea today? It is in fact a carefully managed, sophisticated system of state control, following a logic that G.W.F. Hegel's political thought helps to unravel. Hegel, while credited with creating the philosophical framework for Marx, was also the principal architect of the German state-centric ideal that was later adopted by the far right. According to Hegel, no outside source, including international law, should hold weight over state self-interest and domestic autonomy because a government is a singular political actor that is inherently self-protective but not subject to the ethical constraints of individuals. The state, therefore, is permitted to undertake drastic means to curb dissent: "Those who attack the state itself indirectly … are the worst offenders, and the state has no higher duty than to preserve itself and to destroy the power of such offenders in the surest way it can."[7] When this idea is taken to its extreme, any means necessary are often applied to protect the state from subversion from within, regardless of the moral considerations. This explains North Korea's secretive network of gulags that has been spread throughout the country and for decades has incarcerated countless political prisoners and their families.

History, however, has shown that political theories detached from a satisfactory domestic ethical construct are inherently inadequate. It is perhaps for this reason that the totalitarian regimes of the 20th century have been relatively short-lived. Among these, North Korea has nevertheless continued to survive and is notoriously long-lived compared to others in existence today. Theirs is a system hinged upon the centrality of the state, an adaptation of the form of governance first brought to Korea by the Japanese. The regime is well served by this brand of political philosophy, which lends itself to popular norms of patriotic duty and national cohesiveness.

The North Korean ideology only reaches its full maturation when the regime succeeds in provoking fear of the outside world and of America in particular. In this way the people, who view themselves as incessantly vulnerable, are drawn closer to their protective parent-figure, the state. Yet allegiance to the state has not been the only phenomenon


Secretary Gates and General Sharp en route to visit troops at Camp Casey, South Korea

DOD (Cherie Cullen)

South Korean defense minister and Secretary Gates sign agreements reached during Security Consultative Meeting, October 2010

DOD (R.D. Ward)

holding the DPRK together. The ideology also contains a distinctly moral component designed to nurture lasting popular support.

### Moral Exceptionalism

At first glance, North Korea might appear to be a state in complete contradiction to any moral scheme. If there were an example today of diplomatic bad behavior, habitual renegation of international agreements, gross violations of human rights, and a state propaganda system founded on half-truths, one might suggest that North Korea fits the textbook definition. But a deeper investigation into North Korean ideology yields a different conclusion. In fact, the two primary moral messages conveyed by North Korea's propaganda apparatus provide a foundation for its entire ideological project.

The regime's first claim is that the Korean people are exclusively virtuous. North Koreans are continuously reminded of uniquely Korean attributes such as their affinity toward chastity, selflessness, and austerity—virtues that in North Korean propaganda are regularly contrasted with anecdotal Western vices.[8] Preserving the moral purity of Koreans from outside corruption is a serious affair, and one that calls for drastic means. On the one hand, it makes collective social and economic sacrifices seem reasonable under the DPRK's Military First policy. On the other, it implies a tone of moral exceptionalism that exempts North Koreans from moral obligations vis-à-vis the outside world as a matter of self-preservation. An example is the regime's contempt for international law, known most likely to only a close inner circle that in practice ranges from haphazard violations of intergovernmental agreements to a lucrative, government-sponsored counterfeiting operation. North Korea's capacity to engage in illicit activity is now enormous. Forty-five million dollars in counterfeit U.S. currency, the so-called $100–North Korean Supernote, has been detected in circulation.[9] Today, 40 percent of all North Korean trade either is comprised of arms sales or is illicit.[10]

The next claim made by the regime is that the character and magnanimity of the Dear Leader are beyond reproach. This moral message gives Kim Jong-il the legitimacy and popular support required to stay in power, in part because North Korean propaganda shows him as the "greatest man alive."[11] Kim always appears as a gentle, caring leader who exudes the virtue and austerity of a vulnerable, suffering people. The average North Korean knows no other image of its leader than the one depicted in a modest tunic and often in a loving embrace with common citizens. Strict censorship makes this theme even more compelling and prevents the circulation of rival opinions. As with the Japanese political legacy, this technique may have been adopted from their former occupiers because Hirohito was associated with similar symbols of virtue and purity such as white clothing and white horses.[12]

North Korean propaganda displays Korean virtue in stark contrast to the social excesses of America, touted as the imminent threat lurking at their borders and preying on their Korean brothers to the south. Over the past 60 years, the regime has succeeded in constructing a fear-based worldview premised on an ever-present military and cultural threat from America. This outlook supports a neo-Hegelian brand of authoritarianism that warrants harsh, centralized means to preserve

the moral purity of its people. It also relies on popular appeal for this moral ideal, hinging on the "politico-ideological unity of society" that the elder Kim had set as his goal decades ago.[13]

## Nationalism and Ameriphobia

The notion of an existential threat to uniquely Korean virtue does not find its sole audience north of the 38th parallel. Much can be said about contemporary South Korean feelings, generally implicit, that resemble explicit North Korean themes of suspicion for U.S. self-interest. For example, an American visitor to the National War Museum in Seoul is somewhat surprised by the tone surrounding the history of 1950. Rather than one of gratitude toward America as liberators, the museum emphasizes the fact that U.S. and Soviet diplomats placed the Korean people in their woeful predicament in the first place. In this narrative, the division of the Korean state was the fault of external meddling and the first step toward civil war. It is a perception that to this day is a source of distrust for America.

Perhaps the most surprising indicator of this distrust came to light 2 years ago when the *Korea Times* reported that more first-year South Korean Military Academy cadets viewed the United States as their country's main enemy than saw North Korea in that light. The statistic was later attributed to "inappropriate" education.[14] While it is not fair to say that the majority of South Koreans see America as no more than an imperialistic reincarnation of the Japanese, it is important to acknowledge the degree of cultural unity and solidarity that Koreans have with one another.

Much is said about North Korean nationalism, but a similar thesis could be made for trans-Korean nationalism. This thesis suggests that since 1948, there have essentially been two governments vying for one people. As one of 17 named agencies in the South Korean government, the ROK Ministry of Unification reflects this attitude from the South's perspective. Furthermore, in military-to-military interactions with members of the U.S. Armed Forces, the territory to the north is always written in English as *north Korea*—the lack of capitalization emphasizing that the country is only *temporarily* divided. This basic sentiment is shared by the North Korean regime, which has also articulated its desire for a reunified peninsula, albeit under the government of the DPRK.

According to regime propaganda, America is standing in the way of reunification. As preposterous as this accusation might sound, it appears that such repetitious rhetoric succeeds in subtly casting doubt on American intentions within the South. A recent North Korean press statement intoned this message: "It is the unchanging strategic design of the United States to cling more tightly to South Korea militarily, provoke another Korean war using it as a steppingstone, and going one step further, realize its wild ambition for achieving military domination over Asia."[15] In contrast, Kim Jong-il appears as the courageous leader holding the American military and cultural onslaught at bay and preserving all that is authentically Korean.

Whether or not the regime has been successful in shaping popular attitudes in the South, it is clear that South Koreans have entertained reservations about American interests, especially as ROK economic and military capabilities have grown in recent years. A comment from defector and former regime official Hwang Chang-up is indicative of these feelings, warning that the United States is concerned more about North Korean nuclear weapons than unification.[16] These types of statements almost certainly feed a current of mistrust, foreshadowing future competing American and South Korean priorities. The potential friction point is only exacerbated by the fact that America continues to retain its Cold War position of wartime command over South Korean troops, a command relationship that has endured since the Korean War.

## Wartime Control

The current plan for the transfer of wartime control had its genesis in 2005, when the George W. Bush administration first proposed the idea to the South Korean government. It was then favorably received by South Korean President Roh Moo-hyun, who saw the opportunity as a landmark event for ROK sovereignty. From the perspective of both sides, OPCON transition underscored the ever-increasing economic and military strength of South Korea, making the idea seem not only symbolic but also timely. Considering that the tables had been entirely reversed from the situation 40 years prior, South Korea's command over its own forces during wartime in many ways signals the final stage of its peacetime economic and military triumph over the North.

In the last three decades, the economic gap between North and South has been ever widening, with the North's gross domestic product in 2009 estimated at $40 billion compared to $1.4 trillion for the South.[17] Recent examples of ROK military capabilities have also been impressive, including its assuming command of the United Nations antipiracy mission off the coast of Somalia. In many ways, preparations for the OPCON transition event in 2012 have caused the ROK military to come into its own, heralding a transformation that has been as much technological as psychological.

*General Sharp has insisted that the difference between a U.S. and ROK commander is negligible and that OPCON transition can proceed as scheduled without incurring undue risk*

In the past year, however, the Lee Myung-bak administration has begun to show reluctance, with the repeated objections of retired ROK military officers now being echoed by members of the South Korean administration. Many point to an increasingly unstable North Korea. Indeed, the danger from the North is great: 800 ballistic missiles and 250 long-range artillery systems can target the Seoul National Capital Area, a metropolitan region of over 20 million people.[18] Nuclear tests are evidence of the North's tireless ambition to acquire weapons of mass destruction. An increasingly unstable food situation recalls the famine of the late 1990s, when between 3 and 5 percent of the population died of hunger.[19] Finally, questions over Kim Jong-il's health in 2008 provided cause for a rushed naming of his successor, the 26-year-old Kim Jong-un. Critics say that these factors, taken together, warrant keeping an American commander in charge.

The current American commander, however, feels differently. General Sharp has insisted that the difference between a U.S. and ROK commander is negligible and that OPCON transition can proceed as scheduled without incurring undue risk. Meanwhile, those South Koreans whom we might expect to support OPCON transition, such as pro-ROK sovereignty supporters, have fallen

conspicuously silent. Interestingly, the most recent politician to mention ROK sovereignty was Secretary of Defense Robert Gates, who during a visit in 2009 remarked that the United States looked forward to the ROK armed forces taking on the "proper lead role in the defense of its national territory."[20]

Why, then, is there a difference in opinion? To speculate on the source of this disagreement is beyond the scope of this article. What is clear is that arguments made by both sides have centered around a direct comparison of the ROK military to the DPRK military. The essential question has been all but overlooked, namely: What effect will OPCON transition have on the North Korean regime itself and its ability to maintain its grip as a legitimate government? The answer, in this author's opinion, is that OPCON transition holds real strategic promise because it imperils the North's ideology of regime control.

In the forthcoming OPCON transition debate, attention should shift to the ideological-strategic thesis that Korean nationalism is reason enough for America to disengage from its overt lead role. For the South, wartime control is a demonstration of full ROK autonomy. For the North, OPCON transition is a direct challenge to the DPRK design for regime control. South Korean leadership provides the North Korean people with a compelling rival alternative to the regime, namely an autonomous South Korean government that has ideologically overcome the regime's philosophy of externally directed, fear-based rule. In contrast, American leadership and the status quo play directly into the hands of North Korean propaganda and its political and moral influences.

The prevailing political philosophy advanced within North Korea today includes the Hegelian notion that the state is the citizen's highest, most solemn duty. This idea is not unique to the DPRK, but rather has been the trademark of other 20th-century totalitarian ideologies, ranging from communism on the left to Japanese and German ultranationalism on the right. When the reunification of the Korean Peninsula finally occurs, whether peaceably or as a result of crisis, there will be a tremendous opportunity for South Korea to appeal to Korean nationalism, the same nationalism the Kims' regime has carefully nurtured for decades. The best chance for unification lies here. The United States, on the other hand, is fundamentally ill suited to accomplish this task because the North Korean people are convinced that America is their primordial enemy. Hence, the only true remedy for the North's propaganda apparatus and its ideology of regime control is a ROK government firmly in the lead.

In the moral realm, South Korean leadership holds similar promise because many shared uniquely Korean virtues form the foundation of Korean nationalism. For this reason, the situation necessitates that the South Korean government, rather than an American military commander, be held up in contrast to a self-contradicting North Korean regime. Otherwise, American leadership will continue to veil the North Korean people from the moral discrepancies that exist—that the man purported to be the most virtuous Korean is in reality hardly genuine, and that the entire state system is corrupted by untruthfulness and injustice. These pathologies are not only in opposition to Korean moral virtues, but they are also inconsistent with the image by which Kim is conveyed to his people.

To fill the political and moral void that will be left when the regime finally fails, South Korea must be in command without any appearance of U.S. interference or leadership. Otherwise, the message of the North's propaganda apparatus will continue to survive in the minds of the North Korean people. A perpetuation of American wartime control prevents a political and moral breakthrough and only serves to reinforce the regime's lasting influence over its people, even after the regime ceases to exist. Therefore, in a collapse or jus post bellum situation, the perception that South Korea is in charge will be vital to any reasonable prospect for success. Likewise, the element of U.S. leadership currently in place stands as perhaps the last ideological thread holding back the North's capitulation. Hwang Chang-up has alluded to this point, declaring that "the most effective method South Korea can adopt is an ideological battle. . . . [O]nce we hold sway over North Korea ideologically, then we can defeat the regime."[21] If this is true, then let the battle be theirs. **JFQ**

## NOTES

[1] "Seoul Hints at Delaying OPCON Transition Amid Security Concerns," Yonhap News Agency, January 20, 2010, available at <http://english.yonhapnews.co.kr/national/2010/01/20/96/0301000000AEN20100120009200315F.HTML>.

[2] See, for example, Michael E. O'Hanlon, "Divide and Be Conquered," *Los Angeles Times*, March 3, 2010.

[3] Jung Sung-ki, "No Change in Command Transfer Timeline," *The Korea Times*, March 25, 2010, available at <www.koreatimes.co.kr/www/news/nation/2010/05/205_63030.html>.

[4] Brian R. Myers, *The Cleanest Race: How North Koreans See Themselves—and Why It Matters* (New York: Melville House, 2010), 29.

[5] Andrei Lankov, *From Stalin to Kim Il Sung: The Formation of North Korea, 1945–1960* (New Brunswick, NJ: Rutgers University Press, 2002), 40.

[6] Brian R. Myers, "Ideology As Smokescreen: North Korea's *Juche* Thought," *Acta Koreana* 11, no. 3 (December 2008), 171.

[7] G.W.F. Hegel, *Political Writings* (Cambridge, UK: Cambridge University Press, 1999), 81.

[8] See Myers, *The Cleanest Race*, 90, 115.

[9] Dick K. Nanto, *North Korean Counterfeiting of U.S. Currency* (Washington, DC: Congressional Research Service, June 12, 2009), available at <www.nkeconwatch.com/nk-uploads/2009-counterfeiting-us-currency.pdf>.

[10] Stephan Haggard and Marcus Noland, *Famine in North Korea: Markets, Aid, and Reform* (New York: Columbia University Press, 2007), 247.

[11] Myers, *The Cleanest Race*, 115.

[12] Ibid., 109.

[13] Kim Il-sung, "Report to the 5th Congress of the Workers' Party of Korea on the Work of the Central Committee," *For Correct Management of the Socialist Rural Economy in Our Country* (Pyongyang: Foreign Languages Publishing House, 1977), 314.

[14] Kim Yon-se, "34 Percent of Army Cadets Regard U.S. as Main Enemy," *The Korea Times*, April 6, 2008, available at <www.koreatimes.co.kr/www/news/nation/2008/07/116_22029.html>.

[15] *Roodong Sinmun*, February 9, 2010.

[16] See Mok Yong-jae, "Hwang Pushes for South Korean Ideological Battle," *Daily NK*, December 14, 2009, available at <www.dailynk.com/english/read.php?cataId=nk02200&num=5784>.

[17] *CIA World Factbook*, available at <https://www.cia.gov/library/publications/the-world-factbook/>.

[18] Bruce E. Bechtol, Jr., "The North Korean Military Threat to the Security of the Korean Peninsula and Northeast Asia: Paper Tiger or Ongoing Menace?" Institute for Corean-American Studies Winter Symposium, February 2010, 13, 46, available at <www.icasinc.org/2010/2010w/2010wbeb.html>.

[19] Haggard and Noland, 1.

[20] Robert M. Gates, "Remarks by Secretary of Defense Robert M. Gates from Yongsan Garrison, Seoul," October 22, 2009, available at <www.defense.gov/Transcripts/Transcript.aspx?TranscriptID=4502>.

[21] Mok.


Marines at remote forward base enjoy rare opportunity to use social networking sites to communicate with family and friends

U.S. Marine Corps (Khoa Pelczar)

# Mastering the Art of Wiki
# Understanding Social Networking and National Security

*By* JAMES JAY CARAFANO

Computers, cell phones, other digital devices, and the systems that knit them together have altered how many on the planet do almost everything—especially how they share with each other. With over 1 billion people—some of them enemies of freedom—on the Internet, there is much more on the information superhighway these days than information.

There is a traffic jam of conversation facilitated by email, Facebook, LinkedIn, Twitter, and, of course, Wikipedia, as well as many other social networking tools (often collectively called Web 2.0) that facilitate discussion, debate, and the exchange of ideas on a global scale.[1] This unprecedented capacity to listen and respond is inexorably restructuring the ways that information is created and used. For example, during the 2008 U.S. Presidential election, the campaign of Barack Obama mobilized social networking in revolutionary ways to garner popular support and raise money, reaching a vast audience. The impact of social networking will not end with business and politics but will inevitably affect national security.

Social networking has the potential to touch every aspect of national security including gathering and vetting publicly available open source information, gauging and influencing public opinion, distributing "risk communications" (such as how to respond after a disaster), conducting research and analysis, developing policies, planning and implementing programs and activities in the field, and conducting information operations (the integrated employment of electronic warfare, computer network operations, psychological operations, deception, and operations security).

**Dr. James Jay Carafano is Deputy Director of the Kathryn and Shelby Cullom Davis Institute for International Studies and Director of the Douglas and Sarah Allison Center for Foreign Policy Studies at the Heritage Foundation.**

## The Online World

There are basically two models for effectively distilling and sharing the best information in an organization—top down and bottom up. In the top-down framework, the senior leaders in an organization gather the best information. They use their wisdom, experience, and judgment to ensure that the information is shaped, edited, filtered, turned into knowledge, and then proliferated to the organization. Hierarchical knowledge creation and management work best in a static and predictable environment—one where senior leaders know best. In contrast, in

dynamic situations where experience counts for less, knowledge creation works best from the bottom up. At the grassroots, the immediacy of the junior leader turns out to be where the most effective learning takes place. Their experience is more fresh and relevant.

In the online world, the best knowledge comes from that bottom-up foundation, but that reality has problems as well as promise. Common wisdom holds that among social networks, the group itself assumes responsibility for culling out bad data. This includes everything from battling malicious actors online to pointing out simple errors—such as confusing pop star Michael Jackson with former deputy head of the Department of Homeland Security Michael Jackson. Wikipedia, for instance, is constantly keeping an eye on celebrity bio-pages to ensure that some star or head of state is not prematurely pronounced dead. Still, while the "rely on the crowd" method of adjudicating information may be suitable during normal social networking interactions, there is a real question over whether it is appropriate in matters touching on national security where lives and treasure may be at stake, where there is not time to let the network sort things out on its own, or where classified information once revealed cannot be put back in the safe.

The information jungle is a dangerous place. It has empowered both our scientific and narrative cultures. Information technology allows individuals to conduct more and better analysis, but it also allows opinion-makers to spin better, more compelling stories faster, and to proliferate them more widely. Digital-quick transparency can unmask evils or unearth secrets. Information that is massed to protect us can quickly be used against us. Secrets meant to be seen by almost no one can in minutes be leaked to everyone. The complacent may not survive long.

Information assurance cannot rely on the online crowd when national security is on the line. On such occasions, it is unrealistic to hold to the belief that negotiated Internet interactions are a sufficiently effective mechanism for determining factual and dependable information. Trusted actors and trusted networks must be established before crunch time, the terrible moment when lives and the fate of nations may be at risk. Trust and confidence are a must for a social network that can be depended on under stress.

Since the Internet is neutral, no party can count on a decisive and unassailable advantage across the "cyber-verse." For example, the debate over the impact of social networking on the Iranian election protests centered over whether these tools offered a clear advantage to the protestors or the government. Writing in the *Washington Post* in the wake of Tehran's post-election crisis, John Palfrey, Bruce Etling, and Robert Faris offered several counterpoints to those who had concluded that the force of online political activism is reversible. They argued that there are "sharp limits on what Twitter and other Web tools such as Facebook and blogs can do for citizens in authoritarian societies." Governments "jealous of their power can push back on cyberspace when they feel threatened." They also noted that the "freedom to scream" online may actually help regimes by providing a "political release valve." Repressive regimes can also employ social networking for their own ends, hawking propaganda and spreading disinformation.[2] Indeed, during the crisis, the Iranian government exploited all these advantages and in the end was able to largely stifle overt social unrest.

On the other hand, the Iranian government did not silence the voice of the people. Technology is continuously evolving, as are the practices of how the Internet is used. For instance, the regime in Tehran thought it could maintain permanent dominance of the Web by allowing only slow, expensive dial-up service. That assumption proved wrong. Social networking tools helped dissidents overcome the limitations of the nation's technological infrastructure.

There are also limits to what governments can do. If a regime such as Iran, for example, elected a "nuclear option" and tried to completely shut down the Internet to suppress internal dissent, it might well shut down its industrial, energy production, and financial sectors as well as crippling its capacity to control public media. Likewise, in a global economy, states or groups that conduct massive cyber attacks could do as much damage to themselves as to their enemy. Thus, a kind of "mutual assured destruction" deterrence appears to be evolving in the cyber world. At the same time, while some independent malicious actors may have no compunction about taking on a country, nations have every reason to seek to limit their ability to run amok. That, however, does not mean they will not try.

But nations have never been defenseless online, and even before America became super–security conscious after 9/11, the U.S. Government had not completely ignored post–Cold War threats to the Nation's peace and prosperity. Between 1998 and 2000, Congress held over 80 hearings on terrorism-related issues.[3] Efforts to enhance cybersecurity and combating malicious activity on the Web were on the list of things governments worried about. Likewise, there was a recognition that the Internet could serve as a tool of good governance. Efforts to make the Web serve people were undertaken as well. Instead of creating new practices and means of knowledge creation and knowledge management, E-Government was mostly about putting the way government already worked online. Even among governments, the United States was not the global leader. Nations such as New Zealand, Canada, and Singapore had more ambitious initiatives.

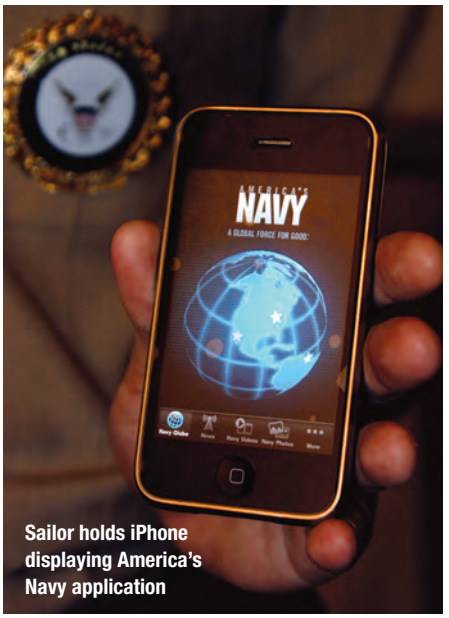
The "reality" of social network competition emerges again and again. It is wrong to look at cyberspace as a place for a static contest. There is no technology, government policy, law, treaty, or program that can stop the acceleration of competition in the cyber universe. Governments will not stop trying to rein things in, but it will always be a fight to the finish. No advantage will be permanent or unassailable. There will always be an enemy trying to take the cyber-heights.

Likewise, the platforms that carry network applications will likely change and evolve as well. Indeed, we are already seeing dramatic shifts in user preferences from personal computers to laptops to cloud computing to cell phones. Some, in fact, argue that computing is quickly becoming more a utility than a product. Software and hardware will mean less and less to social networkers as time progresses. Meanwhile, others are already predicting how online services will evolve, touting that Web 3.0 (where networks intuitively connect individuals to relevant information, not just other people) will soon supersede Web 2.0.

Still others look beyond and muse about the role of artificial intelligence in social networks. How we do what we do in social networks will likely continue to evolve, as will what we do with new applications. The bottom line is that it is a mistake to pin thinking about how social networks will work or what they will do in the future on any current platform or application. For now, what can be said of the global competition is that the two kinds of nations that are likely to be the most dominant competitors are those whose


U.S. Army (C. Todd Lopez)

Army is evaluating commercial handheld command and control solutions using Macintosh platforms




U.S. Navy (Michael B. Lavender)

Sailor holds iPhone displaying America's Navy application

regimes are the most authoritarian—and those whose societies are most free. Authoritarian regimes will utilize the brute force of control to seize social networking heights. Free societies will exploit the advantages of creativity, competition, and innovation. Both will prove remarkably resilient in online warfare. Both will be the main drivers in the course of the competition.

But the U.S. Government and, for that matter, many other governments are not well prepared to exploit social networking for national security. Bureaucracies often respond poorly to dynamic change and disruptive technologies. Web 2.0 can be both. There is growing unease that despite all the Washington talk of tackling cyber security and implementing cyber government, increasingly America may be "cyber-screwed." For starters, Washington is well behind in its willingness and capacity to adapt to the world of Web 2.0. Even President Obama, with his Blackberry by his side and a well-earned reputation as being Web savvy, has had his troubles. One of the first things the administration did in 2009 after moving into the White House was to revamp the President's Web site. A panel of experts assembled by the *Washington Post* gave the new WhiteHouse.gov site an average grade of C+.[4] That grade seemed to track well with the administration's response to the Iranian election protests. Even though there was a flood of information driving the global debate, as the protests grew, the President remained equivocal until several days into the crisis. Yet despite subdued rhetoric from the White House, the administration found itself pummeled by Iranian government accusations of interference, including a charge that an innocent bystander had been shot by the Central Intelligence Agency to foment a riot.

The disappointing results are not surprising. While the White House and many Federal agencies are experimenting with social networking tools, their efforts are largely unguided by sound research or clear and coherent policies that encourage innovation while protecting individual liberties and privacy. The hierarchical practices of traditional government are not keeping pace; they are inadequate for exploiting the explosion of social networking systems.[5]

There are a few lessons to remember when exploiting social networks, and for now we know what works. While there may not be hard and fast rules for social networking, there are some pretty good rules of thumb—principles for effective adoption of social networking tools that address the nature of the technology, structure of the social interaction, and value assigned to social networking transactions.[6]

The preference in social networking is to adopt proven and widely available software and systems that seem user friendly. Simple rules and simple operational routines are the hallmark of widespread adoption of social networking tools. The more intuitive the tool appears, the more likely it is to be adopted. And there has to be something in it for the user. Users are drawn to social networks because they believe participation will bring them a benefit they want. The recent proliferation of applications such as Web 2.0 Suicide Machine and Seppukoo (which allow users to purge their presence from online sites such as Facebook) reflects not so much a rejection of social networking as an affirmation that individuals are not terribly interested in a network from which they feel they derive no real value.

## The Past Was Prologue

Government has had a hard time getting the "adapting" to technology part right from the onset of the information age. In 1996, the Clinger-Cohen Act placed major emphasis on information technology acquisition. It required Federal agencies to treat information technology as a "capital investment," hoping to get the government to think more strategically about all the hardware and software it was buying. The focus of the law, however, was on how agencies acquired new technologies rather than on what kinds of technologies and capabilities they were developing. Many government investments involved developing Intranets (private computer networks), standalone databases, and proprietary software. When the tsunami of social networking applications hit the market and open software offered a rich variety of tools for innovation and collaboration, the U.S. Government stood to the side saddled with a huge investment in systems and databases that operated independently from the Internet and one another. Government struggled to keep up with private sector technology, let alone try to network the public and private worlds.

During the Clinton administration, Vice President Al Gore gave a good deal of thought to defending the information superhighway. In Clinton's second term, policy guidance started to pour forth from the White House. On May 22, 1998, the administration published Presidential Decision Directives (PDDs) 62 and 63. PDD–62 highlighted the growing range of unconventional threats, including cyberterrorism, and initiatives for defending against them. PDD–63 focused specifically on protecting the Nation's critical infrastructure, which included the backbone of the World Wide Web telecommunications systems and the electrical grid, as well as significant users of online services such as the government, transportation, and financial sectors. Washington also spent a lot of time and money (about $100 billion) getting ready for "Y2K," an effort to ensure computer systems would not fail as a result of trying to account for dates in the year 2000.[7]

The combination of the Y2K scare, emergent fears over cyberterrorism, and growing dependence on the Internet led to the creation of the National Infrastructure Protection Center (NIPC), a joint government and private sector partnership that includes representatives from Federal, state, and local government agencies. NIPC tried to incorporate lessons learned from the Federal Government's Y2K efforts and threats of millennial attacks, launching a series of law enforcement and counterterrorism initiatives. In 2000, the White House formulated the first national cybersecurity strategy.

Networking would have been a natural solution for the public-private cooperation and information-sharing called for in the cyber crime report. Discussions of social networking, however, were noticeably absent in the report. Clinton and Gore may have been the first President and Vice President to exchange emails, but Web 2.0 was simply not on the White House radar screen. The Government's Terrorist Surveillance Program proved another intensely controversial initiative. The covert program, first revealed to the public in a December 16, 2005, article in the *New York Times*, authorized monitoring of every electronic social networking tool from telephones to the Internet, email, and text messaging. Since the surveillance might have included communications to U.S. Persons (a term that denotes American citizens and other persons legally resident in the United States), but did not require a search warrant, the program came under intense criticism. In response to the controversy, the Terrorist Surveillance Act of 2006 provided additional authority to conduct electronic surveillance and assigned the special Federal court established under the Foreign Intelligence Surveillance Act with the responsibility for issuing any required warrants for investigations.

Most of what became known about post-9/11 "offensive" efforts on the Internet became instantly controversial. On the other hand, the Intelligence Community's "defensive" capabilities were more mundane and less like lightning rods. In particular, strengthening cybersecurity was a key objective of the Information Sharing Environment (ISE) established in 2007. The ISE is a collection of policies, procedures, and technologies that permits the exchange of terrorism information, including intelligence and law enforcement data. It aims to promote a culture of data-sharing among its participants to ensure that information is readily available to support their missions. The ISE is supposed to connect Federal, state, local, and tribal governments. It also envisioned a critical role for private sector and foreign actors in sharing information to counter terrorist threats.[8] Even 3 years after it was called for, however, it remains—to put it kindly—a work in progress.[9]

In 1988, in response to a computer virus called the "Morris Worm," which was unleashed through the Internet by Massachusetts Institute of Technology student Robert Tappan Morris, Jr., and affected 10 percent of the Internet, the Government issued a contract with Carnegie Mellon University to set up a computer emergency response team (CERT), the first Federally funded team to respond to malicious outbreaks online. After 9/11, another Government initiative was the National Infrastructure Protection Plan (NIPP). Since most sectors of the economy utilize the Internet, cyber became a focal point of the NIPP, which relied on several institutions, particularly information-sharing and analysis centers, to facilitate the exchange of information with critical business sectors, such as financial institutions and energy companies. If the CERTs were the field soldiers of cyber response, the Information Sharing and Analysis Centers (ISACs) were the rear command posts. ISACs were established and funded by the private sector, with the data they handled largely provided by private sector participants. ISACs also receive information from other entities, including law enforcement agencies and security associations. In addition to the ISACs, critical business sectors have Sector Coordinating Councils that develop policy recommendations in coordination with government agencies.

In addition to the strategies outlined by Homeland Security in the NIPP, the Department of Justice kept a foot in the cyber war. Information-sharing between the Government and private sector receives considerable support from InfraGard, a program originally established by the Federal Bureau of Investigation under President Clinton. First developed to assist in cybercrime investigations, InfraGard expanded collaboration with law enforcement, business, and academia on a range of security-related issues after 9/11. InfraGard chapters facilitate information collection, analysis, and training and provide discussion forums to share best practices. It also provides a secure Web-based communications platform.

Private sector companies, universities, research centers, and nongovernmental organizations have also developed capabilities to combat malicious cyber activities and to investigate or disrupt terrorist operations on the Internet. Perhaps the best known of these groups is the Internet Security Alliance, a collaboration among the Electronic Industries Alliance, a federation of trade associations, and Carnegie Mellon University's CyLab, established to provide a forum for information-sharing and to generate suggestions for strengthening information security.

Many other organizations and private sector companies support America's cyber defenses. After 9/11, the U.S. Military Academy at West Point established a Combating Terrorism Center. It joined CompanyCommand and PlatoonLeader (both military networks) as innovative projects started by the academy to help "big Army" adjust to the new challenges of the online battlefield. Among the center's studies is the "Islamic Imagery Project: Visual Motifs in Jihadi Internet Propaganda," which provides a ready guide to commonly used terrorist graphics, symbols, icons, and photographs.

The University of Arizona has also conducted a multi-year project called Dark Web, which attempts to monitor how terrorists use the Internet. The university's Artificial Intelligence Lab has accumulated the world's most extensive database of terrorist-related Web sites—over 500 million pages of messages, images, and videos—and has made it available

to the U.S. military and Intelligence Community. Some of its sophisticated software exposes social linkages among radical groups and seeks to identify and track individual authors by analyzing their writing styles. The Middle East Media Research Institute (MEMRI) publicizes extremist messages on the Internet, including terrorist Web sites, discussion forums, and blogs. After MEMRI published a comprehensive survey of Islamist Web sites in 2004, many of them were closed down by their Internet service providers.

*nongovernmental organizations and private companies provide a variety of analytical and investigative tools for penetrating terrorist operations on the Internet*

In addition to these efforts, nongovernmental organizations and private companies provide a variety of analytical and investigative tools for penetrating terrorist operations on the Internet. For example, the Washington-based SITE Intelligence Group routinely monitors, translates, and posts information from terrorist Web sites and often shares that information with U.S. intelligence agencies.

Finally, software and hardware providers continue to respond to the needs of the marketplace with new services and products to counter illicit online activity, from combating unauthorized intrusions and countering denial-of-service attacks to preventing the disruption or exploitation of systems or data. Providing security services and products is a multibillion-dollar-a-year industry.

**Befuddled Washington**

Government social networking has an even greater challenge because it is not clear if Washington knows what it is trying to do online. This problem is nowhere more apparent than in government's effort to get its message out—a task usually called "public information" when the message is for American audiences and "public diplomacy" when communicating with the rest of the world. Struggling to get the message out and get it right is not new—particularly where matters of national security are concerned. In World War I, the policies promoted by George Creel, the head of the U.S. Committee on Public Information, tried to manage the global pandemic. Later American efforts wrangled equally inelegantly, attempting to promote and protect freedom and provide for free and open expression, all at the same time. Government officials have always had a hard time figuring out whether their job is to push out government's point of view or simply provide a forum for "objective" discussion. Public diplomacy and information programs during World War II were chaotic. Even America's vaunted efforts at combating the ideology of communism during the Cold War were marked by as many setbacks as successes.[10]

Richard Solomon, the head of the U.S. Institute of Peace, observed, "The opportunity is there for State to put out American perspectives on almost any issue, for anybody to pick up—the question is: What should the government be putting out?"[11] This is the same question public diplomacy has been asking since long before the Internet was invented. Washington still lacks a clear sense of purpose online and that is just as big a problem as grappling with the bureaucratic hurdles of exploiting new technologies. In mastering the struggle for the cyber high ground on both ends of the power curve, not knowing what you are trying to do is a real obstacle.

A big part of why Washington struggles is that it is just not good at problem-solving. The last quarter-century has seen an explosion in the human capacity to create and manipulate new knowledge. Despite that fact, the instruments used to inform public policy choices are as creaky as ever. Washington makes policy largely by intuition shaped by an orthodox adherence to 20th-century problem-solving—ideas that have barely evolved since the Cold War.

Even so, something dramatic has been added to the arsenal for analyzing today's challenges—the proliferation of computer technology, the Internet, and everything else that goes with the "information revolution." Modern researchers have access to vast digital libraries and databases as well as powerful search and computational programs. New means of manipulating data, such as *informatics* (the science of information processing), *data-mining* (extracting and analyzing data to identify patterns and relationships), *computer simulation* (modeling a system), and *open source intelligence* (acquiring and analyzing information from publicly available sources to produce actionable intelligence), to name a few, are delivering revolutionary instruments of knowledge discovery.

Ironically, knowledge discovery is proliferating in every field except national security. While the means of knowledge discovery have become more sophisticated, the process of public policymaking has become increasingly intuitive. In Washington, talking points, gut feelings, partisan preferences, and ideological fervor crowd out cutting-edge analysis. Building cyber-strategic leaders from this will be like building castles on sand unless the knowledge and skills imparted to them are based on comprehensive, practical, and unbiased research—research that specifically serves the needs of governments. Knowledge of the present is not good enough to be a first-class cyber competitor.

The debate over how great ideas can be created through Web 2.0 and what comes after it is far from over. Research in the field of social networking is hard pressed to keep up with the rapid pace of change in how information technologies are fielded and employed. Understanding social networking requires a multidisciplinary approach to research that combines the techniques of the social sciences with "hard science" disciplines. This mix of disciplines, which examines how networks function, is often called "network science."[12] Practitioners study diverse physical, informational, biological, cognitive, and social networks searching for common principles, algorithms, and tools that drive network behavior. The understanding of networks can be applied to a range of challenges from combating terrorist organizations to organizing disaster response. Without understanding, the science is all just guesswork and luck (for good or ill).

Some governments and parts of governments "get it." One element that gets it is the U.S. Army, which in 2003 set up the Institute for Collaborative Biotechnologies. One area of focused research for the institute is "bio-inspired networks," studying "high-performance" biological networks for insights into how manmade networks can be made more scalable, robust, and energy efficient. In 2010, the institute oversaw 50 interdisciplinary research teams spanning 8 different academic departments at the Massachusetts Institute of Technology, University of California at Santa Barbara, and the California Institute of Technology. It is possible that the more scientists look to biological systems, the more applicable lessons they are finding for understanding computer systems and the activities on those systems, including social networking.

The potential of network science and its impact on social networks is too big an opportunity for free nations to ignore if they want to be respectable competitors in networked environments. All that said, while comparing cells and cellular phone networks sounds interesting, it is not easy science. A 2005 report by the U.S. National Academies laid out some daunting obstacles, including the difficulty in modeling and analyzing large, complex networks; developing better experiments and measurements of network structures; and establishing common concepts across the disparate disciplines that participate in network science.[13]

## Seizing Cyber High Ground

Thinking about the future is a vital part of holding the cyber heights. Part of the answer is seizing and holding the initiative on knowledge creation. Concerning the competence of social networking, the foundation of knowledge discovery could well hinge on the capacity to conduct cutting-edge network science. Forecasting the future is equally important for serious cyber warriors. Social networking and other information technologies have greatly empowered the tools for understanding and appreciating how complex dynamic systems and competitions will unfold over time. Mastering these methods and combining them to form even richer insights will give competitors a unique edge in anticipating future challenges.

Finally, it is important to look over the horizon and begin to plan how to deal with future challenges. Knowing they are out there and doing nothing to either exploit them or prepare to counter them means a competitor will likely lose in the long run. The technology of social networking will remain as dynamic as the competition to harness it. If Washington does not develop the human capital to create first-class cyber leadership, it will wind up as an also-ran in the social networking war of warfare. **JFQ**

## NOTES

[1] Josef Kolbitsch and Hermann Maurer, "The Transformation of the Web: How Emerging Communities Shape the Information We Consume," *Journal of Universal Computer Science* 2, no. 2 (2006), 187–207.

[2] John Palfrey, Bruce Etling, and Robert Faris, "Reading Twitter in Tehran?" *The Washington Post*, June 21, 2009, available at <www.washingtonpost.com/wp-dyn/content/article/2009/06/19/AR2009061901598.html>.

[3] Laura K. Donohue, "In the Name of National Security: U.S. Counterterrorist Measures, 1960–2000," BCIA Discussion Paper 20001–6, John F. Kennedy School of Government, Harvard University, August 2001.

[4] Jose Antonio Vargas, "Grading WhiteHouse.gov," *The Washington Post*, March 24, 2009.

[5] James Jay Carafano, *Social Networking and National Security: How to Harness Web 2.0 to Protect the Country*, Heritage Foundation Backgrounder No. 2273 (Washington, DC: The Heritage Foundation, May 18, 2009), available at <www.heritage.org/Research/NationalSecurity/bg2273.cfm#_ftn2>.

[6] Quotations from Clay Shirky, *Here Comes Everybody: The Power of Organizing Without Organizations* (New York: Penguin, 2008), 269, 271, 294.

[7] The spending estimate is based on National Communications System, Report 99–62, available at <www.ncs.gov/n5_hp/Customer_Service/XAffairs/NewService/NCS9962.htm>. For an overview of Y2K lessons learned, see David Mussington, *Concepts for Enhancing Critical Infrastructure Protection: Relating Y2K to CIP Research and Development* (Santa Monica, CA: RAND, 2002), 11–18.

[8] "Information Sharing Environment, Information Sharing Environment Implementation Plan," November 2006, available at <http://static/reportimages/AD829E9BA2DCE1A1A490FE89BF499CDD.pdf>.

[9] The Markle Foundation Task Force on National Security in the Information Age, "Nation at Risk: Policy Makers Need Better Information to Protect the Country," Washington, DC, March 2009, available at <www.markle.org/downloadable_assets/20090304_mtf_report.pdf>; Government Accountability Office (GAO), *Information Sharing Environment: Definition of the Results to Be Achieved in Improving Terrorism-Related Information Sharing Is Needed to Guide Implementation and Assess Progress*, GA0–05–492 (Washington, DC: GAO, June 2008), available at <www.gao.gov/new.items/d08492.pdf>.

[10] See Nicholas Evan Sarantakes, "Word Warriors: Information Operations during World War II," in *Mismanaging Mayhem: How Washington Responds to Crisis*, ed. James Jay Carafano and Richard Weitz (Westport, CT: Praeger, 2007), 27–45; Carnes Lord, "Marketing Freedom: Cold War, Public Diplomacy, and Psychological Warfare," in *Mismanaging Mayhem*, 46–66.

[11] Bryant Jordan, "Net Diplomacy," *Federal Computer Week*, October 29, 2000, available at <www.fcw.com/Articles/2000/10/29/Net-diplomacy.aspx>.

[12] See, for example, Committee on Network Science for Future Army Applications, *Network Science* (Washington, DC: The National Academies, 2005).

[13] Ibid., 48, 49.

U.S. Navy (Walter Shinn)

Coastguardsman uses social media monitoring system to assist in rescues and medical evacuations

# A Commander's Strategy for Social Media

*By* THOMAS D. MAYFIELD III

*We must hold our minds alert and receptive to the application of unglimpsed methods and weapons. The next war will be won in the future, not the past. We must go on, or we will go under.*

—General of the Army Douglas MacArthur, 1931

In 1931, General MacArthur could not have imagined many of the forms of warfare that would be used just a few years later during World War II. He understood, however, that changes in methods and weapons could alter the nature of conflict. Just as machineguns, tanks, and aircraft changed the nature of conflicts, so did the telegraph, radio, television, and eventually the Internet. The advances today in the information world, specifically with the advent of social media and new media, may prove as profound as any of these inventions. We must therefore observe and adjust our information strategies in order not to "go under."

One of the challenges that commanders now face is to develop strategies that recognize the shifts in the nature of warfare resulting from social media. There are already examples of militaries that have ignored the realities and have suffered. The effective use of social media may have the potential to help the Armed Forces better understand the environment in which it operates. Social media may allow more agile use of information in support of operations. Moreover, they may be harnessed to help achieve unity of effort with partners in conflict. Finding clever and innovative ways to help achieve the desired ends may be the key to success in a continuously evolving social media environment.

Social media are changing the way that information is passed across societies and around the world. The rapid spread of blogs, social networking sites, and media-sharing technology (such as YouTube), aided by the proliferation of mobile technology, is also changing the conditions in which the United States conducts military operations. The speed and transparency of information have increased dramatically. Events that only a few years ago could have remained state secrets indefinitely are being reported around the world in minutes. The traditional roles of the media are changing with the ubiquitous nature of data transmitting technology. Citizens with cell phone cameras can transmit damning images to the world, unfiltered, in the time it takes to make a phone call. People can use social networking to mobilize groups in support of a cause without having to expose themselves to the risks and costs formerly associated with activism. In response, governments and institutions can do little to effectively stop it. The aftermath of the June 2009 elections in Iran provides an example of how social media may be changing the nature of political discourse and conflict in the world.

**Colonel Thomas D. Mayfield III, USA, is Chief, Plans Division (G3), Headquarters U.S. Army Europe.**

### Tehran, June 20, 2009

Neda Agha-Soltan was sitting in her Peugeot 206 in traffic on Kargar Avenue. She was accompanied by her music teacher and close friend, Hamid Panahi, and two others. The four were on their way to participate in the protests against the outcome of the 2009 Iranian presidential election. The car's air conditioner was not working well, so Neda stopped her car some distance from the main protests and got out on foot to escape the heat. She was standing and observing the sporadic protests in the area when she was shot in the chest (reportedly by a member of the Basij, the pro-government Iranian militia). As captured on amateur video, she collapsed to the ground and was tended to by a doctor and others from the crowd. Someone in the crowd shouted, "She has been shot! Someone, come and take her!" The video spread across the Internet virally, quickly gaining the attention of international media and viewers. Discussions about the incident on Twitter became one of the most viewed topics worldwide by the end of the day.[1]

What happened next reveals the potential power of social media. Within hours, several versions of the video were posted on YouTube and linked to various other Web sites. Millions saw the gruesome photos of Neda's death when they were posted. The images highlighted the harsh response from the Iranian government and added fuel to the next 10 days of violent protests in Tehran. Many people around the world began posting editorials about the protests and the Iranian government's oppressive reactions. Twitter

AP Images/YouTube

**Frame from amateur video on YouTube purporting to show Iranian opposition supporters demonstrating outside Ghoba Mosque in Tehran**

reported millions of tweets, most condemning the Iranian government and its supporters. Iranian students began using Twitter and Facebook, as well as Flickr, the social site that allows users to post and share photos, to communicate to the Iranian audience information about when and where the next protest would take place, and which streets to avoid because of police or militia checkpoints.[2]

The case of Neda demonstrates that social media are not easily contained. Even with all the measures taken by the Iranian government, the images of the protests and reports of the government's abuses continued to make it to the Internet. The protestors quickly devised ways to get around the government efforts to impose blocks on their networking. The Iranian government eventually managed to control much of the online traffic, but it was too late to stop the effects of the social media. Tehran received massive diplomatic pressure from other governments and condemnation from media around the world to put an end to the post-election violence.

Around the world, social media are becoming commonplace tools for political and social activism. If military leaders do not fully understand these tools, they may miss their significant impact on the nature of future conflicts. America's potential enemies are using these technologies now to enhance their efforts. The U.S. military can either engage in the social media environment seriously or cede this ground to the enemy.[3] The development of strategies to account for the impact of social media will be one of the keys to success in future operations.

The germane question to ask is: How can an effective social media strategy have an impact on the outcomes of military operations? A recent *Military Review* article described the use of new media tools in the second Lebanon War involving Israeli forces and Hizballah in 2006.[4] The article contrasted that with Operation *Cast Lead*, when Israeli forces attacked the Gaza Strip in December 2008 and January 2009. The differing approaches taken by Israeli forces in the two operations highlight how an effective new media strategy can impact the strategic outcomes.

In the summer of 2006, Hizballah effectively integrated information operations, including social media, into their tactical operations to fight the Israelis. Hizballah embedded photos and videos into blogs and YouTube to promote a positive self-image and to highlight negative perceptions of Israeli operations. Hizballah used information effectively to limit Israel's strategic options. After 33 days of fighting, a ceasefire was declared and Hizballah claimed victory. The organization was able to create a "perception of failure" for Israel, which ignored the realities of the new media and relied instead on traditional information policies. It was less agile than Hizballah and was unable to match the group in the information war. In contrast, in Operation *Cast Lead*, Israeli forces devised a more effective strategy for the use of social and new media. They developed a proactive information strategy, incorporating social media tools, along with enlisting the support of the Israeli online communities, to set the agenda in the media and control perceptions of the fighting. The result was that the Israelis used information effectively to preserve strategic options enabling them to achieve their objectives.[5]

## The Ends

The strategic framework used by the U.S. Army War College defines a *strategy* as the relationship among ends, ways, and means. To develop a strategy, we must first have objectives or ends in mind. The *ends* are goals sought by the commander devising the strategy.[6] With respect to social media, what are some of the ends a commander might have in mind?

Perhaps the first end that commanders should have in mind when determining their strategy is a better understanding of the environment, or better situational awareness through an effective use of social media. By systematically observing the online community in the area of responsibility (AOR), commanders may be able to develop an ongoing understanding of the society in question, as well as its concerns and interests, and the commanders may be able to identify emerging trends and patterns. Blogs and social networking sites could provide insight to any society where there is a significant online community, particularly in societies with a relatively young population. The Department of State has effectively used social networking sites to gauge the sentiments within societies. U.S. Embassies in many nations are effectively using Facebook and other social media tools in places such as Podgorica, Damascus, Phnom Penh, and Panama to maintain relationships with the local cultures, particularly with the youth who are more likely to engage using social media.[7]

Maintaining a social media presence in deployed locations also allows commanders to understand potential threats and emerging trends within their AORs. The online community can provide a good indicator of prevailing moods and emerging issues. Many of the vocal opposition groups will likely use social media to air grievances publicly. In the fall of 2008, General David Petraeus wrote an article for *Military Review* entitled "Multi-National Force–Iraq Commander's Counterinsurgency Guidance" in which he lists key tasks for his commanders in Iraq.[8] While the tasks listed are intended for fighting the insurgency in Iraq, many of them are universally applicable. For example, he asserts that it is important for commanders to "[u]nderstand the neighborhood" and "[l]ive among the people." An online social media presence can be an integral part of understanding the issues and attitudes in a neighborhood or community. An online presence can play a major role in living among the people in a society that has a significant online community. Social media would certainly not be the only tool used by commanders; however, they could enable the commanders to understand environments and allow them to have better situational awareness of these environments.

A second desired end for social media in a theater of operations may be to assist the command in providing better, more agile, and more credible public information in the AOR (both strategic communications and local/tactical information). As demonstrated in the example above of the Israel Defense Forces, aggressive engagement in the social media environment can aid a commander in winning the information fight. General Petraeus's guidance emphasizes the importance of several related tasks. He directs us to "fight the information war relentlessly" and to "be first with the truth."[9] Clearly, a social

media program can play a key role in accomplishing these tasks. Understanding that social media have altered the way and the speed with which news is reported, commanders will be best served if they are actively engaged and immersed in this new environment. With an aggressive online presence, commanders can be better prepared to counter false and negative reporting as events occur. They can better interdict and react to bad news if they are already engaged and understand the way reporting in the AOR is likely to proceed as events occur. Finally, by being proactive, commanders can avoid letting enemy elements set the agenda by being there first with the truth. As demonstrated in Operation *Cast Lead*, commanders can use social media to help set the agenda in a strategically beneficial way.

The third and final end for commanders using social media in an AOR is enhanced unity of effort. General Petraeus in his guidance argues that commanders should strive for unity of effort with the U.S. Embassy, interagency partners, local governmental leaders, and nongovernmental organizations (NGOs) to make sure all are working to achieve a common purpose.[10] The characteristics discussed earlier relating to the ability of social media to aid in organizing can be used to enhance unity of effort with partner organizations in the theater of operations. The Israel Defense Force used new media methods to enlist the support of the Israeli "blogosphere" to help achieve a common purpose during Operation *Cast Lead*. A proactive and innovative social media strategy using social networking, blogs, and Twitter-like capabilities can aid commanders in ensuring all concerned entities in the theater of operations are sharing the necessary information to work toward a common goal.


**Facebook page supporting IDF Operation *Cast Lead***

**ISAF–NATO Facebook page**

## The Ways

The second element in developing a strategy is to identify the *ways*, or how one organizes and applies the resources.[11] What are the organizational schemes and methods required to achieve the ends that the commander has stated?

The first way is that social media use must be in the form of a Commander's Social Media Program. That is to say, social media should have the support and interest of the commander and key members of his staff and should be formalized into a program with responsibilities assigned to members of the commander's staff. The commander should view social media as an asset rather than a threat. Social media planning should be incorporated across the spectrum of conflict. The commander should state his intent for information effects, explicitly noting the role social media should play. That allows his staff to generate options much the same way as is done for other combat multipliers. A proactive engagement with social media incorporated into the commander's operational planning would likely provide the best results.

There will certainly be skeptics about the need for a command social media program. In an article linked to the Department of State's Social Media Hub, entitled "Eight Ways to Ruin Your Social Media Strategy," mistake number one is to "Pretend you can do without it."[12] As seen in the case of the Israel Defense Forces' experience, ignoring new media is done at our own peril.

A second way to take advantage of social media is to organize the social media program for success. The U.S. military has experimented with ways of organizing for success in strategic communication (SC) for the last few years. The experience gained in organizing for strategic communication may provide some insight into organizing for social media success as well. The Joint Warfighting Center *Commander's Handbook for Strategic Communication* lays out five models that have been used for organizing SC. The options include:

- increasing command emphasis (least costly)
- tasking an existing staff leader/section
- integrating a direct planning team
- centralizing control of all SC-related activities under a separate directorate (most costly)
- having an SC director with a small coordinating staff and supporting working group.

The final option has gained the most traction in the field, with several combatant commands adopting a similar structure.[13] That option provides the ability to incorporate the best attributes of the other options and maintain an appropriate level of command emphasis on the SC program. While commanders may choose to employ a similar methodology for social media, integration of social media planning into an existing SC structure may also be an effective way to ensure success. Commanders will have to weigh the costs with the potential benefits in their particular situation.

The natural reaction of many commanders may be to assign one staff section as the proponent for social media, leaving the responsibility for integration to them. While that approach may be easier to implement than some of the other options, the risk is the social media program will become viewed as a niche program and will not get the attention it

might deserve. Furthermore, the social media program would assume the natural biases of the assigned staff element, decreasing its broad effectiveness. For example, if J6 (Command, Control, Communications, and Computer Systems staff section) were the proponent, it might input a technical bias, and likewise the Public Affairs (PA) section might tend to approach social media as an outreach tool only. Thus, broad integration may provide the best opportunity to achieve the results desired.

*the information security concerns over experimentation of social software on Department of Defense computers are not trivial*

The third way to benefit from social media is to create a social media monitoring team to act as the eyes and ears of the strategy team. Team members may be viewed as "social media scouts," observing, monitoring, and collecting information on the state of the online community in the AOR. The monitoring team represents a systematic way to take advantage of the content and trends in the social media. Without a systematic approach, there may be little chance of making accurate observations and drawing the correct conclusions from the online traffic in the AOR. If every staff section were to independently monitor Facebook, Twitter, YouTube, or the local language versions of social networks and blogs, without lateral coordination within the staff, there will likely be significant gaps in the monitoring of the social media environment.

The monitoring team should contain broad staff representation to be effective. The team will require members with local language skills, cultural understanding, and a high degree of familiarity with the social media tools and protocols. To be effective, they will need to conduct field research in the AOR. They will also need to observe the Internet cafes and local habits in the AOR and become familiar with the social media platforms popular in the culture.

The fourth way to ensure success in a social media strategy is to find a balance between security and sharing. The information security concerns over experimentation of social software on Department of Defense (DOD) computers are not trivial. Security officers will be inclined to say no to extensive use of social media on networks that are used for official purposes.[14] There is considerable discussion within DOD on this issue. The Services have significant disagreement on the right level of access to allow, balanced against the need for security. The DOD policy released on February 25, 2010, directs that "the NIPRNET [unclassified networks] shall be configured to provide access to Internet-based capabilities across all DoD Components."[15] The policy goes on to give the components significant latitude to limit access to defend against malicious activity when needed. There may be ways of using firewalls or separated networks to ensure security of information while still benefiting from the use of social media. Each command will have to weigh this balance and make the decision based on its needs.

Since speed and agility are key elements of successful social media strategy, the fifth way to enhance success in a strategy is to enact policies to allow the social media campaign to be agile. Restrictive and cumbersome approval chains may inhibit the ability of the operators to achieve results. Perhaps the best approach is to allow for centralized planning and decentralized execution.[16] The enemy will not be constrained from posting information to the Internet by a cumbersome approval process and thus has the ability to act very quickly. Operation *Valhalla* in Iraq in 2006 provides an illustrative example.

During a successful firefight against the Jaish al-Mahdi (JAM) forces, U.S. Special Forces and Iraqi forces killed a number of enemy fighters, rescued a hostage, and destroyed a weapons cache—by all measures, a very successful operation. By the time U.S. and Iraqi forces returned to their base, someone had repositioned the bodies and removed the weapons of the JAM fighters so it looked like they were murdered while at prayer. They photographed the bodies in these new poses and uploaded the images onto the Internet, along with a press release explaining that American Soldiers killed the men while they were in a mosque. All this took the enemy less than an hour. The public reaction was predictably negative. The U.S. forces had a combat camera crew with them during the operation, and some of the Soldiers wore helmet cameras. U.S. forces were in possession of the evidence to disprove the claims, but a cumbersome and highly centralized process for releasing information prevented the correct story from reaching the media for nearly 3 days. By the time U.S. forces released the correct version of Operation *Valhalla*, the strategic damage was done.[17] The inability to react immediately to the enemy claims in the previous example was largely for policy reasons. To promote agility, the U.S. military's policies must allow for decentralized execution of operations involving new media.

Decentralization of execution, however, may force commanders to accept levels of risk with which they may not be comfortable. The commander will essentially delegate the control of information releasing authority to low levels. Clear rules of engagement distributed to all the potential social media operators may be able to mitigate the risks. The need for agility will often conflict with the need to carefully control the strategic message.[18]

One of the key elements for commanders to enhance agility in their social media program is to allow and encourage social media operations to be executed even at the lowest unit level. Many of the closest relationships established in an AOR are formed at battalion level and below. Local government leaders, tribal leaders, police, and militias are all developing relationships at the very lowest levels. The leaders at these units will know how best to interface with the population. Web sites, blogs, and links to Facebook pages can be used for nearby activities. In Africa, there are examples of local groups reporting tactical information such as roadblocks and ambushes to Web sites set up by State Department teams. The site then consolidates them onto a map for locals to check when they are traveling.[19] Commanders may be able to enhance local relationships with the positive use of social media at the unit level.

The sixth and final way in which a commander can take advantage of social media is to set up social networking sites as an outreach tool to enhance unity of effort. As General Petraeus mentioned in his guidance, there are a number of key partners in theater with whom units must cooperate. Seemingly simple efforts such as establishing a Facebook page could allow partner organizations a better understanding of the commander's intent. Joint Task Force–Haiti, supporting relief operations in the aftermath of the January 2010 earthquake, has effectively used social media as a tool for outreach to other organizations engaged in the effort.

There are numerous key relationships in the AOR relative to social media strategy. The obvious ones are local governments, press, civic organizations, and the populace in general, as well as NGOs operating in the area. Commanders should also consider outreach to the blogger community (if there is one), businesses, Internet service providers, and cellular network providers. These relationships would better enable the social media program to be effective and adaptable to changes.

## The Means

The final component in the development of a strategy is the identification of the means. The *means* are the resources available to pursue the objectives. Fortunately, in the U.S. military today, the means to conduct an effective social media strategy are readily available. To employ the strategy listed above, there may be a requirement to reorganize and reprioritize resources within deployed headquarters as described in the discussion of the ways, but there will be no wholly new skills or equipment required.

Some of the key means are the individual talents and skills of Servicemembers. Skilled information operators, PA specialists, and intelligence collectors and analysts are already conducting operations at all levels and in all Services. Language and cultural skills will continue to be a critical factor in our ability to conduct operations around the world. When engaging with social media, operators trained to function effectively in the cultures in which we are operating will be vital assets. The "digital natives" will be critical to success in the social media environment as well. The authors of a report from the "New Media and the Warfighter" workshop held at the U.S. Army War College define *digital natives* as "those young service members who are savvy in the use of new media devices, platforms, networks, and possibilities—and are underexploited assets in the information-led wars against new adversaries."[20] Employing these younger and more tech-savvy operators in roles that will have strategic impact requires some change to the traditional hierarchical mindset. The bright and talented personnel will continue to be the foundation for success.

These digital natives, however, may lack the strategic insight and understanding of more senior strategists and planners, who will have to provide clear guidance and oversight to ensure the actions of the digital natives match the strategic intent of the commander. For the relationship between the leaders and the operators to work, senior leaders must have an understanding of the capabilities and limitations of social media. Social media may be one case where the senior leaders must be trained to have an understanding of what the soldiers and junior officers already know. Inclusion of an introduction to social media into commanders' courses may be an appropriate initiative.

Finally, the military's ties with academia and industry will be more important than ever. These relationships have already been established. DOD has some effective ties with the blogger community and with many companies engaged throughout the social media community. The relationships DOD enjoys today will have to continue to grow in order to ensure the success of any social media strategy.

Social media and new media are changing the ways information moves around the world. Speed and transparency of information have increased, the roles of traditional and new media are changing, and social networking tools allow collaboration as never seen before. There will no doubt be changes to the nature of conflicts as a result. A key to successfully adapting to the changes will be commanders' ability to develop strategies that take advantage of the changes and deny the enemy exclusive rights to the same. The U.S. military has the tools available to perform the tasks inherent in a strategy that will allow it to capitalize on the emerging trends in information. An innovative strategy that incorporates the lessons already learned in the social media environment will allow the Armed Forces to improve their ability to understand the environment, communicate more effectively, and generate unity of effort throughout the battlefield. **JFQ**

### NOTES

[1] "'Neda' Becomes Rallying Cry for Iranian Protests," CNN.com/World, June 22, 2009.

[2] "16 Azar Green Routes," UnitedForIran, December 6, 2009, available at <www.flickr.com/photos/united4iran/4165827330/>. This site provides an example of social media tools used to share information among the Iranian protestors.

[3] Huda al Saleh, "Al-Qaeda Continues Using Modern Technology to Recruit Youth," January 5, 2010, accessed at <http://aawsat.com/english>.

[4] William B. Caldwell, Denis M. Murphy, and Anton Menning, "Learning to Leverage New Media: The Israeli Defense Forces in Recent Conflicts," *Military Review* (May–June 2009), 2–10.

[5] Ibid.

[6] Robert H. Dorff, "A Primer in Strategy Development," in *U.S. Army War College Guide to Strategy*, ed. Joseph R. Cerami and James F. Holcomb (Carlisle, PA: Strategic Studies Institute, 2001), 11–18.

[7] The Social Media Hub, Department of State Office of Innovative Engagement, available at <https://www.intelink.gov/communities/state/smp/>.

[8] David H. Petraeus, "Multi-National Force Commander's Counterinsurgency Guidance," *Military Review* (September–October 2008), 210–212.

[9] Ibid.

[10] Ibid.

[11] Dorff, 11.

[12] Catharine P. Taylor, "Eight Ways to Ruin Your Social-Media Strategy," available at <www.bnet.com/2403-13237_23-366324.html?tag=content;btmTier>.

[13] *Commander's Handbook for Strategic Communication* (Norfolk, VA: U.S. Joint Forces Command, Joint Warfighting Center, 2008), III–4.

[14] Mark Drapeau and Linton Wells II, *Social Software and National Security: An Initial Net Assessment*, Defense and Technology Paper 61 (Washington, DC: Center for Technology and National Security Policy, 2009).

[15] Department of Defense, "Directive-Type Memorandum (DTM) 09–026—Responsible and Effective Use of Internet-based Capabilities," Washington, DC, Februrary 25, 2010.

[16] Rafal Rohozinski and Dierdre Collings, *Bullets and Blogs: The New Media and the Warfighter* (Carlisle, PA: Center for Strategic Leadership, U.S. Army War College, 2008).

[17] Cori E. Dauber, "The Truth is Out There: Responding to Insurgent Disinformation and Deception Operations," *Military Review* (January–February 2009), 13–24.

[18] Rohozinski and Collings.

[19] Kimberly Harrington, Department of State, Office of Innovative Engagement, interview by author, Washington, DC, November 19, 2009.

[20] Rohozinski and Collings.

# U.S. Army War College
# STRATEGIC LANDPOWER
## *Essay Contest 2011*

The United States Army War College and the United States Army War College Foundation are pleased to announce the annual **STRATEGIC LANDPOWER** Essay Contest.

The topic of the essay must relate to the strategic use of landpower. A specific topic of interest, for this year's contest is the application of design in conflict termination.

Anyone is eligible to enter and win except those involved in the judging. The Army War College Foundation will award a prize of $4000 to the author of the best essay and a prize of $1000 to the second place winner.

For more information or for a copy of the essay contest rules, contact:
Dr. Michael R. Matheny, U.S. Army War College, Department of Military Strategy, Planning and Operations, 122 Forbes Avenue, Carlisle, PA 17013-5242 (717) 245-3459, DSN 242-3459, michael.matheny@us.army.mil

**STRATEGIC LANDPOWER Essay Contest Rules:**

1. Essays must be original, not to exceed 5000 words, and must not have been previously published. An exact word count must appear on the title page.

2. All entries should be directed to: Dr. **Michael R. Matheny, USAWC Strategic Landpower Essay Contest, U.S. Army War College, Department of Military Strategy, Planning and Operations, 122 Forbes Avenue, Carlisle, PA 17013-5242.**

3. **Essays must be postmarked on or before 17 February 2011.**

4. The name of the author shall not appear on the essay. Each author will assign a codename in addition to a title to the essay. This codename shall appear: (a) on the title page of the essay, with the title in lieu of the author's name, and (b) by itself on the outside of an accompanying sealed envelope. This sealed envelope should contain a typed sheet giving the name, rank/title, branch of service (if applicable), biographical sketch, address, and office and home phone numbers (if available) of the essayist, along with the title of the essay and the codename. This envelope will not be opened until after the final selections are made and the identity of the essayist will not be known by the selection committee.

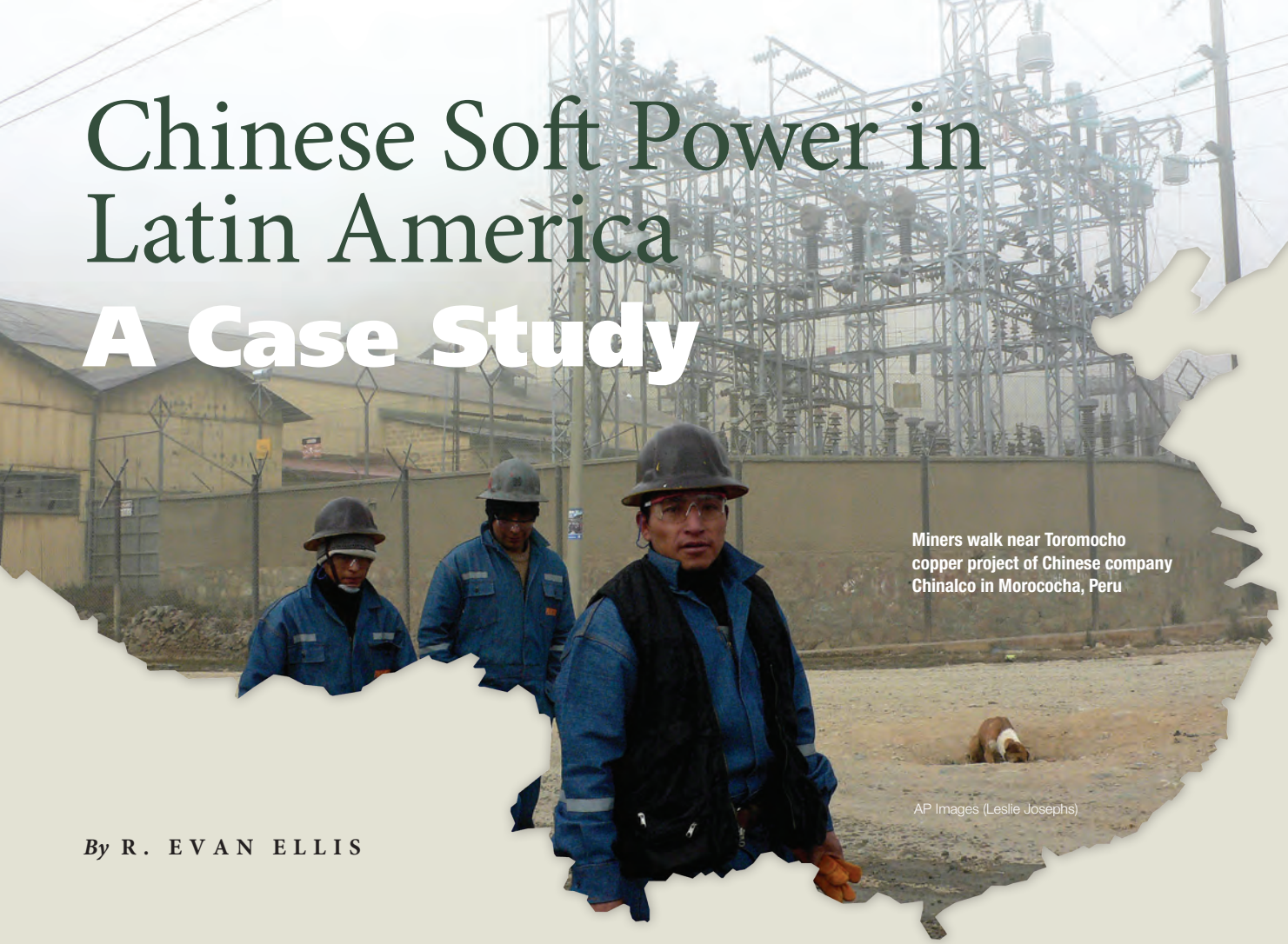
5. All essays must be typewritten, double-spaced, on paper approximately 8 ½" x 11". Submit two complete copies. If prepared on a computer, please also submit the entry on a disk, indicating specific word-processing software used.

6. The award winners will be notified in early Spring 2011. Letters notifying all other entrants will be mailed by 1 April 2011.

7. The author of the best essay will receive $4000 from the U.S. Army War College Foundation. A separate prize of $1000 will be awarded to the author of the second best essay.

# Chinese Soft Power in Latin America

## A Case Study



Miners walk near Toromocho copper project of Chinese company Chinalco in Morococha, Peru

AP Images (Leslie Josephs)

*By* R. EVAN ELLIS

The reemergence of China as a dominant global actor highlights longstanding ambiguities in U.S. thinking regarding what constitutes national security. People's Republic of China (PRC) policymakers have emphasized the "peaceful" nature of China's rise and have generally avoided military or political actions that could be seen by the United States as "threatening." Nonetheless, the economic, institutional, and cultural battles through which the PRC has advanced its position have both leveraged and contributed to an erosion of the U.S. strategic position globally. The advance of China and the multidimensional strategic challenge that it poses are most effectively characterized by one of the most loosely defined and misunderstood buzzwords in the modern parlance: soft power.

**R. Evan Ellis is an Assistant Professor of National Security Studies in the Center for Hemispheric Defense Studies at the National Defense University.**

The concept of *soft power* was introduced in 1990 by Harvard Professor Joseph Nye, who defined it as "a dynamic created by a nation whereby other nations seek to imitate that nation, become closer to that nation, and align its interests accordingly."[1] Although the term is used to refer to a range of concepts, this article analyzes Chinese soft power in terms of the willingness of governments and other actors in the international system to orient themselves and behave in ways that benefit the PRC because they believe doing so to be in their own interests.

Such a definition, by necessity, is incomplete. There are many reasons why other actors may decide that actions beneficial to the PRC are also in their own interests: they may feel an affinity for the Chinese culture and people and the objectives of its government, they may expect to receive economic or political benefits from such actions, or they may even calculate that the costs or risks of "going against" the PRC are simply too great.

Soft power is a compelling concept, yet it operates through vaguely defined mechanisms. In the words of Nye, "in a global information age . . . success depends not only on whose army wins, but on whose story wins."[2] The implications of soft power in the contemporary environment are difficult to evaluate because they involve a complex web of interconnected effects and feedback in which the ultimate results of an action go far beyond the initial stimulus and the ultimate importance of an influence goes far beyond what is initially apparent.

This article examines Chinese soft power in the specific context of Latin America. The United States has long exercised significant influence in the region, while the PRC has historically been relatively absent. Nonetheless, in recent years, China's economic footprint in Latin America, and its attempts to engage the region politically, culturally, and otherwise, has expanded enormously. Understanding the nature and limits of PRC soft power in Latin America casts light on Chinese soft power in other parts of the world as well.

AP Images (Sven Creutzmann)

**Chinese President Hu Jintao and Cuban President Raul Castro watch signing of treaties in Havana after Hu signed dozens of trade and investment deals with Cuba**

## The Nature of Chinese Soft Power

In general, the bases of Chinese soft power differ from those of the United States, leading analysts to underestimate that power when they compare the PRC to the United States on those factors that are the sources of U.S. influence, such as the affinity of the world's youth for American music, media, and lifestyle, the widespread use of the English language in business and technology, or the number of elites who have learned their professions in U.S. institutions.

It is also important to clarify that soft power is based on perceptions and emotion (that is, inferences), and not necessarily on objective reality. Although China's current trade with and investment position in Latin America are still limited compared to those of the United States,[3] its influence in the region is based not so much on the current size of those activities, but rather on hopes or fears in the region of what it could be in the future.

Because perception drives soft power, the nature of the PRC impact on each country in Latin America is shaped by its particular situation, hopes, fears, and prevailing ideology. The "Bolivarian socialist" regime of Hugo Chávez in Venezuela sees China as a powerful ally in its crusade against Western "imperialism," while countries such as Peru, Chile, and Colombia view the PRC in more traditional terms as an important investor and trading partner within the context of global free market capitalism.

The core of Chinese soft power in Latin America, as in the rest of the world, is the widespread perception that the PRC, because of its sustained high rates of economic growth and technology development, will present tremendous business opportunities in the future, and will be a power to be reckoned with globally. In general, this perception can be divided into seven areas:

- hopes for future access to Chinese markets
- hopes for future Chinese investment
- influence of Chinese entities and infrastructure in Latin America
- hopes for the PRC to serve as a counterweight to the United States and Western institutions
- China as a development model
- affinity for Chinese culture and work ethic
- China as "the wave of the future."

In each of these cases, the soft power of the PRC can be identified as operating through distinct sets of actors: the political leadership of countries, the business community, students and youth, and the general population.

***Hopes for Future Access to Chinese Markets.*** Despite China's impressive rates of sustained growth, only a small fraction of its population of 1.3 billion is part of the "modern" economy with the resources that allow them to purchase Western goods. Estimates of the size of the Chinese middle class range from 100 million to 150 million people, depending on the income threshold used, although the number continues to expand rapidly.[4] While selling to Chinese markets is a difficult and expensive proposition, the sheer number of potential consumers inspires great aspirations among Latin American businesspeople, students, and government officials. The Ecuadorian banana magnate Segundo Wong, for example, reportedly stated that if each Chinese would eat just one Ecuadorian banana per week, Ecuador would be a wealthy country. Similar expressions can be found in many other Latin American countries as well.

In the commodities sector, Latin American exports have expanded dramatically in recent years, including Chilean copper, Brazilian iron, and Venezuelan petroleum. In Argentina, Chinese demand gave rise to an entire new export-oriented soy industry where none previously existed. During the 2009 global recession, Chinese demand for commodities, based in part on a massive Chinese stimulus package oriented toward building infrastructure, was perceived as critical for extractive industries throughout Latin America, as demand from traditional export markets such as the United States and Europe fell off.

Beyond commodities, certain internationally recognized Latin American brands, such as José Cuervo, Café Britt, Bimbo, Modelo, Pollo Campero, and Jamaican Blue Mountain coffee, sell to the new Chinese middle class, which is open to leveraging its new wealth to "sample" the culture and cuisine of the rest of the world. Unfortunately, most products that Latin America has available to export, including light manufactures and traditional products such as coffee and tropical fruits, are relatively uncompetitive in China and subject to multiple formal and informal barriers to entry.

Despite the rift between hopes and reality, the influence of China in this arena can be measured in terms of the multitude of business owners who are willing to invest millions of dollars and countless hours of their time and operate in China at a loss for years, based on the belief that the future of their corporations depends on successfully positioning themselves within the emerging Chinese market.

The hopes of selling products to China have also exerted a powerful impact on politi-

cal leaders seeking to advance the development of their nations. Chilean presidents Ricardo Lagos and Michelle Bachelet, for example, made Sino-Chilean trade relations the cornerstone of Chile's economic policy, signing the first free-trade pact between the PRC and a Latin American nation in November 2005. Peruvian president Alan Garcia made similar efforts to showcase that nation as a bridge to China when it hosted the Asia Pacific Economic Cooperation summit in November 2008. Governments in the region have also invested significant sums of money in the China-related activities of trade promotion organizations such as APEX (Brazil), ProChile, ProComer (Costa Rica), Fundación Exportar (Argentina), and CORPEI (Ecuador), among others, as well as representative offices in Beijing, Shanghai, Guangzhou, and other Chinese cities, with the objective of helping their nationals to place products in those countries. Latin American leaders, from presidents to mayors, lead delegations to the PRC and fund elaborate pavilions in Chinese culture and trade shows such as the Canton Trade Fair and the Shanghai World Expo in an effort to help their countries' businesses sell products in the PRC.

***Hopes for Future Chinese Investment.*** China's combination of massive sustained trade surpluses and high internal savings rates gives the PRC significant resources that many in Latin America hope will be invested in their countries. Chinese president Hu Jintao helped to generate widespread awareness of the possibility of Chinese investment in the region during his trip to five Latin American countries in 2004, specifically mentioning tens of billions of dollars in possible investment projects. A public controversy over whether his use of the figure $100 billion was actually referring to trade or investment has only called more attention in Latin America to China as a potential source of funds.

Although the expected Chinese investment was initially slow to materialize, today, thanks to China's growing familiarity with doing business in Latin America, and its enormous financial reserves (including a foreign currency surplus that had reached $2.5 trillion by mid-2010[5]), the PRC has begun to loan, or invest, tens of billions of dollars in the region, including in high-profile deals such as:

- $28 billion in loans to Venezuela; $16.3 billion commitment to develop the Junin-4 oil block in Venezuela's Orinoco oil belt
- $10 billion to Argentina to modernize its rail system; $3.1 billion to purchase the Argentine petroleum company Bridas
- $1 billion advance payment to Ecuador for petroleum, and another $1.7 billion for a hydroelectric project, with negotiations under way for $3 billion to $5 billion in additional investments
- more than $4.4 billion in commitments to develop Peruvian mines, including Toromocho, Rio Blanco, Galleno, and Marcona
- $5 billion steel plant in the Brazilian port of Açu, and another $3.1 billion to purchase a stake in Brazilian offshore oil blocks from the Norwegian company Statoil; a $10 billion loan to Brazil's Petrobras for the development of its offshore oil reserves; and $1.7 billion to purchase seven Brazilian power companies.

For Latin America, the timing of the arrival of the Chinese capital magnified its impact, with major deals ramping up in 2009, at a time when many traditional funding sources in the region were frozen because of the global financial crisis. Moreover, as Sergio Gabrielli, president of the Brazilian national oil company Petrobras has commented, China is able to negotiate large deals, integrating government and private sector activities in ways that U.S. investors cannot.[6]

*China is able to negotiate large deals, integrating government and private sector activities in ways that U.S. investors cannot*

***Influence of Chinese Entities and Infrastructure in Latin America.*** Although the presence of Chinese corporations and workers in Latin America pales by comparison to that of the United States, it is growing and exerting an increasing weight in select countries.

Particularly in states such as Ecuador and Venezuela, Chinese corporations are becoming increasingly critical for the functioning of the extractive industries that generate significant portions of the state's revenue. In Ecuador, Chinese petroleum and service companies directly operate seven oil blocks, are a partner in others through consortiums, and account for almost 40 percent of nonstate oil production, while China Railway Road and Tongling are ramping up for a $3 billion project in the recently opened Ecuadorian mining sector. In Venezuela, Chinese companies are one of the key actors maintaining oil production in the mature oilfields of Maracaibo and Anzoátegui, a vital current revenue stream for the Chávez regime. In the Orinoco belt in the south of Venezuela, Chinese investment, technology, and manpower, including Chinese-made drilling rigs, are a key to the development of that nation's future oil potential, while a May 2010 agreement makes Chinese companies key players in the extraction of Venezuelan iron, gold, bauxite, and coal.[7]

Although Chinese companies have yet to attain the level of "key employers" or have a major role in many Latin American communities, they play a growing role in strategically important sectors in many Latin American countries. For example, in telecommunications, the Chinese companies Huawei and ZTE are increasingly important product, service, and infrastructure providers,[8] and in logistics, companies such as China Shipping, China Overseas Shipping, and Hutchison Whampoa play increasingly vital roles in Latin America's foreign trade.

Ironically, Latin American Chinese communities have played a relatively limited role in this expanding influence. Although there are large, historically rooted Chinese communities in countries such as Peru, Ecuador, Panama, and Brazil, Chinese immigrants have traditionally sought to keep a low profile in these societies. The structure of these communities has also served to channel new Chinese immigrants into certain traditional occupations, such as restaurants, the retail sector, or farming, with the result that ethnic Chinese today have a fairly narrow involvement in emerging China–Latin America trade, even in key hubs for trade such as Colón, Iquique, or Ciudad del Este.

Beyond business ties, the PRC has an important and growing presence in the region's military institutions. In addition to frequent visits by senior-level officers and defense leaders, Mexico and almost all of the countries of South America send officers to professional military education courses in the PRC, including a 5-month course for midgrade officers taught in Spanish in Beijing. Chinese-made clothing and nonlethal equipment are also becoming increasingly common

within Latin American militaries. In addition, thanks to opportunities provided by the regimes of Ecuador, Venezuela, and Bolivia, the PRC has begun to sell sophisticated hardware in the region, such as radars and K–8 and MA–60 aircraft. As happened in commercial industries such as motorcycles, cars, and consumer appliances, Chinese military goods companies such as Norinco are likely to leverage their experience and a growing track record for their goods to expand their market share in the region, with the secondary consequence being that those purchasers will become more reliant on the associated Chinese logistics, maintenance, and training infrastructures that support those products.

Beyond Chinese corporations and military ties, the PRC is also taking on a progressively important role in regional institutions, such as the Organization of American States (OAS), Inter-American Development Bank (IADB), and United Nations peacekeeping operations in Haiti. Although the PRC has only observer status in the OAS, for example, its delegation is a strong contributor to the activities of the body.[9] With respect to the IADB, China has leveraged its seat at the table as an opening for doing business in the region, such as the $10.2 billion currency swap with Argentina, which it signed on the sideline of the IADB's annual meeting in March 2009. Also, through its initial financial contribution to the IADB, the PRC became part of a special committee overseeing loans to highly impoverished countries in the region, affording it expanded contacts with and subtle pressures over countries that do not currently recognize the PRC diplomatically, including Haiti, Honduras, and Nicaragua. In the case of Haiti, Chinese leverage is further bolstered by having had police forces on the ground there since 2006, through PRC participation in the United Nations Stabilization Mission in Haiti.[10]

***Hopes for the PRC to Serve as a Counterweight to the United States and Western Institutions.*** China's historical status as a "leader of the developing world" positions it as the natural ally of the new generation of Latin American populist leaders, such as Hugo Chávez, Rafael Correa, and Evo Morales. During his first trip to Beijing after being elected president, for example, Morales proclaimed himself to be a "great admirer of Mao," while Chávez has exclaimed that Mao and South American revolutionary icon Simón Bolívar would have been "great friends." While these leaders may primarily be seeking Chinese investments and commodity purchases, the position of the PRC as a geopolitical "alternative" to the United States shapes the way that they court the Chinese.

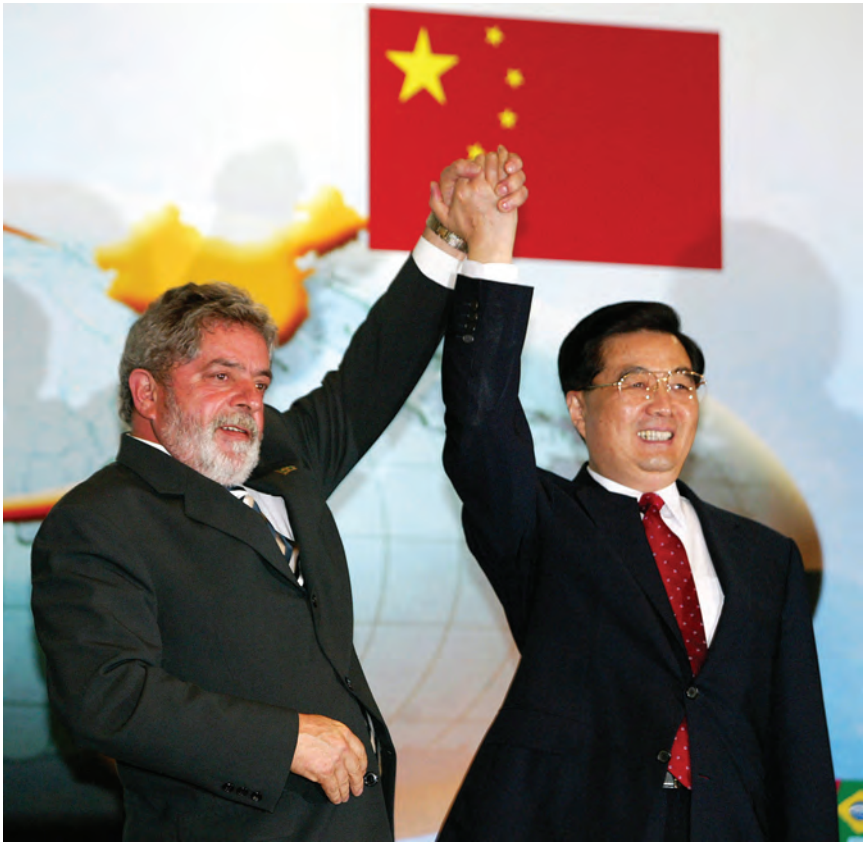
In permitting such hopes, the PRC has, to date, been careful not to associate itself directly with the anti-U.S. activities or rhetoric of these regimes, so as not to damage its strategically important relationship with the United States and the West. Nonetheless, the relationship cannot avoid some flavor of the relationships between the Soviet Union and its Latin American client states during the Cold War. Bolivia turned to China to purchase K–8 combat aircraft, for example, after the United States blocked its ability to procure aircraft from the Czech Republic.[11]

***China as a Development Model.*** The tremendous, sustained economic growth that the PRC has enjoyed since opening up to the world in 1978 has caused many in Latin America to look to China's integration of capitalism and authoritarian politics as a development model, even while the U.S. combination of liberal democracy, free markets, and privatization is increasingly seen as ineffective for solving the region's endemic problems, such as corruption, poverty, and inequality. For traditional Latin American elites, the Chinese model is particularly attractive because it suggests that it is possible to achieve prosperity and growth without relinquishing political power.

As with other Chinese sources of soft power, the impact of the "Beijing Consensus" in Latin America relies on perceptions rather than realities; differences between the two regions—including the relative submission to authority in the Chinese work culture, Chinese willingness to save rather than spend, and another part of the world serving as the market for Chinese exports—make the Chinese success story difficult to repeat in Latin America.

***Affinity for Chinese Culture.*** The PRC has actively promoted Chinese culture and language throughout the world, including through such landmark events as the 2008 Olympics in Beijing and 2010 World Expo in Shanghai, visited by an estimated 5 million foreign tourists,[12] as well as establishing more

AP Images (Adriano Machado)



**Brazilian President Luiz Inacio Lula da Silva and Chinese President Hu Jintao celebrate at closing of investment and trade seminar**

than 282 Confucius institutes worldwide, including 20 in Latin America. Cultural exchanges are a featured part of China's dealings with Latin America, consistent with the "nonthreatening" character that Beijing wishes to emphasize in these interactions.

Despite PRC "marketing efforts," by contrast to the global impact of U.S. culture, Chinese culture is arguably one of the PRC's weakest levers of soft power in Latin America, with interest in Chinese culture arguably reflecting, more than driving, China's influence in the region. Although some Chinese culture is reaching the Latin American mainstream, perceptions of it in Latin America are generally limited and superficial, sometimes based on media reports or experiences with ethnic Chinese living in those countries. Such perceptions are often mixed, including respect for the Chinese work ethic, a sense of mystery regarding Chinese culture, and often a sense of mistrust arising from the perceived differentness of that culture and commercial competition from Chinese products.

***China as "the Wave of the Future."*** Perhaps China's greatest source of soft power is the most intangible. China's emergence as a key global player is a phenomenon that has assumed almost mystical proportions within Latin America. The rapid growth in PRC trade with and investment in Latin America, and the expansion of contacts at all levels, only reinforce the perceived significance of "China's rise," as observed from Latin America.

In addition to opportunism for commerce, Latin America's belief in the rise of China and its globally transformational implications draws the attention of the people and leaders of the region to the PRC and shapes their course of action. Costa Rican president Oscar Arias, for example, established regular diplomatic relations with the PRC as a necessary part of ensuring the relevance of his country as an international actor.

At the popular level, the rise of China is most likely behind a swelling interest in the Chinese language in the region. The dedication of 5 or more years by students to gain a basic capability in the Mandarin language and its character set, for example, is arguably driven by their calculation that the ability to communicate in Chinese will be fundamental to the pursuit of opportunities in the PRC, and with Chinese businessmen and government officials, in the future.

## Use of Chinese Soft Power

One of the most important questions associated with the rise of China is how it is likely to use its growing soft power. Although such an endeavor is, by nature, speculative, Chinese interests and patterns of behavior to date suggest the continued use of that influence in at least the following areas:

- diplomatic recognition of Taiwan
- access to Latin American markets
- protection of Chinese investments in and trade flows from the region
- protection of Chinese nationals
- working against the consolidation of U.S. influence in the region and its institutions.

Although the Chinese government repeatedly states its commitment to noninterference in the internal affairs of partner nations, in reality the PRC is as interested in such issues as any other outside country. Only the issues that the PRC focuses on, and the ways in which China applies pressure, differ.

***Diplomatic Recognition of Taiwan.*** For the PRC, the government of Taiwan represents an important issue of political legitimacy and internal security. Currently, 12 of the 23 nations in the world that diplomatically recognize the government of Taiwan are found in Latin America and the Caribbean. Although the People's Republic of China does not publicly threaten to block investment in or loans to countries that do not recognize the PRC, China repeatedly emphasizes the issue in its public diplomacy in the region, and makes such investments and market access difficult for those countries that do not recognize it, while simultaneously nurturing expectations regarding the opportunities that diplomatically recognizing the PRC could bring. When Costa Rica changed its diplomatic recognition from Taiwan to the PRC in May 2007, for example, it received an aid package that included an $83 million soccer stadium, the purchase of $300 million in government bonds, various highway, public works, and aid projects, and a $1 billion joint venture to expand the country's petroleum refinery, as well as PRC aid in facilitating access to Chinese markets by traditional Costa Rican products such as coffee. In part, such Chinese generosity was directed toward the other countries in the region that still recognized Taiwan in order to demonstrate the types of benefits that could be made available if they too were to change their diplomatic posture.[13]

Although the PRC and Taiwan have informally agreed to refrain from the use of economic incentives to competitively "bid" for diplomatic recognition, since Costa Rica's switch, the allure of the PRC has prompted declarations of interest in changing diplomatic posture by Panamanian president Richard Martenelli, Paraguayan president Fernando Lugo, and Salvadoran president Maricio Fuenes—although all did so prior to assuming office.

***Access to Latin American Markets.*** Latin American markets are becoming increasingly valuable for Chinese companies because they allow the PRC to expand and diversify its export base at a time when economic growth is slowing in traditional markets such as the United States and Europe. The region has also proven an effective market for Chinese efforts to sell more sophisticated, higher value added products in sectors seen as strategic, such as automobiles, appliances, computers and telecommunication equipment, and aircraft. In expanding access for its products through free trade accords with countries such as Chile, Peru, and Costa Rica, and penetrating markets in Latin American countries with existing manufacturing sectors such as Mexico, Brazil, and Argentina, the PRC has often had to overcome resistance by organized and often politically well-connected established interests in those nations. In doing so, the hopes of access to Chinese markets and investments among key groups of businesspeople and government officials in those nations have played a key role in the political will to overcome the resistance. In Venezuela, it was said that the prior Chinese ambassador to Venezuela, Zheng Tuo, was one of the few people in the country who could call President Chávez on the telephone and get an instant response if an issue arose regarding a Chinese company.

***Protection of Chinese Investments in and Trade Flows from the Region.*** At times, China has applied more explicit pressures to induce Latin America to keep its markets open to Chinese goods. It has specifically protested measures by the Argentine and Mexican governments that it has seen as protectionist: and, in the case of Argentina, as informal retaliation, China began enforcing a longstanding phytosanitary regulation, causing almost $2 billion in lost soy exports and other damages for Argentina.[14]

China has also used its economic weight to help secure major projects on preferential

terms. In the course of negotiating a $1.7 billion loan deal for the Coco Coda Sinclair Hydroelectric plant in Ecuador, the ability of the Chinese bidder SinoHidro to self-finance 85 percent of the projects through Chinese banks helped it to work around the traditional Ecuadorian requirement that the project have a local partner. Later, the Ecuadorian government publicly and bitterly broke off negotiations with the Chinese, only to return to the bargaining table 2 months later after failing to find satisfactory alternatives. In Venezuela, the Chávez government agreed, for example, to accept half of the $20 billion loaned to it by the PRC in Chinese currency, and to use part of that currency to buy 229,000 consumer appliances from the Chinese manufacturer Haier for resale to the Venezuelan people. In another deal, the PRC loaned Venezuela $300 million to start a regional airline, but as part of the deal, required Venezuela to purchase the planes from a Chinese company.[15]

***Protection of Chinese Nationals.*** As with the United States and other Western countries, as China becomes more involved in business and other operations in Latin America, an increasing number of its nationals will be vulnerable to hazards common to the region, such as kidnapping, crime, protests, and related problems. The heightened presence of Chinese petroleum companies in the northern jungle region of Ecuador, for example, has been associated with a series of problems, including the takeover of an oilfield operated by the Andes petroleum consortium in Tarapoa in November 2006, and protests in Orellana related to a labor dispute with the Chinese company Petroriental in 2007 that resulted in the death of more than 35 police officers and forced the declaration of a national state of emergency. In 2004, ethnic Chinese shopkeepers in Valencia and Maracay, Venezuela, became the focus of violent protests associated with the Venezuelan recall referendum.

As such incidents increase, the PRC will need to rely increasingly on a combination of goodwill and fear to deter action against its personnel, as well as its influence with governments of the region, to resolve such problems when they occur.

***Blocking the Consolidation of U.S. Influence in the Region and Its Institutions.*** The rise of China is intimately tied to the global economy through trade, financial, and information flows, each of which is highly dependent on global institutions and cooperation. Because of this, some within the PRC leadership see the country's sustained growth and development, and thus the stability of the regime, threatened if an actor such as the United States is able to limit that cooperation or block global institutions from supporting Chinese interests.

*one of the most significant barriers between the PRC and Latin America is language*

In Latin America, China's attainment of observer status in the OAS in 2004 and its acceptance into the IADB in 2009 were efforts to obtain a seat at the table in key regional institutions, and to keep them from being used "against" Chinese interests. In addition, the PRC has leveraged hopes of access to Chinese markets by Chile, Peru, and Costa Rica to secure bilateral free trade agreements, whose practical effect is to move Latin America away from a U.S.-dominated trading block (the Free Trade Area of the Americas) in which the PRC would have been disadvantaged.

Finally, the PRC benefits from the challenges posed to the dominance of the United States in the region by regimes such as Venezuela, Ecuador, and Bolivia, and its trade and investment with those regimes help to keep them economically viable. Nonetheless, as mentioned above, the PRC is careful to avoid association with the anti-U.S. rhetoric and projects of those regimes, which could damage its more strategically important relationship with the United States.

## Limits to Chinese Soft Power

The growth and exercise of soft power by the People's Republic of China have limits that are important to recognize. As with the sources of Chinese soft power, those limits are not the same as the limits to U.S. soft power. Limits to Chinese soft power in Latin America principally arise from the significant gap between the two cultures, the associated difficulty in learning each other's culture and language, a lack of understanding of each side by the other, and a pervasive sense of mistrust of the Chinese within Latin America generally.

The cultural gap between China and Latin America touches upon many areas, from differing consumer preferences limiting the appeal of Latin American exports such as coffee and beef, to different attitudes toward authority in business and administrative dealings, which contribute to labor problems and other difficulties where the PRC has operated in Latin America.

One of the most significant barriers between the PRC and Latin America is language. Whereas a relatively significant portion of Latin Americans have some ability in English, very few speak or read Chinese, and even fewer Chinese can communicate in Spanish, although the number is growing.[16] Although Chinese-language programs are proliferating in Latin America, the difficulty of and time required for learning Mandarin and the Chinese character set are a powerful impediment to the growth of ties between the two cultures.

Compounding the language barrier is a relative lack of Chinese knowledge regarding Latin America. Apart from major governmental institutes—such as the China Academy of Social Sciences, which currently has the world's largest Latin America studies program—and truly multinational Chinese corporations—such as Hong Kong–based Hutchison Whampoa, China Shipping, China Overseas Shipping, Huawei, and ZTE—the general knowledge of the region among Chinese businesspeople and government functionaries is limited, restricting the ability of the PRC to develop broad and sophisticated programs to advance its objectives in the region.

Perhaps most importantly, despite the best efforts of Chinese businesspeople and politicians to reach out to Latin America, they are too frequently perceived as "not one of us"—a reality reflected even in Chinese communities, which often remain only partly integrated, despite deep historical roots in many Latin American cities such as Lima and Guayaquil.

Such distance often translates into a persistent mistrust, even where both sides perceive benefits from cooperation. Latin American businesspeople commonly express misgivings, suggesting that the Chinese are aggressive and manipulative in business dealings, or conceal hidden agendas behind their expressions of friendship and goodwill.

AP Images/Imaginechina


**Venezuelan officials bury foundation stone at groundbreaking for Venezuela Pavilion at Shanghai World Expo 2010**

Chinese companies in Latin America are often seen as poor corporate citizens, reserving the best jobs and subcontracts for their own nationals, treating workers harshly, and maintaining poor relations with the local community. In the arena of China–Latin America military exchanges, it is interesting to note that Latin American military officers participating in such programs are often jokingly stigmatized by their colleagues in ways that officers participating in exchange programs in the United States are not.

Finally, Chinese influence is diluted by increasing interactions between Latin America and other extraregional actors, such as India, Russia, Iran, and others. Although the PRC is arguably the most significant new suitor of the region, it is not the only alternative. For Nicaragua and populist regimes in the Andean region, Russia provides important alternatives with respect to arms purchases and energy sector investments. An $18 billion commitment by a Russian consortium to develop the Junin-6 oilfield in Orinoco, for example, may have helped to accelerate China's subsequent commitment to invest $16.3 billion in Junin-4. In addition to Russia, India is increasingly engaging in commercial opportunities, particularly in high technology, services, and commodity sector investments, while challenging the PRC monopoly over "south-south" developing country partnerships in the region. When China cut off purchases of Argentine soy oil, for example, it was India that picked up the slack.

Analysts looking for signs of imminent Chinese coercion or intervention in Latin America are likely to be disappointed. Nonetheless, Chinese soft power in Latin America still raises important national security issues, even if the PRC does not explicitly seek to subvert or marginalize the United States as part of its reemergence onto the world stage.

In Latin America, as elsewhere, China's currently modest influence is providing it with triumphs of ever-growing scale in strategically important business, culture, and technology arenas. Although no specific event may directly threaten the U.S. national interest, the collective effect is to restructure the global flows of value added and influence in a manner beneficial to China, making the ability of the United States to successfully pursue its own national goals and interests increasingly dependent on the acquiescence of the PRC.

For analysts focused on the "rise" of China in Latin America and elsewhere, the issue is not whether China is a threat, or whether it has the right to pursue its national interests in Latin America and other parts of the world. Rather, it is important to recognize the dynamics that this reemergence creates in a region with close human, geographical, and economic ties to the United States, and to prepare to mitigate the risks, meet the challenges, and rise to the opportunities that China's entry into Latin America makes possible. **JFQ**

## NOTES

[1] Joseph S. Nye, *Bound to Lead: The Changing Nature of American Power* (New York: Basic Books, 1990). Nye further refined the concept in *Soft Power: The Means to Success in World Politics* (New York: PublicAffairs, 2004).

[2] Joseph S. Nye, "The Rise of China's Soft Power," *The Wall Street Journal Asia*, December 29, 2005.

[3] In 2009, PRC bilateral trade with Latin America, counting Cuba, was $111.5 billion, while U.S. trade with the region was $530 billion, about 4.75 times larger. See *Direction of Trade Statistics* (Washington, DC: International Monetary Fund, June 2010).

[4] Leslie T. Chang, "China's Middle Class," *National Geographic*, May 2008.

[5] "An Unusual Rebuttal from China's Forex Regulator," *The Wall Street Journal*, May 27, 2010.

[6] John Lyons, "Brazil Turns to China to Help Finance Oil Projects," *The Wall Street Journal*, May 18, 2009.

[7] "Venezuela exploitará hierro, acero, bauxita y oro con China," May 16, 2010, official Web site of the government of Venezuela, available at <www.vtv.gob.ve>.

[8] See, for example, Janie Hulse, *China's Expansion into and U.S. Withdrawal from Argentina's Telecommunications and Space Industries and the Implications for U.S. National Security* (Carlisle Barracks, PA: Strategic Studies Institute, September 2007).

[9] Alexander Ador Netto, public comments as part of a panel on Chinese engagement with Latin America at The George Washington University, April 6, 2010.

[10] China expanded this presence by also temporarily sending rescue workers in the days following the January 2010 earthquake.

[11] "Bolivia Builds Defenses Against 'Poachers' of Resources," UPI.com, August 9, 2010.

[12] "The Shanghai World Expo Opens May 1," China Digital Times, April 27, 2010.

[13] For more details, see R. Evan Ellis, *China and Latin America: The Whats and Wherefores* (Boulder, CO: Lynne Rienner Publishers, 2009), 215–217.

[14] Rodrigo Orihuela, "Argentina Soybean Growers 'Optimistic' Talks Will End China's Oil Blockade," Bloomberg News, April 6, 2010.

[15] "China prestará a Venezuela $300 millones para crear aerolínea," *El Universal* (Caracas), April 24, 2010.

[16] In many business and technical interactions, English is used as the common language between Chinese and Latin Americans.

# Chinese Views on Deterrence

*By* DEAN CHENG

Celebration of 50th anniversary of PLA Navy's North Sea Fleet as it pursues capability to operate from Indian Ocean to western Pacific

Imaginechina via AP Images

The issue of Chinese views of deterrence and its role within Chinese security policy has become increasingly important in analyses of future East Asian security developments. In considering Beijing's views, three considerations should be kept in mind:

- There is no bolt-out-of-the-blue experience in the history of the People's Republic of China (PRC) comparable to Pearl Harbor or Operation *Barbarossa*.
- The People's Liberation Army (PLA) does not seem to exhibit nearly the same degree of concern with inadvertent wars or the lessons from World War I as is common among American decisionmakers.
- The PRC view of deterrence is not bilateral, but more multilateral, as China has been concerned with a range of threats on its periphery.

**Dean Cheng is a Research Fellow for Chinese Political and Security Affairs at The Heritage Foundation.**

Each of these issues affects China's views of deterrence.

## Chinese Definition of Deterrence

It is important first to consider how the Chinese define *deterrence* and how that compares with the Western understanding of that term. The Chinese term that is often equated with deterrence is *weishe*. In the *PLA Encyclopedia*, for example, the term *weishe zhanlue* is translated as "strategy of deterrence."[1]

But translations are often imprecise. There is the Italian saying, "*Tradutore, traditore*," or "All translators are liars." For most Western analysts, deterrence is seen as dissuading an opponent from acting in a particular way or following a particular course of action. Thus, Thomas Schelling, in his 1966 book *Arms and Influence*, defines *deterrence* as "the threat intended to keep an adversary from doing something."[2] This definition is echoed by other Western analysts of deterrence. John Mearsheimer in *Conventional Deterrence* notes that "deterrence, in its broadest sense, means persuading an opponent not to initiate a specific action because the perceived benefits do not justify the estimated costs and risks."[3]

Schelling specifically differentiates deterrence from *compellence*, which he defines as "the threat intended to make an adversary do something."[4] Glenn Snyder makes the same point by noting that deterrence "is the power to *dissuade* as opposed to the power to coerce or compel."[5]

This is in sharp contrast with the term *weishe*, which embodies *both* deterrence *and* compellence. The *PLA Encyclopedia*, again, defines a *strategy of deterrence*, or *weishe zhanlue*, as "the display of military power, or the threat of use of military power, in order to compel an opponent to submit."[6] Other authoritative Chinese volumes expand on this.

Generals Peng Guangqian and Yao Youzhi, in the PLA textbook *The Science of Military Strategy*, note that "deterrence plays two basic roles: one is to dissuade the opponent from doing something through deterrence, the other is to persuade the opponent what ought to be done through deterrence, and *both* demand the opponent *to submit to the deterrer's volition*."[7] Thus, Peng and Yao in essence combine Schelling's definitions of deterrence and compellence within the Chinese term *weishe*.

A similar conflation occurs in a volume authored by the PLA National Defense University's Military Science Research Department, which attests that the purpose of deterrence is "to halt, or prevent, the other side from starting a conflict, and thus protect one's own interests from aggression. *Or, it is to shake the other side's will to resist* (dikang yizhi), *and thus seize those interests or benefits that originally would have required conflict in order to obtain them*."[8]

Finally, in *National Defense Theory* (*guofang lilun*), the second of a PLA-published series of volumes used as national defense teaching materials, strategic deterrence is seen as the adroit application of military strength, involving actual use or nonuse, to psychologically constrain an opponent's actions, *or to cause him to submit*.[9] This same volume goes on to state specifically that not only can a defending side utilize deterrence to compel an aggressor to abandon offensive intentions, but also an offensive side can implement strategic deterrence, causing a defender to conclude that the cost of resistance is too high. By causing the other side to capitulate without fighting, or with minimal violence, one can then achieve the goal of "not fighting yet causing the enemy's troops to submit (*buzhan er qu ren zhibing*)."[10] This, of course, is consistent with Sun-Tzu's observation that the greatest general is the one who can win without fighting.

DOD (Cherie Cullen)

Secretary of Defense and Chinese officials participate in U.S.-China Track Two Dialogue in Washington

## Components of Deterrence

From the Chinese perspective, strategic deterrence (*zhanlue weishe*) involves all the components of "comprehensive national power (*zonghe guojia liliang*)."[11] These include military forces, economic power, diplomatic influence, scientific and technological capabilities, and even political and cultural unity. These serve to compel or deter opponents. These capabilities must be integrated so there is a coherent strategic deterrent at the disposal of the national leadership.

An essential component is real military power suitable to the types of wars that will be fought.[12] By this, the PLA means actual military forces currently fielded, in contrast with military *potential*, such as that embodied within a strong economy or a strong scientific and technological base. In today's environment, that means fielding a military that can fight "local wars under informationalized conditions"—that is, joint forces capable of exploiting modern information technology to wage noncontact, nonlinear, nonsymmetric warfare on land, sea, air, outer space, and cyberspace.

Successful deterrence requires not only capabilities, however, but also the will to use said power. Moreover, it requires the ability to persuade an opponent that one *has* both that capability and will.[13] This latter aspect is of special importance because from the Chinese perspective, successful application of *weishe* requires influencing the opponent's decision-makers. As *The Science of Military Strategy* notes, deterrence requires transmitting to an opponent both the existence of actual strength and the determination to use that strength in order to "impact directly on his mentality in creating a psychological pressure to shock and awe the opponent."[14] *Weishe* is ultimately as much psychology as it is capability.

In discussing military capabilities for deterrent purposes, PLA analyses include conventional and nuclear forces, but also, increasingly, space and information capabilities as well.

First, there is nuclear deterrence, which the Chinese characterize as coming in three degrees:

- "maximum nuclear deterrence," in which an opponent may be disarmed with just the initial massive strike
- "minimum nuclear deterrence," in which a handful of nuclear weapons may strike an opponent's cities

"moderate intensity nuclear deterrence," which involves a "sufficient and effective" nuclear capability.[15]

While the PLA has generally been seen as fielding a "minimum nuclear deterrence," it may now be shifting toward a "moderate intensity nuclear deterrence." The problem with nuclear deterrence, however, is that the destructiveness of nuclear weapons raises questions about the credibility of threats involving them.

Conventional deterrence relies on a nation's conventional military forces. In Chinese analysis, this is gaining in importance as conventional forces are more controllable, and ironically less destructive, than nuclear forces. They are therefore more usable than nuclear forces. Moreover, as modern technology has advanced, it has made nonnuclear forces much more capable, granting them the ability to wage long-range precision strikes and making "noncontact" warfare possible.

Space systems both enhance other forms of deterrence, while also serving as a deterrent in their own right. For conventional deterrence, they make it possible to fight noncontact, nonlinear, nonsymmetrical wars by providing all the necessary positioning, targeting, navigational, and weather data. Moreover, the ability to detect opponents makes it possible to deter enemy action by denying him the element of surprise.

For nuclear deterrence, PLA authors suggest that space systems may neutralize an opponent's nuclear deterrent so that, when paired with one's own nuclear forces, an opponent will be deterred or can be coerced due to the unpalatable choices it faces.[16]

In addition to complementing nuclear and conventional deterrence, PLA writings suggest that space systems may deter an opponent on their own. A space force effects deterrence in a number of ways. In the first place, because of the combination of expense, fragility, and vulnerability, one could hold an opponent's space infrastructure hostage. Much like nuclear deterrence, space deterrence, in this regard, becomes a question of cost-benefit analysis: Is, say, Taiwan worth the likely cost of repairing or replacing a badly damaged or even destroyed space infrastructure?[17]

Moreover, because space systems affect not only military but also economic, political, and diplomatic spheres, damage to them would have wide-ranging second-order repercussions.[18] Damaging an opponent's space infrastructure would impose economic and diplomatic costs beyond those of simply replacing satellite systems. The combination of first- and second-order effects may be sufficient to persuade an opponent that it cannot attain victory at an acceptable price.

Finally, PLA authors also discuss the concept of information deterrence. Information deterrence—and information warfare, the use of information techniques writ large to influence foreign governments, militaries, and populations—is seen as a stand-alone form of interaction, distinct from more traditional forms of warfare, and offering the potential of achieving "enemy troops [submitting] without war," that is, winning without fighting—the acme of the generals' skill, as Sun-Tzu writes.

There are two aspects to information deterrence. The first, more operational, aspect is the ability to influence the flow of information on the battlefield. The side that is able to better exploit information is seen as exercising information deterrence, a concept that is receiving growing attention in PLA writings. The second, more strategic, aspect is the ability to influence decisionmakers and the publics of one's own country, that of an opponent's, and those of third parties.[19] This includes not only affecting the flow of information, but also having the ability to provide one's own information and narrative. Within this broader context, the Chinese discuss what they term the "three warfares" of legal warfare (or lawfare), psychological warfare, and public opinion (or media warfare). One should consider the recent creation of the Chinese 24-hour English language news service, with global access, within this context.

## Views of Deterrence

So, how do China's views of deterrence mesh with 21st-century security requirements?

In the first place, *weishe* is not new. Deterrence has long been part of Chinese military thinking. The concept of People's War, the development of China's nuclear forces, and preparations for protracted war were all driven in part by the hope that such measures would make potential aggressors hesitate, while also putting in place the mechanisms necessary to fight and defeat an opponent should deterrence fail.

Second, just as China believes that maintaining national security requires "comprehensive national power," so, too, strategic deterrence is best achieved through not only military but also economic, diplomatic, and political means. Only a rich, unified nation can deter an opponent across the full spectrum of capabilities—lending a whole new meaning to "escalation dominance."

That said, it should be noted that the avowed goals of PRC defense policy now include constraining or limiting wars. One Chinese article notes that Jiang Zemin explicitly stated that limiting wars was now a vital part of the Strategic Guidelines for the New Period, which is the fundamental guidance for PLA thinking.[20] In essence, according to PLA authors, the Chinese military is expected to fulfill the mission of helping forestall the outbreak of war.

This view is consistent with Chinese views of *weishe*, since deterrence and warfighting are seen not as opposites, but as complements. Wars can serve to underscore deterrence, and deterrence may occur within war.[21] As important, the ability to "fight and win wars is the prerequisite for constraining wars."[22] In essence, the PRC believes that being able to fight and win wars, and making sure an opponent knows that, is the key to deterrence.

To this end, the uptick in public Chinese military activity, from out-of-area operations in the Gulf of Aden, to military exercises such as Vanguard 2010 and increased activity along the Ryukyus, to harassment of U.S. platforms such as the USNS *Impeccable* and *Victorious*, should all be seen in the context of the application of *weishe* toward the United States and other nations—both deterrence and compellence.

Finally, for the PLA and PRC leadership, the core question is how to realize a particular political goal without using force, while causing the enemy to believe that force may nonetheless be used. This is an essential consideration because it emphasizes that the point of *weishe* is not simply to deter enemy actions, or even compel submission, but to achieve a given political goal. Thus, for the PLA, and arguably for the PRC leadership, *weishe* is not an end, but a means. **JFQ**

## NOTES

[1] PLA Encyclopedia Committee, *Chinese Military Encyclopedia*, Supplemental Volume (Beijing: Military Science Publishing House, 2002), 477.

[2] Thomas Schelling, *Arms and Influence* (New Haven: Yale University Press, 1967), 69.

[3] John J. Mearsheimer, *Conventional Deterrence* (Ithaca: Cornell University Press, 1983), 14.

[4] Schelling, 69.

[5] Emphasis added. Glenn Snyder, "Deterrence and Defense," in *The Use of Force*, ed. Robert Art (New York: University Press of America, 1988), 31.

[6] PLA Encyclopedia Committee, 477.

[7] Peng Guangqian and Yao Youzhi, *The Science of Military Strategy* (Beijing: Military Science Publishing House, 2005), 215.

[8] Emphasis added. National Defense University Science Research Department, *New Perspectives on Military Transformation: Explaining 200 New Military Concepts* (Beijing: PLA Press, 2004), 85.

[9] Luo Youli, ed., *National Defense Theory* (Beijing: Military Science Publishing House, 2002), 113–114.

[10] Ibid., 114.

[11] Zhou Peng and Yun Enbing, "Developing the Theory of Strategic Deterrence with Chinese Characteristics," *China Military Science*, no. 3 (2004).

[12] Xu Shouwen, "Briefly Discussing Strategic Deterrence in the Information Age," *PLA Daily*, May 7, 2009.

[13] Zhou and Yun.

[14] Peng and Yao, 214.

[15] Ibid., 218.

[16] Hong Bin and Liang Xiaoqiu, "The Basics of Space Strategic Theory," *China Military Science*, no. 1 (2002).

[17] Xu Wei and Chang Xianqi, "Discussing Space Deterrence," *Academy of Equipment Command and Technology* 13, no. 1 (February 2002).

[18] Li Jingjun and Dan Yuquan, "The Strategy of Space Deterrence," *China Military Science*, no. 1 (2002).

[19] "Information Deterrence and You," *PLA Daily*, June 9, 2004.

[20] Zhou and Yun.

[21] Ibid.

[22] Chen Zhou, "On the Development of China's Defense National Defense Policy in the New Situation," *Chinese Military Science*, no. 6 (2009).


# Red Wings Ascendant

# The Chinese Air Force Contribution to Antiaccess

**PLAAF Su–27 Flanker is a multirole fighter-bomber**

DOD (D. Myles Cullen)

*By* MICHAEL P. FLAHERTY

During the 1995–1996 Taiwan Strait crisis, the United States intervened by deploying two carrier groups in response to Chinese missile tests near major Taiwanese ports. These tests were a means of coercively influencing pro-independence elements during the Taiwan presidential election and were considered by China to be an "internal" matter. The U.S. action therefore triggered enormous nationalistic resentment, rooted largely in historical humiliations and infringements on Chinese sovereignty by foreign powers. They also fueled a determined drive to mitigate or prevent such infringements on Chinese sovereignty in the future.

The national security strategy of China is built upon the concepts of sovereignty and territorial integrity. In defending these core national interests, People's Liberation Army Air Force (PLAAF) capabilities, doctrine, and training have been developed to support a comprehensive antiaccess/area-denial strategy. While these antiaccess capabilities cannot yet effectively counter U.S. capabilities, they have contributed to mounting U.S. concerns over China's current military modernization efforts. These concerns also facilitate misperceptions about "preemptive" Chinese military doctrine. If not clarified, dangerous miscalculations on both sides of the Pacific are possible, particularly if tensions over Taiwan are renewed.

While the Chinese air force has modified doctrine and improved capabilities to deter U.S. intervention in a Taiwan scenario, it remains a force with limited striking power. Due to a lack of experience and training in offensive air operations and its adherence to the strategic concept of active defense (*jiji fangyu*), China's air force is also not prepared to launch preemptive attacks in the absence of preexisting hostilities.[1] But, as these capabilities and doctrine mature, U.S. forces and

**Lieutenant Colonel Michael P. Flaherty, USAF, is a Deputy Director for Intelligence at the National Joint Operations and Intelligence Center, J3, Joint Staff.**

AP Images (Andy Wong)

Chinese and Philippine officials gather prior to discussion about claims to disputed islands in South China Sea

bases in the region will become increasingly vulnerable to Chinese antiaccess capabilities, requiring further efforts to enhance survivability, redundancy, and standoff capabilities to maintain the ability to project and sustain power in the region. For this reason, it is imperative to understand Chinese actions in their cultural and strategic contexts.

While China has never officially acknowledged an antiaccess strategy, the Chinese concept of active defense as well as recently modernized PLAAF capabilities, doctrine, and campaign planning have predisposed the PLAAF toward this approach in its role of defending China's sovereignty and territorial integrity.[2] Yet the PLAAF still faces significant challenges. These include an inability to refit all units with cutting edge weapons systems, weaknesses in China's aviation industry, lagging development of power projection enablers, and deficits in training. Any assessment of the implications of these developments must first examine the formulation of China's access-denial strategy, as well as the PLAAF transition to an offensive and defensive doctrine, which predisposes it toward this strategy. What then remains is to demonstrate how developing PLAAF capabilities, doctrine, and training combine to support an access-denial strategy with acknowledged implications for U.S. power projection.

## Formulation of Access-denial Strategy

China's most significant security concern is Taiwan. The U.S. deployment of two carrier groups to the region during the 1995–1996 Taiwan Strait crisis remains in the Chinese memory as a galling infringement on China's sovereignty. The value and logic of an access-denial strategy are therefore obvious in reference to Taiwan. But such a strategy has clearly appealed to Chinese strategists since at least the 1991 Gulf War. A key lesson learned from the Gulf War was that allowing a modern military opponent unfettered access to land, sea, and air territories in which to build up and employ forces, as well as regional bases and logistics hubs to sustain them, was a recipe for defeat. In discussing the lessons of the Gulf War, General Liu Jingsong, former president of the People's Liberation Army's (PLA's) Academy of Military Science, pointed out that the very assembly and positioning of coalition forces constituted "first firing" and justified action to postpone or even deter actual war.[3]

While the People's Republic of China (PRC) has never publicly acknowledged an antiaccess strategy, a 2000 U.S. National Defense University paper projected a consensus view that regional powers such as China would inevitably "develop anti-access strategies in response to U.S. dominance of the air and seas."[4] Yet it was not until the Department of Defense (DOD) *2005 Annual Report to Congress on the Military Power of the People's Republic of China* that U.S. analysts officially acknowledged China as placing an emphasis on antiaccess strategies, designed to "deny entry into the theater of operations."[5] This emphasis reflects the continuing sensitivity of the Chinese toward matters of sovereignty and territorial integrity. The overwhelming majority of China's historic military clashes have involved such border and sovereignty issues.[6] China today remains concerned about the vulnerability of its economically productive coastal areas to air and sea threats, and also fears that the United States would intervene to protect Taiwan should a Tai-

wanese declaration of independence trigger a Chinese military response.[7] China holds that Taiwan is Chinese territory and *denial* of Taiwan as a base for other powers to threaten the mainland or its sea lines of communication is therefore a logical assertion of China's sovereignty.[8]

As a rationale for adopting an access-denial strategy, the inviolability of China's territory and sovereignty cannot be overstated. Certain strands of classical Chinese culture and military philosophy support this argument. Military philosophers such as Sun Tzu, Sun Bin, and Shang Yang as well as the Confucian tradition (*fei gong* or "non-offense") advocate a cautious attitude toward war but allow "righteous war."[9] Defense of sovereignty or territory is considered righteous, particularly when responsive instead of provocative.[10]

China's heritage as a geographically isolated, agriculturally based civilization has also focused Chinese approaches to warfare on defense of land (territory), as demonstrated in China's historical lack of interest in maritime empire, as well as in cultural artifacts such as the Great Wall.[11] The "100 Years of Humiliation" ushered in by the Opium Wars and Western exploitation of Chinese military weakness in the 19th century, as well as Japanese occupation and atrocities during the 20th century, have engendered a defensive mindset toward foreign interventions that persists in modern China. Thus, the logic of defending China's territory by deterring or denying foreign intervention (antiaccess) is reinforced by China's perceptions of its own comparative weakness throughout the Cold War and various confrontations around its land and maritime periphery, including interventions in the Korean War and border conflicts with India, the Soviet Union, and Vietnam. Beijing considered most of these to be strategically defensive in response to some violation of China's sovereignty and territorial integrity.[12]

China's best strategy for defending these core interests is rooted in the PLA's traditional strategic concept of active defense (*jiji fangyu*). Active defense guides counterattacks *after* hostilities begin (for example, once the enemy has attacked or invaded Chinese territory). It is semantically different from the subordinate PLA principles of seizing the initiative, "gaining mastery before the enemy has struck" (*xian fa zhi ren*), or "gaining mastery after the enemy has struck" (*hou fa zhi ren*), all of which can be elements of active defense. As a guiding tenet, active defense carries nuances of "conflict avoidance, strategic guile, and as a last resort, carefully picking the battlefield and the battle."[13] Mao once stated that "China will never make a preemptive attack" and yet "active defense is defense in an offensive posture."[14] In preconflict situations, active defense emphasizes political caution and conflict avoidance, but once hostilities have begun, it emphasizes offensive counterattacks.[15] *Once conflict begins*, active defense can be characterized as strategically defensive and tactically offensive.

This active defense concept is often misunderstood outside of its cultural context. It underlies U.S. concerns regarding China's developing force projection capabilities, as well as misperceptions of the preemptive nature of Chinese military doctrine and campaign planning.[16] In analyzing China's developing offensive-defensive doctrine and its basis in active defense, U.S. analysts tend to focus on China's "preemptive" approach. An example noted by U.S. defense analysts is that the *Science of Strategy* asserts defensive counterattacks need not passively await the enemy's military strike but could be militarily preemptive in response to political maneuvers; "for the 'first shot' on the plane of politics must be differentiated from the 'first shot' on the plane of tactics," and if "any country or organization violates the other country's sovereignty or territorial integrity, the other side will have the right to 'fire the first shot' on the plane of tactics."[17] These declarations are perceived by U.S. analysts as justifying preemptive offensives in response to political maneuvering. However, the Chinese perspective would emphasize the violation of Chinese sovereignty—for instance, *if Taiwan declared independence*—as justifying a military response specifically against Taiwan, *but not necessitating attacks on its allies* regardless of their declared intentions to come to Taiwan's defense in such a scenario.

This is not to say that miscalculations could not occur, but rather that for PLAAF preemptive strikes on U.S. airfields, carrier groups, and bases to be launched as a true expression of active defense, they would have to be *preceded* by U.S. violation of China's sovereignty or territorial integrity (such as active military intervention in the scenario above). Ambiguities regarding the threshold such intervention would have to meet in order to trigger a Chinese counterattack have biased U.S. analysts toward worst-case scenarios that obscure the strategic intent of active defense. As a precedent, in the 1970s, Deng Xiaoping applied active defense to the PLAAF, stating that "active defense also contains an offensive element. . . . The bombers of the air force are defensive weapons."[18] This is an acknowledgment that seizure of the initiative is crucial in modern air warfare, but *not* an argument for preemption outside the context of preexisting hostilities. This approach is therefore different from the Western idea of preemption, which includes the possibility of strategic preemption as part of the *initiation* of conflict. For instance, the 2002 and 2006 U.S. National Security Strategy documents assert a justification for strategic preemption or even preventive war in dealing with emerging threats in the absence of attacks on U.S. territory.[19]

AP Images/Xinhua News Agency

**Chinese helicopters escort landing ships during joint land, sea, and air military exercise**

AP Images/Imaginechina

**PLAAF JH–7 takes off during drill as part of China's efforts to operate from the Indian Ocean to the western Pacific in "active defense" of its territory and sovereignty**

Attention to these nuances places Chinese campaign plans in their cultural and strategic contexts by highlighting the Chinese national sensitivity to matters of sovereignty and territorial integrity. It also clarifies how active defense, when guiding modern doctrine and modern long-range capabilities, predisposes the PLAAF to an antiaccess approach.

The PLAAF's expanding role in active defense emerged gradually in concert with its transition from an air defense role to one with both offensive and defensive capabilities and doctrine. Chinese President Jiang Zemin repeatedly asserted that future major military threats to China would come from enemies using long-range precision-guided weapons to carry out raids and that sea and air would be the primary battlegrounds of the future. Therefore, the air force would be the strategic service with a "decisive status and role in protecting national security and sovereignty."[20] The PLAAF has thus developed modernized offensive capabilities and doctrine grounded in the tenet of active defense.

## Evolution of Offensive-Defensive Doctrine

For much of its history, the PLAAF was limited to homeland air defense roles. But the role that airpower played in the U.S. victory in the Gulf War had a significant impact on PLAAF theorists, driving recognition of weaknesses in capabilities and doctrine and highlighting China's vulnerability to modern air threats. Following the Central Military Commission's direction of the PLAAF in the early 1990s to prepare against air raids and support other components, the air force began to shape its own campaign doctrine and weapons development programs.[21] New offensive capabilities and doctrine now balance the PLAAF defensive tradition, and both enable antiaccess options not previously available.

Since the 1990s, China has paid close attention to developments in airpower thought in other countries. In formulating its own offensive-defensive doctrine, the PLAAF has synthesized U.S. assessments of the Gulf War, Kosovo campaign, and U.S. operations in Afghanistan and Iraq, building on the doctrine that it has practiced since the days of Russian assistance and influence. It has also considered contemporary Russian discussions on enhancing the role of its air force with new offensive and defensive missions.[22] While U.S. doctrine may be too radical for the current capabilities and culture of the PLAAF, the exposure to these ideas has driven a recognition of the air force as a major national capability to contain and win wars, yielding a significant PLAAF role in strategic deterrence and a desire for the capability to win high-tech local wars with airpower.[23] President Jiang Zemin asserted that "we must construct a powerful people's air force 'with Chinese characteristics,' that is both offensive and defensive."[24]

As part of this drive and in order to "construct an informationized force and win an informationized war," Chinese national security strategy forums established imperatives to accelerate PLAAF modernization, transform it from a homeland air defense type of air force to a type that combines both offense and defense, and develop modernized capabilities to defend China's security and interests.[25] The concept of "informationization" permeates PLA doctrine and emphasizes the holistic integration of digitally linked information, sensors, weapons, and automated command and control systems via common networks.[26] In 2004, in accord with the Central Military Commission's new military strategy program, the PLAAF formalized this approach in a new air force strategy (actually more operational doctrine than strategy), which "integrated air and space, with both attack and defense (*kong tian yiti*, *gong fang jianbei*)."[27]

This offensive-defensive doctrine enhances the PLAAF ability to defend China's sovereignty and territorial integrity with modern offensive capabilities. That these same capabilities support an antiaccess strategy is clearly supported by PLAAF campaign planning efforts. PLAAF antiaccess capabilities are integrated in the "joint anti–air raid" campaign as well as the component specific "air offensive" campaign, "air defense" campaign, "airborne" campaign, and "air blockade" campaign, all of which propose attacks on adversary bases and naval forces at the outset of operations.[28] In envisioning these campaigns, PLA military authors have stated that "the core of a strategy that combines offense and defense is aerial offense."[29] They explicitly state adherence to the principle of active defense and taking the initiative, partially or mostly annihilating enemy capabilities at the very beginning of hostilities and "*at long range, before these can be thrown into operations*."[30] Air offensives are considered a primary operational form with which to achieve strategically defensive goals, specifically denying or disrupting access to forward bases and deployed capabilities.[31]

As noted above, these statements can be perceived as assertions of preemptive doctrine if analyzed outside their theoretical context of active defense. Within this context, the focus of PLAAF air campaign planning is on denying force projection and sustainment capabilities once hostilities have begun. The joint air raid campaign stipulates that operations are to be carried out within (military regional) theaters, but also "to carry out assaults against enemy bases (or platforms) for

takeoffs and launchings of air raid weapons."[32] To this end, PLA logistical planning for this campaign focuses on organizing conventional missile forces, long-range or sea-based air defense missile forces, air force and naval aviation, and Second Artillery Corps forces to "launch violent attacks against enemy airfields and aircraft carriers," seeking to destroy enemy capabilities *before they can be employed*.[33]

Even the air defense campaign envisions long-range strike assets executing "determined *counterattacks* against enemy air force bases and naval air launch and cruise missile launch platforms" and that air defense operations will "take on the quality of offense within defense, defense within offense, and offense interwoven with defense."[34] These campaign plans state the requirement for offensive air defense capabilities to "attack such targets as the enemy's command and control, intelligence and reconnaissance systems, his naval bases, airfields, missile sites and ships." They also acknowledge that the scope of air defense has "transformed from passive to active and from homeland defense to defense outside the homeland."[35] Thus, campaign planning and doctrine apply antiaccess approaches to increase the cost of violating China's sovereignty or territorial integrity.[36] For execution, they require modern capabilities.

## Development of Antiaccess Capabilities

To execute an access-denial strategy, the PLAAF requires capabilities effectively designed to neutralize U.S. forces, bases, and sustainment infrastructure already in the region. It must also be able to prevent follow-on forces from entering the region, extend its own defensive capabilities to regional entry points, and ultimately convince the United States and its allies that the cost of entry into the region will be prohibitive.[37] In practical terms, these capabilities include advanced and extended range air defense, air-to-air, and precision-strike capabilities. They also include command and control ($C^2$) and intelligence, surveillance, and reconnaissance (ISR) capabilities, as well as force projection enablers such as aerial refueling, airlift, and logistic capabilities. Full development and informationization of these capabilities coupled with dominance of the electromagnetic spectrum could enable the PLAAF, in conjunction with other arms of the PLA, to hold carrier strike groups at risk, deny or disrupt regional airfields, bases, and logistic nodes, and deny airspace over or near Chinese territory or forces.

The PLAAF has chosen to deter or deny the threat of aircraft penetrating China's territory and airspace, or seizing air dominance over PLA forces, via advanced and extended range surface-to-air missiles (SAMs) and fighter aircraft. Modernizing air-to-air capabilities now complement advanced Russian and indigenous SAMs. Older aircraft feature selectively improved electronics, radar, and engines, and some variants are equipped for aerial refueling, extending their combat radius and enhancing aerial access-denial options as far as the South China Sea.[38] More modern multirole fighters also incorporate an extended combat radius, advanced avionics, aerial refueling capability, some stealth design characteristics, and data link capabilities that allow sharing of information with the KJ series Airborne Warning and Control Systems (AWACS). These can also employ a variety of upgraded air-to-air missiles for an extended beyond-visual-range (BVR) attack capability.[39]

While these more modern aircraft remain limited in number, they have already reversed the balance of air superiority with Taiwan. Indigenous production of these aircraft will eventually increase the expertise and capabilities of China's aviation industry.[40] However, despite steadily growing numbers of aircraft with ever increasing ranges, the operational reach of these capabilities is still constrained by minimal aerial refueling training and a limited number of aerial refueling–qualified pilots and refueling-configured aircraft.[41] If these limitations are overcome, the PLAAF's ability to hold U.S. force projection capabilities at risk at extended range would be greatly enhanced.

Evolving PLAAF precision-strike capabilities add another layer of antiaccess competencies to deter, disrupt, or deny regional bases, as well as naval surface and carrier operations. These include upgraded aircraft that can employ modern precision ordnance including anti-radiation missiles, air-launched land attack and antiship cruise missiles, and a variety of television, laser, and Global Positioning System/Global Navigation Satellite System–guided precision munitions. These last include "bunker buster" munitions that can be employed in long-range access-denial attacks on hardened targets such as aircraft shelters and command and control bunkers at regional bases beyond China's periphery (for instance, Kadena Air Base).[42]

The remainder of the PLAAF's long-range strike capability resides with its H–6 bomber and cruise missile variants, which can attack various fixed targets (including Guam) with either conventional or nuclear payloads. These capabilities give the PLAAF a significant role in strategic deterrence as well as extended range access denial.[43] PLAAF capabilities are also complemented by evolving PLA Navy (PLAN) strike capabilities that allow both the PLAAF and PLAN to strike a variety of land and sea targets at extended range, potentially preventing deployment or employment of forces from these targets.[44] However, while these capabilities represent significant progress for the PLAAF, China's aviation industry is still weak in the areas of aircraft engines, guidance and control systems, and enabling technologies.[45] Also, PLAAF ability to logistically support and sustain force projection operations beyond its periphery, particularly in antiaccess scenarios that might include sustained long-range strikes or the seizure of regional bases, is limited.[46]

A holistic approach to integration of $C^2$ and ISR has enhanced coordination and employment of access-denial capabilities across the PLA. As noted above, informationization encompasses digital linkage of information, sensors, weapons, and automated $C^2$ systems via common networks while denying these capabilities to opponents.[47] The focus of PLAAF airborne early warning and ISR development has also been on increasing search range and situational awareness of regional airspace and enabling surveillance and targeting support for other extended range antiaccess capabilities.[48]

Informationization has also driven a PLAAF capability to deny access to the electromagnetic spectrum. By 2006, the Department of Defense assessed that "China's investments in advanced electronic warfare programs had given the PLAAF technological parity with or superiority over most potential adversaries."[49] Seizure of electromagnetic dominance via "integrated network electronic warfare" (*wangdian yitizhan*) is envisioned in the initial phases of any future campaigns. This approach is conceived by PLA theorists as electronic, computer network, and kinetic strikes to "disrupt and deny network information systems that support enemy war fighting and power projection capabilities"; in other words, *access denial*.[50] The significance of such electromagnetic antiaccess capabilities to the PLAAF is clearly demonstrated in

campaign planning. To employ such capabilities effectively, PLAAF doctrine and training must integrate these and other antiaccess capabilities.

## Doctrinal Integration

The PLAAF has made significant progress in integrating its antiaccess capabilities in doctrine. PLAAF operational planning increasingly reflects doctrinal principles that integrate current weapons systems while anticipating the best ways to employ developing offensive-defensive capabilities in air campaigns. Three of these principles are clearly relevant to employing these capabilities in support of access-denial strategies: (1) *Seize the initiative through offensive operations*; (2) *Concentrate force at the decisive points*; and (3) *Tight defense*.[51]

The first of these, "S*eize the initiative through offensive operations,*" is similar to the familiar Western principle of the "Offensive," but in the context of active defense conveys the awareness that offensive action is the only way to seize the initiative and gain momentum in modern air campaigns. This will be difficult for PLAAF culture to assimilate as it has no tradition of aggressively employing airpower for offensive missions. Also, PLAAF pilots and commanders are not yet confident in their abilities to employ airpower in such a fashion.[52]

The second applicable principle, "*Concentrate force at the decisive points*," conveys a preference for concentrating the most modern aircraft capabilities to conduct offensive operations against high-value airborne assets in the struggle for air dominance or against priority surface targets, particularly antiaccess targets as evidenced by PLAAF campaign plans.[53] Priority in air campaign planning is placed on destruction of enemy aerial force projection capabilities (AWACS, aerial refueling tankers, airlift and combat aircraft) in the air and on the ground. These airstrikes would closely follow Second Artillery missile strikes or PLAN strikes and would occur in conjunction with electronic warfare (jamming) and computer network attacks (and potentially attacks from and against space-based infrastructure).[54] *The Science of Campaigns* (2006) describes a potential scenario where the PLAAF takes the lead in attacking enemy air bases and aircraft carriers. Missiles, "anti-radiation UAVs," and electronic jamming attacks are employed against air bases and early warning radars, followed by airstrikes on command and control centers, runways, parked aircraft, and fuel depots. Continuous missile and airstrikes are then concentrated in time and space to "annihilate enemy air capabilities" and achieve air dominance over PRC territory and forces.[55]

A third principle of "*Tight defense*" focuses on ensuring there are no weak points in the defense and that all important sectors are protected by one means or another.[56] This principle supports the intent of the PLAAF's antiaccess approach to defending China's sovereignty and territorial integrity. By performing its role in active defense along with the other branches of the PLA, the PLAAF adds its own capabilities to the other layers of air, land, sea, space, and cyber-based antiaccess capabilities presented by these other services.

The PLAAF has made slower progress in integrating its antiaccess capabilities in training. The PLAAF and PLAN continue to emphasize training for attacks on aircraft carriers. PLAAF training now includes aerial combat training between dissimilar aircraft, long-range offensive air missions, surface task force protection missions, and live munitions delivery.[57] New, semi-permanent opposition forces (known as BLUEFOR) employ foreign tactics and doctrine to train the PLAAF.[58] However, while the scope for pilot initiative has improved with more modern systems and somewhat less rigid training scenarios, air intercept training still relies heavily on ground control. Also, while some new BVR tactics and doctrine have been observed, these remain immature and limited.[59] Airborne infantry training (a PLAAF responsibility) is limited by airlift capacity, and in-flight refueling training is still limited by the small number of aerial tankers and refueling-configured combat aircraft.[60] When added to the limitations above, it is clear that PLAAF capabilities, doctrine, and training must still evolve considerably in order to challenge U.S. power projection capabilities.

## Implications for U.S. Power Projection

While the development of antiaccess capabilities has not been uniform across the PLAAF, and continues to lag relative to U.S. power projection capabilities, impressive progress has been made over the last decade. On September 16, 2009, U.S. Defense Secretary Robert Gates acknowledged that China's "investments in cyber and anti-satellite warfare, anti-air and anti-ship weaponry, and ballistic missiles could threaten America's primary way to project power and help allies in the Pacific—particularly our forward bases and carrier strike groups."[61] The PLAAF can now contest local air dominance over the Taiwan Strait, creating new options for Chinese coercive diplomacy.[62] The range of air refueling–capable Su–30MKKs deployed in the Nanjing and Guangzhou Military Regions can already threaten U.S. forces in Okinawa, though not with the effect additional tankers and air refueled aircraft could offer.[63] H–6 bombers can now employ air-launched land attack cruise missiles from within Chinese airspace against Okinawa, Japan, and the Korean Peninsula. Reported H–6 engine modifications could potentially give the H–6 a 3,000-kilometer radius of action, allowing access-denial strikes against Guam.[64] All of these capabilities will be increasingly integrated with other PLA service capabilities and China's space-based reconnaissance, positioning, and terrestrial over-the-horizon targeting capabilities to enhance antiaccess options against U.S. power projection.[65]

If China shares these capabilities with hostile regimes, they could challenge U.S. force projection efforts worldwide. While these capabilities cannot yet *defeat* current U.S. capabilities, they are still significant. They represent incremental progress in narrowing the gap to eventually deny, disrupt, delay, or neutralize U.S. forces, bases, and sustainment infrastructure already in the region, and prevent follow-on forces from entering the region. They could eventually extend China's active defense options to regional entry points. Ultimately these PLAAF capabilities serve as elements of a modest but relentlessly improving deterrent to U.S. intervention in the region by increasing the cost of such intervention to unacceptable levels. As these capabilities and doctrine mature, U.S. forces and bases in the region will be increasingly vulnerable to Chinese access-denial capabilities, requiring further efforts to enhance survivability, redundancy, and standoff capabilities in order to maintain the ability to project and sustain power in the Pacific.

PLAAF offensive and defensive doctrine and modernized capabilities are guided by the strategic tenet of active defense. They are therefore optimized for an antiaccess strategy in defending China's sovereignty and territorial integrity, and in fact predispose the PLAAF toward such an approach. While China has never acknowledged this strategy,

it has been increasingly integrated within doctrine and training as revealed above. Although this has contributed to concerns and misperceptions about Chinese intentions regarding their growing force projection capabilities and campaign planning, it is important to comprehend these capabilities and plans within their context of *active defense*. This is crucial to an understanding of the Chinese national sensitivity to matters of sovereignty and territorial integrity and could prevent miscalculations on both sides of the Pacific by placing Chinese actions in their cultural and strategic contexts. It also enables clarification of the specific situations in which PLAAF operations are likely to be preemptive or offensive, mitigating analytical biases towards "mirror-imaging" Chinese intentions when assessing PLA doctrine.

While still not on par with U.S. capabilities, the PLAAF has made impressive progress in its ability to hold U.S. forces and bases at risk and is narrowing the technological gap. Yet joint integration and training still lag behind, and doctrine will need to evolve as new capabilities are assimilated. Given the vulnerability of U.S. bases and forces in the region, the PLAAF's expanding capabilities will present a steadily increasing challenge to U.S. force projection capabilities during the next several decades. **JFQ**

## NOTES

[1] See the next section of this article for a discussion of how the PLA's tenet of Active Defense guides counterattacks *after* hostilities begin (for example, once the enemy has attacked or invaded Chinese territory) as opposed to a doctrine of preemptive attack. The sources of this data are cited in that section though analytical interpretations vary depending on the linguistic and military proficiency of the translator:

[2] A great number of official and academic documents discussing PLAAF doctrine, campaign planning, and training are available at the unclassified level in Mandarin Chinese, but have yet to be consistently translated into English or made widely available for analysis. I have referenced several of these below in notes 27, 29–36, and 52–57, in some cases translating, retranslating, or transliterating their contents myself and in collaboration with native Chinese speakers.

[3] John Wilson Lewis and Xue Litai, "The Quest for a Modern Air Force," in *Imagined Enemies: China Prepares for Uncertain War* (Stanford: Stanford University Press, 2006), 237.

[4] Sam Tangredi, *All Possible Wars? Toward a Consensus View of the Future Security Environment, 2001–2025* (Washington, DC: National Defense University Press, 2000), 41, 78–82.

[5] Department of Defense (DOD), *Annual Report to Congress: Military Power of the People's Republic of China 2005* (Washington, DC: Government Printing Office, 2005), 33.

[6] David M. Lampton, *The Three Faces of Chinese Power: Might, Money, and Minds* (Berkeley: University of California Press, 2008), 16.

[7] Ibid., 40–41.

[8] Ibid., 50.

[9] DOD, *Annual Report to Congress: Military Power of the People's Republic of China 2009* (Washington, DC: Government Printing Office, 2009), VII.

[10] Ge Dongsheng, *On National Security Strategy* (Beijing: Military Science Publishing House, 2006), 203.

[11] Ibid.

[12] DOD, *Annual Report, 2009*, 12.

[13] Lewis and Xue, 40.

[14] Ibid.

[15] Ibid.

[16] DOD, *Annual Report, 2009*, 12.

[17] Ibid.

[18] Lewis, 227.

[19] *The National Security Strategy of the United States* (Washington, DC: The White House, 2002), Section 5, and *The National Security Strategy of the United States* (Washington, DC: The White House, 2006), 12.

[20] He Weirong, "Military Thought on the Air Force," *Chinese Air Force Encyclopedia* (Beijing: Aviation Industry Press, 2005), 1–5.

[21] Lewis, 223–227.

[22] He, 1–5.

[23] Guo Jinxiao, "The Science of Air Force Strategy," *Chinese Military Encyclopedia* (Beijing: Military Science Publishing House, 2002), 311–312.

[24] Ge, 215.

[25] Ibid.

[26] Lampton, 42.

[27] Ji Fuxin, "The Science of Air Force Command," *Chinese Air Force Encyclopedia* (Beijing: Aviation Industry Press, 2005), 157–158.

[28] DOD, *Annual Report, 2009*, 13, and Ge, 236.

[29] Ge, 234.

[30] Ibid., 236.

[31] Guo, 311–312.

[32] Lu Wen, "Logistics Support of Anti-Air Raid Operations," in *Theater Campaign Logistics Support*, ed. Xu Guoxin (Beijing: National Defense University Press, 1997), 98.

[33] Ibid., 113.

[34] Yu Liming et al., *The Science of Campaigns (2006)* (Beijing: National Defense University Press, 2006), 602–605.

[35] Ge, 236.

[36] Ibid., 238.

[37] Tangredi, 79.

[38] Tong Hui, *Chinese Military Aviation, 1995–2009, Section 1: Fighters, 1–2*, available at <http://cnair.top81.cn/>.

[39] Ibid.

[40] DOD, *Annual Report, 2009*, VIII.

[41] Ibid.

[42] Tong.

[43] Ibid.

[44] Ibid.

[45] DOD, *Annual Report, 2009*, 37.

[46] Ibid., 38.

[47] Lampton, 42.

[48] DOD, *Annual Report, 2009*, 62.

[49] Ibid., VIII.

[50] Ibid., 14.

[51] I have noted several contradictions (possibly a result of evolution in PLA thought over time) and inaccuracies in available English translations of Chinese Air Force Campaign Principles and have therefore undertaken my own translations and transliterations from the source documents below. Any errors of interpretation are entirely my own: Zhang Yanbing, "Air Force Campaign Principles," *Chinese Air Force Encyclopedia* (Beijing: Aviation Industry Press, 2005), 95–96; Lin Hu, "Air Force Campaign," in *Chinese Military Encyclopedia*, vol. 2, ed. Song Shilun and Xiao Ke (Beijing: Military Publishing House, 1997), 446; Yu et al., 334; Yang Xiaobo et al., *Science of Joint Campaign Command* (Beijing: Military Science Publishing House, December 2005), 282.

[52] Ibid.

[53] Ibid.

[54] Ibid.

[55] Yu et al., 347.

[56] Additional interpretations from Zhang Yanbing, *Chinese Air Force Encyclopedia*; Lin Hu, *Chinese Military Encyclopedia*; Yu Liming et al., *The Science of Campaigns (2006)*, 334; Yang Xiaobo et al., *Science of Joint Campaign Command*, 282.

[57] IHS (Global) Limited, "World Air Forces, China," *Jane's World Air Forces*, (Singapore: IHS, July 2009), 3–5.

[58] DOD, *Annual Report, 2009*, 51.

[59] IHS, 15.

[60] DOD, *Annual Report, 2009*, VIII.

[61] Tony Cappaccio, "China's New Weapons May Threaten U.S. Bases, Ships, Gates Says," September 16, 2009, available at <www.bloomberg.com/apps/news?pid=20601080&sid=am6ExRzB1cjo>.

[62] DOD, *Annual Report, 2009*, VIII.

[63] IHS, 4.

[64] Ibid., 16.

[65] DOD, *Annual Report, 2009*, VII, 22–23.

B–2 aircraft will be capped at its current total of 21 operational aircraft

U.S. Air Force (Kevin J. Gruenwald)

# Long-range Conventional Strike

# A Joint Family of Systems

*By* ROBERT P. HAFFA, JR., *and* MICHAEL W. ISHERWOOD

U.S. plans to modernize long-range conventional strike have undergone significant changes over the last decade. In 2001, the U.S. Air Force elected to cap the B–2 fleet at the 21 already in service, based on the belief that the stealth bomber did not offer the advanced technologies needed to penetrate the integrated air defenses expected to be fielded by future adversaries. The Air Force supposed the technologies required for the next-generation long-range strike system—supersonic cruise, large payload, and very low observability—might not be available until about 2037.

The 2006 Quadrennial Defense Review (QDR), expressing concern regarding a more salient threat, pulled the next-generation long-range strike system ahead by nearly two decades, calling for an initial operational capability in 2018. Subsequently, an Air Force analysis of alternatives scaled down the requirements for a new aircraft to meet that timeline. The 2018 bomber was to be manned, subsonic, and "highly survivable." Skills and facilities to develop and produce such an aircraft were judged to be at hand, while planned upgrades would add capability as technology matured. The 2018 goal was within reach.[1]

The 2010 QDR Report offers a different approach. While it agrees with previous assessments regarding the need to expand conventional long-range strike capabilities, the report does not focus solely on a long-range bomber to meet those requirements. Rather, it advocates a "family of systems" to "support U.S. power projection operations over the next two to three decades." Included in that "family" are a number of parallel efforts:[2]

- expand the capacity of the *Virginia*-class attack submarines
- experiment with prototypes of a naval unmanned combat aerial system (N–UCAS)
- examine options for a new Air Force long-range surveillance and strike aircraft
- assess alternatives for a new joint cruise missile
- experiment with conventional prompt global strike prototypes.

This article examines the capabilities that each of these family members brings to meeting the Nation's conventional long-range strike requirements, and estimates when such capabilities might be fielded. To do so, we need to first set aside some major factors that will influence choices and trades among this mix of strategic systems.

The first of these factors are the "enablers" that permit such a family of strike systems to operate effectively. Central to any long-range strike capability, as recognized in the QDR, are robust command, control, communications, and computers, and intelligence, surveillance, and reconnaissance (ISR) capabilities. Survivable airborne ISR assets, jam-resistant satellite communications, and long-endurance unmanned air vehicles to act as communications relay platforms are essential components of this infrastructure. Additionally, the 2010 QDR calls for improving the survivability and capability of space-based ISR assets, increasing investment in electronic attack, and improving the resiliency of U.S. forward bases. Regardless of the composition of a layered mix of long-range strike systems, these improvements will have to be made, acknowledging that some of these needed capabilities will be organic to long-range strike family components.

The second issue that this article does not address is the nuclear mission. The 2010 Nuclear Posture Review (NPR) makes clear U.S. nuclear priorities and programs required to underwrite deterrence while reducing deployed nuclear weapons and launchers in accordance with arms control negotiations. As the nuclear triad is downsized, a prudent

**Dr. Robert P. Haffa, Jr., is Director of the Northrop Grumman Analysis Center. Colonel Michael W. Isherwood, USAF (Ret.), is a Senior Analyst in the Northrop Grumman Analysis Center.**

hedge within an uncertain international security environment, as recognized by the NPR, is a modernized conventional long-range force. That future force is likely to be composed of a layered mix of the family of systems enumerated in the QDR.

Third, this is a *capability*, not a budgetary assessment. Speaking at the Eisenhower Library in May 2010, Secretary of Defense Robert Gates stated, "Realistically, it is highly unlikely that we will achieve the growth rates necessary to sustain the current force structure."[3] Thus, the family of conventional long-range strike systems will face programmatic and budgetary hurdles as they are developed and fielded. That said, with respect to long-range surveillance and strike, the U.S. defense portfolio has been significantly out of balance for more than a decade, with serious shortfalls in long-dwell surveillance and prompt global strike. For example, between 1999 and 2006, the Air Force invested $48.6 billion in short-range systems, compared with $5.1 billion in long-range capabilities.[4]

With ISR, nuclear, and budgetary issues reserved for future analysis, what are the challenges this family of systems will be called upon to meet in the future? A number of nations have invested in capabilities to deny the U.S. military the ability to operate with impunity in and around their territory, resulting in a diverse array of antiaccess and area-denial (A2/AD) technologies being developed and deployed. Those capabilities act to push U.S. forces further back from forward bases used previously to project military power. Which are the most worrisome A2/AD capabilities?[5]

Short- and medium-range ballistic missiles (SRBMs and MRBMs) in the hands of plausible military opponents, particularly when armed with cluster-type submunitions, place aircraft on U.S. forward bases in U.S. Central Command and U.S. Pacific Command at risk. China has fielded over 1,000 such missiles while continuing to produce more each year. The Chinese DF–21 ballistic missile, with a range of 1,500 nautical miles and guided by the Global Positioning System, can reach U.S. and allied bases in Korea, Japan, the Philippines, and Thailand. The closest air base outside its range is in Guam, more than 1,500 nautical miles from the Chinese mainland. In another region of U.S. vital interest, Iran has between 300 and 1,500 SRBMs and MRBMs. The Shahab-3, with a range of 1,000 nautical miles, could strike U.S. and allied bases as far west as Incirlik, Turkey, or Akrotiri, Cyprus, and as far east as Manas, Kyrgyzstan, while holding bases and ports throughout the Middle East at risk.[6]

Land-based bombers outfitted with cruise missiles could also threaten forward U.S. forces and allied facilities. The Chinese HK–6k aircraft has a 2,000-nautical-mile combat radius but when outfitted with six CJ–10 cruise missiles can reach another 1,300 miles, holding at risk U.S. installations in Guam and Wake Island, as well as facilities and forces in all of Japan and the northern half of Australia. U.S. and allied naval forces also must contend with the A2/AD challenge. The HK–6k can employ the Mach 2+ Kh-31, a sea-skimming missile armed with a high explosive or antiradiation warhead. Bomber forces could be escorted by the Su–30, a fourth-generation fighter equal to the Air Force's F–15E with a refueled range of 1,400 nautical miles. Whether targeting land- or sea-based forces, an adversary's composite fighter-bomber strike force could confront the United States and its allies with an air-sea battle the likes of which has not been seen since World War II.[7]

Cruise missiles also expand the arc of area denial. Iran has 300 or more Silkworm antiship missiles that could clog the Strait of Hormuz with damaged military and civilian ships, while their fast naval boats, equipped with the 100-mile-range C–802 cruise missile, could deny access to naval forces attempting to pierce a blockade.[8]

Submarines in an A2/AD role present a two-pronged threat to U.S. forces. Both Iran and China have diesel submarines to endanger close-in naval task forces. The Chinese have also acquired a dozen Russian *Kilo*-class submarines capable of launching the Sizzler cruise missile, designed to penetrate a maritime air defense network. China is producing 3 to 4 diesel submarines per year to field a future fleet of about 60 attack submarines.[9]

Integrated air defenses can deny U.S. airpower access over contested territory, with the Russian-exported "double digit" surface-to-air missile (SAM) systems effective out to 125 nautical miles.[10] China is deploying advanced SAM systems with its naval forces—creating lethal engagement zones for U.S. fighter and bomber crews far from the Chinese coastline.[11]

Advanced jet fighters will add to the A2/AD challenge. The Sukhoi-developed T–50, a fifth-generation fighter designed to rival the F–22 and F–35, is expected to reach initial operational capability with the Russian air force in 2015.[12] China is pursuing a similar aircraft—the J–XX—building on the fourth-generation Russian Su–30 and Chinese F–10 inventory.[13]

Collectively, these offensive and defensive capabilities will stress current U.S. and allied power projection forces in the Western Pacific and Persian Gulf regions. Carrier- and land-based aircraft may need to operate at least 1,500 nautical miles from an adversary's coastline to reduce risk. If conventional forces attempt to penetrate that arc, they will require highly effective air and missile defenses plus passive survival capabilities.

Unfortunately, the current inventory of conventional U.S. long-range strike systems provides a limited range of options and displays a force declining in quantity and quality. The


Lockheed (David Drais)

**AF–1 and AF–2 models of F–35A Lightning II joint strike fighter complete test flight**

inventory consists of conventional air- and sea-launched cruise missiles and the B–2 bomber.

The Air Force conventional air-launched cruise missile (CALCM) inventory has dwindled. The CALCM is no longer in production; the only source of additional missiles is conversion from the nuclear variant. A single B–52 can carry up to 20 CALCMs, which rely on a combination of satellite navigation and on-board guidance systems to deliver a 3,000-pound warhead over a range of roughly 600 nautical miles. The Tomahawk land-attack missile (TLAM)—armed with either a 1,000-pound unitary warhead or 166 submunitions—can range up to 1,000 nautical miles and has been upgraded with satellite navigation allowing for reduced mission planning time and in-flight target updates. Up to 36 TLAMs can be carried on a *Virginia*-class submarine, while the number on surface combatants varies with the number of vertical launching systems (VLS) aboard. The B–2 bomber is a low-observable aircraft with an unrefueled range of 6,000 nautical miles. Its two-man crew can use onboard sensors to search, track, and engage mobile targets, while delivering 80 500-pound Global Positioning System–guided bombs or 16 2,000-pounders (for fixed targets), or large numbers of the 250-pound small diameter bomb.

Of this force, only the B–2 (supported, perhaps, by F–22 fighters) provides commanders the confidence to operate effectively within a sophisticated integrated air defense system. While the air- and sea-launched cruise missiles, flying at low altitude, may penetrate hostile airspace, their predictable flight paths and nonstealthy airframes make them vulnerable to interception by advanced SAMs and modern air-to-air fighters.[14]

Cognizant of the increased challenges and the need to forge a stronger team to address the A2/AD challenge, the Air Force Chief of Staff and Chief of Naval Operations signed a memorandum initiating a joint effort to develop a new concept of operations (CONOPS) called "AirSea Battle." Although the memorandum was classified, subsequent wargames and publications suggest that this CONOPS focuses on ensuring the ability to project U.S. military power into the Western Pacific and Persian Gulf. In addition to engaging in conflicts in which adversaries employ A2/AD capabilities, this CONOPS will take into account scenarios that give rise to "overnight" demands for striking targets at intercontinental distances from North America, operations in which prospective adversaries increasingly confront U.S. forces with time-sensitive targets, and situations in which long-range strike systems would need to be able to reach deep targets from the last refueling point.[15] Therefore, an understanding of the complementary capabilities of a family of long-range conventional strike systems is essential to developing the right joint force mix to assure access and successfully fight any future AirSea Battle.

The attributes that the family of long-range strike systems may require will be defined in part by the types of targets they may have to strike in addition to the scenario. The following offers a representative cross section of targets that air and maritime commanders may engage during the early stages of major combat operations.

The 2010 QDR advances a family of systems to underwrite future U.S. power projection capabilities. By expanding the long-range strike solution beyond solely a bomber aircraft, the QDR seeks to provide the joint commander with a range of options to hold at risk fixed and mobile targets over great distances where adversaries seek to protect their territory with state-of-the-art defenses. The value added by each member of this family of systems can be defined, in part, by assessing their contribution to eight operational attributes:

- promptness: reach any target worldwide within 1 hour
- persistence: maintain on station/position for ISR and time-sensitive targeting for more than 4 hours
- time-sensitive: possess organic as well as integrated "find, fix, and track" capabilities to engage fixed or highly mobile targets
- multitarget: engage more than one target nearly simultaneously
- command and control: retasking assets to meet the commander's intent in a denied communications environment
- standoff: achieve desired effects from a range of 1,000 nautical miles or more
- penetration: operate, succeed, and survive within a high threat environment
- nonkinetic: provide options such as electronic attack and cyber capabilities.

## The Family of Long-range Strike Systems

***Expand the Capacity of the* Virginia*-class Attack Submarines.*** Enabled by stealth, the nuclear-powered attack submarine (SSN) has long been recognized as a platform that can penetrate otherwise credible A2/AD zones to conduct ISR and strike operations. U.S. attack submarines are not detectable by most of the sensors deployed to find surface and airborne systems (to include over-the-horizon radar), employ sea-launched cruise missiles such as the conventional Tomahawk, and covertly infiltrate special operations forces. Assuming adequate connectivity and stealth superior to that of the adversaries' submarines and sensors, the SSN, given state-of-the-art weapons and signature, is a capable platform operating autonomously in an area as large as 1.5 million square miles with a 1,000-mile cruise missile. As it sails today, the SSN is a premier conventional long-range strike system when facing an antiaccess environment.

Adding capability to the new *Virginia*-class SSN will make it even more effective as that environment becomes increasingly dangerous. Current plans for the Block 3 (and later) *Virginia*-class submarines are to replace the 12 VLS now hosting the Tomahawk cruise missile with 2 *Virginia* payload tubes (VPT) that can launch 6 missiles from a Multiple All Up Round Canister in each tube. The additional volume provided by the VPT allows the *Virginia*-class SSN to accommodate a larger ballistic missile, adding greater range while cutting the time to target and, simultaneously, improving platform connectivity. The first of these boats, the *North Dakota*, with an improved bow and launcher technologies borrowed from the *Ohio*-class guided missile submarines, is scheduled for delivery in 2014. Such a capability would counter antiaccess threats by being able to hold at risk a range of fixed targets at long ranges from a stealthy stance.

***Experiment with Prototypes of a Naval Unmanned Combat Aerial System.*** The N–UCAS now in development could make significant contributions to conventional long-range strike. This unmanned combat air vehicle (UCAV), about the size of a modern jet fighter, is expected to cruise at 450 knots and operate with a 1,500-nautical-mile combat radius unrefueled, while having the potential to remain airborne for 50 to 100 hours when air-refueled. Planned for the UCAS ISR suite are electro-optical/infrared and infrared search and track sensors, signal collection, and advanced radar capable of electronic attack. Its weapons bay can carry 4,500

pounds and deliver a wide array of air-to-air and air-to-ground munitions.

While UCAS CONOPS are still being shaped, the combination of sensors, range, and weapons could allow the UCAV to detect and track mobile targets out to 100 nautical miles, and, if loitering in hostile airspace, place weapons on target within 15 minutes of tasking. Its sensors are being developed to provide both wide area search and precise tracking of mobile or fixed targets for precision weapons employment, allowing UCAS to operate in a semi-autonomous mode.

The UCAS will be a low-observable airframe with self-protection systems enabling it to operate in an A2/AD environment. If launched from a carrier 1,500 nautical miles from an adversary's shore, the UCAS can operate for 24 hours along a hostile coastline, or penetrate 500 nautical miles inland and loiter for more than 11 hours during a 50-hour sortie with repeated autonomous refuelings. A carrier-based UCAS squadron, composed of 12 air vehicles, could support 5 continuous orbits along the coast or 2.4 continuous orbits 500 nautical miles inland for 24 hours each day. In contrast, a squadron of manned fighter aircraft, owing to human performance limits, could maintain at best only one orbit along the coast.

The most valuable capability UCAS brings to a family of long-range strike systems may be its ability to engage and defeat a time-sensitive target in a matter of minutes owing to its persistence, sensor suite, multiple-target capability, and kinetic or nonkinetic weapons systems. It also offers the joint force the ability to function as a communications relay node in a communications-denied environment, allowing the afloat commander to dynamically adjust the tasking for airborne assets.

***Assess Alternatives for a New Joint Cruise Missile.*** A number of alternatives exist from which a new joint cruise missile program could be pursued to augment U.S. conventional long-range strike capability. In 2002, the Defense Threat Reduction Agency initiated an Advanced Concept Technology Demonstration with the purpose of showing a joint supersonic cruise missile capable of "functionally disabling time sensitive weapons of mass destruction (WMD) targets" as well as hardened and deeply buried targets. Key performance parameters for the demonstrator included a terminal accuracy of 3 meters or better, a range of 400 to 600 nautical miles, a cruising speed in the range of Mach 3.5–4.5, warhead penetration capability, and a single-digit minutes response time. The missile was to be designed to be launched from surface ships, airborne platforms, and submarines.[16]

At least two joint cruise missile platforms may have been developed in response to this request. The U.S. Air Force Research Laboratory has reportedly been testing hypersonic propulsion technology in the X–51A "WaveRider" program under the Rapid Identification and Prosecution of Targets in Denied Environments (RIPTIDE) project.[17] Based on the X–51A missile designed to achieve Mach 6 over a range of several hundred miles, the RIPTIDE range requirements will exceed 1,000 nautical miles to demonstrate long-range, quick-response strike. Envisioned to be launched by a bomber aircraft and incorporating various payloads, a hypersonic cruise missile will need several years of testing before reaching the technological readiness levels suitable for fielding.

A second technology demonstration effort is being conducted by the Office of Naval Research in collaboration with the Defense Advanced Research Projects Agency (DARPA), U.S. Air Force, and National Aeronautics and Space Administration.[18] The Revolutionary Approach to Time-critical Long Range Strike program seeks to develop a cruise missile with Mach 3 speed and a 500-pound penetrating warhead. Although initial flight tests may be restricted to about 5 minutes, implying a range of about 150 nautical miles, desired growth opportunities for the missile call for increased speed (Mach 4), cruise (15 minutes), and range (more than 600 nautical miles). While these objectives suggest the application for such a missile to long-range strike, the flight demonstration vehicle is being designed to show the potential as a tactical weapon.[19] Thus, the missile could be launched from a tactical fighter or from a VLS on a ship or submarine.

Conventional cruise missiles have been used successfully by U.S. forces in recent conflicts. However, their advantages of standoff range have often been offset by the lengthy duration of their subsonic flight (making them impractical to use on a mobile moveable target), their unreliability, their vulnerability, the one-way nature of their mission (they are neither recallable nor recoverable), and, notably, their relative cost per precision round—roughly 80 times the cost of a direct-attack munition. Thus, when budgetary factors are considered, the value of alternative cruise missiles being evaluated for their contribution to a family of long-range strike systems may be dependent on the platform carrying them and how deeply it can penetrate the A2/AD zone before launch to maximize the probability of prompt target destruction.

***Examine Options for a New Air Force Long-range Surveillance and Strike Aircraft.*** Often viewed as the backbone of the Nation's long-range strike capability, the heavy bomber provides a variety of options based on its payload and range. Following the 2006 QDR, an Air Force analysis of alternatives concluded that a bomber built within the next decade could provide a payload capacity of 14,000 to 28,000 pounds and have an unrefueled combat radius up to 3,000 nautical miles while operating in the subsonic flight regime. It would require a mix of low-observable technology and advanced self-protection systems to ensure survivability in an A2/AD environment. If the next-generation bomber (NGB) is to be more a member of a family of long-range strike systems, rather than its sole provider, then these relatively modest capabilities, already at a high level of technological readiness, may suffice.

The NGB also requires a wide area surveillance and search sensor system, plus capabilities to provide precise tracking and engagement of fixed or mobile targets. With a payload three to six times larger than the UCAS, the NGB could strike a wider array and quantity of aimpoints, including deeply buried and/or hardened targets demanding a single 4,800-pound bomb. Loiter time will also matter; therefore, one approach to the NGB may be to have an optional unmanned version. An NGB based 2,500 nautical miles from a tanker orbit 500 miles from an adversary's coast could remain 10 hours along the littoral and penetrate an additional 500 miles inland during a 26-hour mission. If the next-generation bomber were remotely piloted, the total time on station per sortie could match that of the UCAS, with the added value of a significantly greater payload. Like the UCAS, NGB can provide a prompt response during times of heightened tensions from an airborne alert posture.

Perhaps more important, the manned NGB provides combatant commanders with an airborne command and control capability that can operate autonomously with greater flexibility in a denied communications environment. Thus, the NGB could act as the

quarterback for the long-range strike team when in line of sight to the UCAS, *Virginia*-class submarine, and cruise missiles, ensuring a more accurate, timely, and all-azimuth strike. Such a CONOPS suggests that the NGB will not be a B–2–like "lone wolf" aircraft, but rather a weapons system capable of integrating and executing the air and maritime commanders' AirSea Battle gameplan.[20]

***Experiment with Conventional Prompt Global Strike Prototypes.*** The option of conventional prompt global strike (PGS)—usually interpreted as placing conventional warheads on top of existing U.S. land- or sea-based intercontinental ballistic missiles—is probably the most controversial member of this proposed family of systems. Yet the need has been noted, and concrete proposals for acquiring such a capability have been advanced for some time. A February 2007 report issued to Congress by the Secretaries of State and Defense posited that such a capability was desirable, feasible, and acceptable.[21] In fact, the 2010 NPR calls out the need for such a conventional system and the necessity of keeping margins in the nuclear force structure under the arms control treaties to account for the systems. Thus far, Congress has not agreed to field a PGS system, owing principally to a concern that a launch might be misinterpreted by an adversary to be a nuclear attack, provoking an in-kind response.

Nevertheless, there are a number of scenarios that call for a prompt conventional strike on a fixed target: the need to strike a missile launcher poised to attack the United States or an ally, perhaps with WMD; an opportunity to strike key terrorist leaders or a cache of WMD at a time-sensitive moment; or the need to take down elements of an adversary's integrated air and missile defenses prior to a wider assault into an A2/AD region. If the risk to the current inventory of U.S. long-range strike systems is to increase at a pace more rapid than the proposed development and fielding of some of the family members noted above, then the deployment of a prompt global strike capability becomes more important in the near term.

Clearly, a PGS system would provide a niche capability, and measures would have to be instituted to distinguish prompt conventional strike from the triad of nuclear deterrent forces. Land-based conventional intercontinental ballistic missiles (ICBMs) could be deployed on U.S. territory, but not in hardened silos, separated from any nuclear weapons storage facility, and subject to inspection and verification under established arms control regimes. A more futuristic version of a land-based PGS capability envisions an ICBM launching a hypersonic glider that would remain within the atmosphere and use satellite communications to maneuver and deliver a 1,000-pound conventional weapon. With the glide range of these systems and the relatively small size of the reentry vehicle, a single land-based PGS missile could be used to hit multiple targets thousands of miles away. Currently, DARPA is pursuing the Force Application and Launch from Continental United States program, which is intended to demonstrate the flight characteristics of hypersonic glide vehicles launched from a decommissioned Peacekeeper ICBM system. These vehicles are designed to have global coverage from a single continental U.S.–based launch point. Although the first flight test of the vehicle in April 2010 was unsuccessful, DARPA intends to fly a second vehicle to demonstrate the technology in early 2011 to help determine if a deployment date of 2020 is realistic.[22]

Both land- and sea-based PGS systems have political challenges, including arms control limits and nuclear ambiguity. Because of these challenges, limited numbers of systems are expected to be employed. Here, various basing modes (land-based, nuclear-powered cruise missile submarine, *Virginia*-class) and missiles (two-stage SLBM variants, kinetic energy warhead, boost-glide missile, or hypersonic cruise missile) could substantially lower the nuclear ambiguity that has thus far stymied conventional Trident modification development and deployment.[23]

Any prognosis on when the family of systems might be available to the joint force is fraught with budgetary and political uncertainty. Based on reasonable technological and fiscal assumptions, a timetable to begin deploying a family of long-range strike systems could be similar to the accompanying figure.

In analyzing the QDR's directive to expand future U.S. conventional long-range strike capabilities, we have briefly described and compared some of the attributes of the systems suggested in that report. The table reflects a partial evaluation of each of the members of a family of long-range strike systems. Unsurprisingly, the worth of these individual systems varies markedly with the scenario envisioned. Penetrating deep into defended territory, attacking targets from the continental United States or U.S. territory, hitting time-sensitive targets by loitering and surviving in defended airspace, and striking promptly and preemptively can all lead to differing solutions. Given this range

**Figure. Timetable for Deploying Family of Long-range Strike Systems**

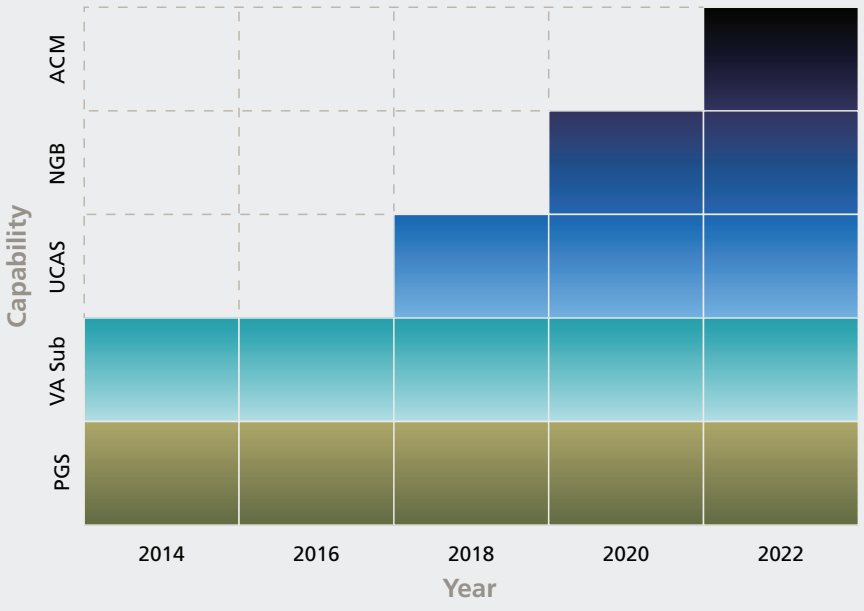


**Table. Summary of Family of System Attributes**

| | Prompt | Persistent | Time-sensitive | Multitarget | Command and control | Standoff | Penetrating | Nonkinetic |
|---|---|---|---|---|---|---|---|---|
| *Virginia*-class submarine | | | | | | | | |
| Unmanned combat aerial system | | | | | | | | |
| Cruise missile | | | | | | | | |
| Next-generation bomber | | | | | | | | |
| Prompt conventional global strike | | | | | | | | |

of requirements, a move away from a single, large, technologically sophisticated, and costly conventional strike platform toward a family of systems offering varied long-range strike options and capabilities appears prudent in a security environment populated by diverse adversaries presenting varied antiaccess challenges.

There is more work to be done, and several studies are under way. One task that we have embarked on with our colleagues is to employ a physics-based model comparing and contrasting the capabilities of these separate family members in an illustrative major combat operation scenario where the joint team must operate in an A2/AD environment. Preliminary runs suggest that a family of long-range strike systems would significantly increase the options available to combatant commanders in an A2/AD environment—from 16 B–2s to 5 additional weapons systems and capabilities offering reduced risk to mission execution and improved assurance of mission accomplishment. An increased capacity *Virginia*-class submarine may be the first of this family of systems that can be fielded. But PGS and advanced cruise missiles offer great promise in the near and longer term to rapidly engage fixed and hardened targets, while UCAS and NGB offer short- and far-term options for the time-sensitive targeting necessary to engage mobile and fleeting targets.

The Secretary of Defense, building on the QDR's findings, was right to direct a study of long-range strike systems to shape future investment decisions. To ensure that U.S. long-range capability does not continue to atrophy in the face of increasingly nonpermissive environments, it is important to accelerate the studies and initiate the investments. **JFQ**

## NOTES

[1] See Robert P. Haffa, Jr., and Michael W. Isherwood, *The 2018 Bomber: The Case for Accelerating the Next Generation Long-Range Strike System*, Northrop Grumman Analysis Center Papers, August 2008.

[2] Department of Defense (DOD), *Quadrennial Defense Review Report* (Washington, DC: DOD, February 2010), 33.

[3] Remarks as delivered by Secretary of Defense Robert M. Gates, Eisenhower Library, Abilene, KS, May 8, 2010, accessed at <www.defense.gov/Speeches>.

[4] See Michael G. Vickers, "The QDR and Long-range Surveillance and Strike," November 10, 2005, available at <www.csbaonline.org/4Publications/PubLibrary/B.20051110.LRSSOvrvw/B.20051110.LRSSOvrvw.pdf>.

[5] For an earlier but more comprehensive analysis, see Andrew F. Krepinevich, Jr., Barry D. Watts, and Robert O. Work, *Meeting the Anti-Access and Area-Denial Challenge* (Washington, DC: Center for Strategic and Budgetary Assessments, 2003).

[6] Anthony H. Cordesman and Adam C. Seitz, *Iranian Weapons of Mass Destruction: The Birth of a Regional Nuclear Arms Race?* (Washington, DC: Center for Strategic and International Studies, 2009), 103–108.

[7] Andrew F. Krepinevich, Jr., *Why AirSea Battle?* (Washington, DC: Center for Strategic and Budgetary Assessments, 2010), 20–21. See also Jan Van Tol et al., *AirSea Battle: A Point of Departure Operational Concept*, available at <www.csbaonline.org/4Publications/PubLibrary/R.20100518.Air_Sea_Battle__A_/R.20100518.Air_Sea_Battle__A_.pdf>.

[8] In 2006, Hizballah effectively used this missile against an Israeli ship. See Krepinevich, 30–31.

[9] Ronald O'Rourke, *China Naval Modernization: Implications for U.S. Navy Capabilities—Background and Issues for Congress* (Washington, DC: Congressional Research Service, October 21, 2009), 6.

[10] Krepinevich, 32–33.

[11] David A. Deptula, *Global Threat Brief*, May 2008.

[12] David Nowak, "Russia Tests 5th-generation Fighter Jet," Associated Press, January 29, 2010.

[13] Deptula.

[14] Various open sources credit the SA–10 target tracking radar with the ability to detect and track low altitude targets, to include cruise missiles. Globalsecurity.org reports that the "76N6S low altitude target search radar/low altitude detector (LAD) is independent for detecting approach of going away air targets, including cruise missiles with small reflecting surface at low and extreme low altitudes under conditions of reflecting signals from objects and effective electronic counter-measures." The SA–10 (S–300) can detect and track targets with a cross section of 0.02 $m^2$. See <www.ausairpower.net/clamshell.html>.

[15] See Barry D. Watts, *The Case for Long-Range Strike: 21st Century Scenarios* (Washington, DC: Center for Strategic and Budgetary Assessments, 2009), accessed at <www.csbaonline.org/4Publications/PubLibrary/R.20090203.The_Case_for_Long-/R.20090203.The_Case_for_Long-.pdf>.

[16] See "Joint Supersonic Cruise Missile (JSSCM)," accessed at <www.patriotfiles.com>.

[17] "USAF Studies Riptide Hypersonic Missile Plan," *Aerospace Daily*, April 14, 2010, 3.

[18] See <www.onr.navy.mil/en/Media-Center/Fact Sheets/RATTLRS>.

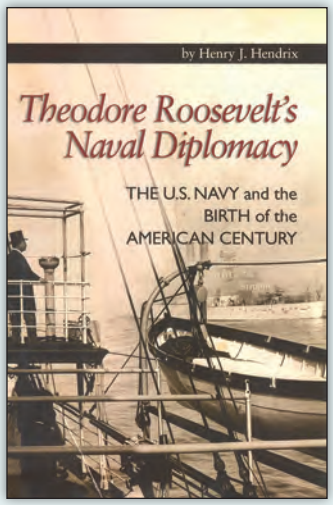
[19] See <www.globalsecurity.org/military/systems/munitions/rattlrs.htm>.

[20] Jason Sherman, "Schwartz: New Bomber Requirements Scaled Back," *Inside Defense*, March 30, 2010.

[21] Secretary of Defense and Secretary of State, *Report to Congress on Conventional Trident Modification (U)* (Washington, DC: DOD, February 1, 2007).

[22] "U.S. Faces Choice on New Weapons for Fast Strikes," *The New York Times*, April 23, 2010, A1.

[23] *U.S. Conventional Prompt Global Strike: Issues for 2008 and Beyond* (Washington, DC: The National Academies Press, 2008). See also Bruce M. Sugden, "Speed Kills: Analyzing the Deployment of Conventional Ballistic Missiles," *International Security* 34, no. 1 (Summer 2009), 113–146.




**Theodore Roosevelt's Naval Diplomacy: The U.S. Navy and the Birth of the American Century**

*By Henry J. Hendrix*

Annapolis: Naval Institute Press, 2009
230 pp. $34.95
ISBN: 978–1–59114–363–5

*Reviewed by*
THOMAS BRUSCINO

Henry J. Hendrix has found a fascinating topic for historians and senior military officers with *Theodore Roosevelt's Naval Diplomacy*. The book explores the intersections among policymaking, diplomacy, military force, and technological development. At the center of it all stands Roosevelt, and in effect the book as a biography focuses on the essential role naval power played in Roosevelt's life, thinking, and political career.

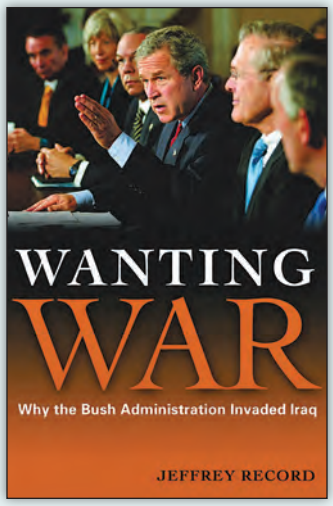
Roosevelt's interest in naval affairs began early in his life, sitting at the knees of two uncles as they told stories of their service in the Confederate navy during the Civil War. His budding interest only grew in adulthood when he became a careful scholar of naval history and author of *The Naval War of 1812*, a book that still ranks among the most important on the topic. In the course of his studies, Roosevelt anticipated and agreed with the arguments of Alfred Thayer Mahan. Both believed that history showed that maritime power was essential to national security and prosperity, and when Roosevelt moved into positions of influence and power, he rigorously and coherently put those ideas into practice. As Hendrix points out, from early on, Roosevelt recognized the inextricable link between what he wanted the Navy to do and what the Navy actually could do. He knew that without a sufficient number of ships and the appropriate level of naval technology, all the intentions in the world did not matter. So as he ascended from Assistant Secretary of the Navy to Vice President to President, Roosevelt pushed for the expansion and development of naval forces and technology.

More importantly, Roosevelt used the available ships and technology to great effect, as Hendrix shows in several examples. The first instance came prior to the actual outbreak of war with Spain in 1898, when Assistant Secretary Roosevelt sent the squadron under Commodore George Dewey into a position to attack the Spanish fleet in Manila, allowing the United States to expand its influence in the Pacific. Interestingly, as Hendrix argues, that war would end up being about the only example of the actual employment of force in Roosevelt's use of naval power. Most of the time, the judicious application of the threat of force did the job, and Roosevelt made good use of the Navy in support of his diplomatic agenda. Hendrix's second example, the Venezuelan crisis of 1902–1903, saw Germany (and, to a lesser extent, Great Britain) trying to insert itself into the Western Hemisphere under the guise of collecting outstanding debts from Venezuela. Roosevelt demanded that the Germans accept arbitration on the issue, and when the Kaiser ignored the demand, Roosevelt gathered the squadrons along the Atlantic into a single fleet under the command of Admiral Dewey and had them run exercises in the Caribbean. The demand became an ultimatum, and the Germans acquiesced. The year 1903 provided another example of Roosevelt's use of naval diplomacy, this time as the Panamanians declared independence from Colombia. With an eye toward building and running the Panama Canal, the American President sent ships and Marines, including the commandant of the Marine Corps himself, to deter the Colombians from using military force to quell the rebellion.

Roosevelt had to be more circumspect when a bandit in Morocco kidnapped an American citizen for ransom. Even then, the threat of assault from the sea, either to coerce the Moroccan government or to launch a punitive raid directed at the bandit, played a key role in resolving the dilemma. Likewise, applied naval force had little to do with Roosevelt helping to negotiate the peace at Portsmouth, New Hampshire, between Russia and Japan, but his acute understanding of the link between diplomatic leverage and military power gave him great insight in his Nobel Peace Prize–winning efforts. His final major national security gesture as President became his most famous use of naval forces to support American national power. The sailing of the Great White Fleet around the world was largely symbolic, but it was a powerful symbol and a perfect capstone to a career dedicated to the belief that national security and prosperity were derived from maritime power.

Hendrix provides a concise, readable, and analytically astute narrative of Roosevelt's remarkable career. He is less successful in his somewhat rushed conclusion in linking these events to current affairs, but that has little effect on the overall value of the book to historians and military professionals. All too often, we discuss leveraging the diplomatic, information, military, and economic elements of national power as if those elements were somehow independent and equal in peacetime policymaking and wartime strategy-making. It is exceedingly useful to have an example of a historical policymaker who pursued policies that intertwined diplomacy and the threat of military force with an eye toward security and economic implications. Equally important and telling was the military's role in all of this: by preparing for war, not debating policy decisions, the U.S. Navy gave the President options and made clear when some options were not feasible. For telling this story, Henry Hendrix is to be applauded. **JFQ**

**Thomas Bruscino is an Assistant Professor of Military History at the U.S. Army School of Advanced Military Studies.**




**Wanting War: Why the Bush Administration Invaded Iraq**
*By Jeffrey Record*
Washington, DC: Potomac Books, Inc., 2010
217 pp. $24.95
ISBN: 978–1–59797–437–0

*Reviewed by*
JOSEPH J. COLLINS

President John F. Kennedy reminded scholars and pundits of their limits: "The essence of ultimate decision remains impenetrable to the observer—often, indeed, to the decider himself. . . . There will always be dark and tangled stretches in the decision-making process—mysterious even to those who may be most intimately involved" (Allison and Zelikow, *Essence of Decision*, 1999). The young President, himself an author of note, knew the difficulties of reconstructing the past and the delicate complexities of navigating the shoals of motivation. It is nevertheless imperative that national decisions, policies, and operations be dissected, analyzed, and assessed, lest we repeat our mistakes, a common failing of great powers.

Jeffrey Record, an Air University scholar-practitioner with impeccable credentials, has taken up that challenge on the war in Iraq. Drawing on the growing record of how we entered into our second war with Iraq, Record has produced an excellent interpretative analysis of the rationale for the George W. Bush administration's invasion of Iraq. Along with the post-Inchon phase of the Korean War and the Vietnam conflict, Record believes that Operation *Iraqi Freedom* was America's third costly and unnecessary war of choice. In a scorching attack on the neoconservative reasoning underpinning the war, Record's central thesis is that the decision to invade was:

*more about the United States than about Iraq. Specifically, the invasion was a conscious expression of America's unchecked global military hegemony that was designed to perpetuate that hegemony by intimidating those who would challenge it. The invasion represented power exercised first and foremost for its own sake.*

Record skillfully weaves insights from many previous studies, including my own (*Choosing War*, INSS Occasional Paper No. 5 [NDU Press, April 2008]), into his narrative. The heart of his book is the nearly 70-page chapter 4, "The Reasons Why." There, the author discusses the rationale, aims, objectives, and motives of the war. Among the "reasons why"—and I draw on his terminology spread over a few dozen pages—he analyzes the need to redeem the false victory in *Desert Storm*, demonstrate a new willingness to use force, assert the principle of preventive military action, intimidate North Korea and Iran, promote political reform in the region, create a regional alternative to Saudi Arabia, eliminate an enemy of Israel, vindicate defense transformation, and reestablish the imperial presidency. Record concludes by looking at the consequences of the war, which he believes will be regarded as "a horrible mistake."

The final few pages of the book assess the war in Iraq in light of the Weinberger Doctrine. Record wisely concludes that the war violated the doctrine's prudent prescriptions, but that doctrine itself is not an accurate gauge for assessing future cases where the use of force may be necessary.

While one may salute Record's attempt to get at the root causes, it is also important to pay attention to what the people who made or contributed to these decisions were thinking at the time. For example, in the Pentagon in 2003, we told ourselves that invading Iraq was about the "3 Ts plus WMD:" *threats* to the region from Iraq, the *tyranny* of Saddam's regime, its support to *terrorist* groups, and of course, Iraq's stockpile of weapons of mass destruction (WMD) and its research and development programs. The WMD issue created the sense of urgency, and its veracity in our eyes had been validated by the October 2002 National Intelligence Estimate on Iraqi weapons of mass destruction. It is easy to dismiss this thinking today, but the climate of fear in the country and among national decisionmakers in 2002 was sufficiently strong to warp both visions of the future and the decisionmaking process.

Under fear and pressure, smart people can do things that in retrospect appear stupid. While postwar studies can and should create elaborate maps to the rationale that underpins decisions, the actual decisionmaking process is messier and warped by bureaucratic pathologies. There are often as many prime motives as there are senior participants in the process. Learning takes place but often does not insulate an administration from making mistakes. Important warnings that do not fit preconceptions are ignored. Scholars of decisionmaking have to restrain themselves. Things are not always subject to strict tests of rationality. Without prudent judgment, scholars can impose too much order on the confusion that is modern-day policymaking.

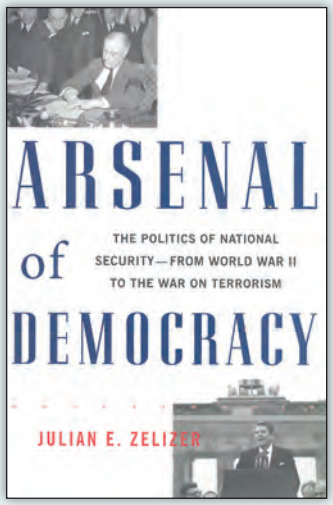
Record makes a valuable contribution to the literature on the underlying rationale behind the invasion, but he would, I am sure, agree that much work remains to be done. Picking up the banner, the U.S. Army War College's Strategic Studies Institute is working on a series of 10 or more monographs to comprehensively examine the strategic decisions related to the war. The *Operation* Iraqi Freedom *Key Decisions Monograph Series*, edited by Colonel John R. Martin (Ret.), is off to a great start with two important volumes by Steven Metz, the first on the decision to go to war (*Decisionmaking in Operation* Iraqi Freedom: *Removing Saddam Hussein by Force*) and the second on the Surge (*Decisionmaking in Operation* Iraqi Freedom: *The Strategic Shift of 2007*). The U.S. Naval Institute Press has done its part by publishing John Ballard's 2010 book, *From Storm to Freedom: America's Long War with Iraq*, which will help to create a fuller narrative by taking the reader from Operation *Desert Storm* in 1990–1991 to the current war.

The war in Iraq continues, and it remains difficult to draw a final conclusion on our efforts there. Jeffrey Record's book provides a useful placeholder:

*The experience of the Iraq War almost certainly will diminish America's appetite for the kind of interventionist military activism that has characterized post–Cold War U.S. foreign policy, especially that during the Clinton and George W. Bush administrations. … Future enemies undoubtedly will attempt to lure the United States into fighting the kind of… messy wars into which it stumbled in Vietnam and Iraq. But if such*

*wars are wars of choice rather than wars of necessity for the United States, it should think more than twice before entering them.* **JFQ**

**Joseph J. Collins teaches strategy at the National War College. He was the Deputy Assistant Secretary of Defense for Stability Operations from 2001 to 2004.**




**Arsenal of Democracy: The Politics of National Security—From World War II to the War on Terrorism**
*By Julian E. Zelizer*
New York: Basic Books, 2009
583 pp. $35
ISBN: 978–0–465–01507–8

*Reviewed by*
JORDAN MICHAEL SMITH

According to realism, the dominant form of American international relations theory since the discipline first emerged, countries act primarily in response to the anarchical structure of the international system. In *Arsenal of Democracy*, Julian Zelizer subtly aims to upend that belief. He argues that, far from being an incidental factor in foreign policymaking, domestic factors have always been prominent: "Even during the Cold War," that supposed golden era of bipartisanship, "partisan and intra-partisan competition over national security was much stronger than most accounts suggest" (p. 4). From Franklin Roosevelt to Barack Obama, there has rarely, if ever, been a period of national consensus over international affairs, Zelizer claims.

Zelizer, a Princeton political historian, argues that Democrats have oscillated between two foreign policy agendas—one emphasizing the FDR- and Truman-nourished commitment to liberal internationalism, and the other more skeptical toward military intervention after Vietnam. Republicans, meanwhile, have bounced between an isolationism wary of foreign commitment and a large security state, and a unilateral internationalism bordering on militarism (pp. 5–6).

Zelizer is a Democrat who clearly favors the liberal internationalist approach he outlines, but he recognizes that it is not without flaws. Because it prioritizes alliance and diplomacy, a traditional liberal foreign policy is particularly susceptible to demagogic charges of softness and even treason from the right wing. In the book's telling, the midterm elections of 1950 destroyed the Democrats' sense of self-confidence: "The wounds that Republicans inflicted during these elections would not heal for many decades. Psychologists talk about how entire generations can be emotionally scarred as a result of living through war. The story is much the same in these formative years of the Cold War. Democrats would not for decades feel secure with the issue of national security as they had under FDR and, for a while, under Truman" (p. 120). The election also permanently transformed the Republicans: the "GOP, internalizing the arguments of the Republican Right, crossed a threshold in how far it was willing to go in calling Democrats weak on national security and in making partisan use of the issue."

The 1950 election traumatized two Democratic Senators (and eventually Presidents) of particular note: John F. Kennedy and Lyndon Johnson. Both men were terrified of appearing soft on national security, and as a result felt unable to retreat from Vietnam (though Zelizer is clear that Johnson also believed abandoning South Vietnam would be disastrous for national security reasons). The trauma of the Vietnam War, in turn, shell-shocked Democrats into being wary of using force abroad, which further hampered their credibility on national security in the eyes of the electorate.

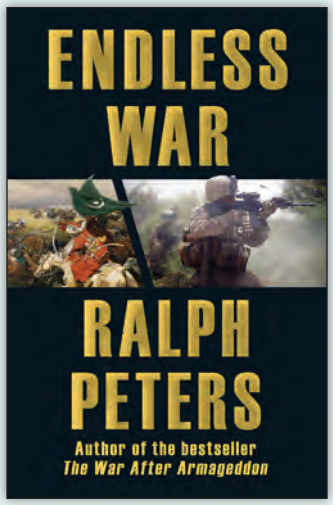
None of this is exactly new, but never before has anybody laid out so comprehensively the partisan debates over foreign policy. After reading Zelizer's book, it is impossible to believe that a bipartisan foreign policy has ever existed for more than brief, rare periods. Security challenges have *always* been matters that parties and politicians fought over and sought to leverage electorally. More depressingly, both parties have been persistently willing to put electoral concerns ahead of national security interests. Many Republicans at the time knew Eugene McCarthy was lying but kept quiet because his smears were effective. Similarly, if less ruinously, many Democrats attacked the Bush administration in 2006 for letting operations at major American ports be bought by a Dubai company, even though they understood the acquisition brought no actual threat to national security.

Among the most exciting attributes of *Arsenal of Democracy* is its grasp of the relevant literature. On everything from Vietnam to Iraq, Zelizer uses the most recent, accurate, respected scholarship. Time and again one jumps to the endnotes to check the source of a novel quotation, only to be impressed with the breadth of research undertaken. Nearly as impressive is the book's even-handedness. Though Zelizer is a liberal, he is critical of liberalism and can be complimentary toward conservatives. The only real exception is Ronald Reagan, who is not given enough credit for bucking his base and recognizing early on that Mikhail Gorbachev was indeed a different type of Soviet leader. The book is highly critical of President George W. Bush (justly, in my view), and sees the present as an opportunity for the Democrats to rebrand themselves as the party that can once again be trusted to secure the country.

The book does not quite answer realism's charge. Zelizer never explores why American voters preferred certain stances—say, zealous anticommunism in 1950—over others. A realist might say that, in a democracy, voters and elites will likely support policies that give their state power and security. Indeed, with the book's thesis being that America's two major parties have always fought over national security credibility, *Arsenal of Democracy* could be taken as evidence of the power of the international system to influence a state's behavior. I would argue that the anarchical world causes American voters to seek security.

In any case, Zelizer's book is not primarily theoretical, but historical. And as history it is consistently readable and important. It deserves a wide readership. **JFQ**

**Jordan Michael Smith is a writer living in Washington, DC.**




**Endless War: Middle Eastern Islam vs. Western Civilization**
*By Ralph Peters*
Mechanicsburg, PA: Stackpole Books, 2010
273 pp. $27.95
ISBN: 978–0–8117–0550–9

*Reviewed by*
SAM J. TANGREDI

For more than a decade, Ralph Peters has been one of America's finest essayists—an analyst and commentator with a novelist's skills. This is not something a member of the literati might admit because Peters writes about the true nature of war, not a popular subject outside an audience of national security professionals. But his eloquently phrased insights on current defense issues are now being publicly sought, particularly at conferences and panels that want at least one known contrarian. And as in his books, Peters never fails to deliver what they seek.

*Endless War* is different in at least two respects from his other book-length collections of articles and commentaries previously published in journals. First, it contains a number of shorter articles—some previously appearing in the military history journal *Armchair General* and online. Second, although Peters has often written about conflicts and contradictions of militant Islam and about wars of religion, *Endless War* goes further into political incorrectness by using an "inconvenient truth"—*Middle Eastern Islam vs. Western Civilization*—as the subtitle. Peters discusses this religious-cultural conflict as much from a historical perspective as from a current view. His lead essays are assessments of historical wars in which Islamic forces won or lost, and he discusses some of the tactics they used. But the underlying message of this new book suggests that in this endless religion-fueled conflict, the best the West can do is hold to a policy of deterrence and defense of national interests, and that a truly peaceful resolution can only come about by—metaphorically speaking—divine intervention.

However, Peters's publisher wimped out. You will find the subtitle on the title page, but it is nowhere on the cover. In fact, not every essay discusses militant Islam, which makes it a more broadly interesting book.

Particularly thought-provoking is the essay "Better than Genocide," in which Peters suggests that ethnic cleansing—defined as the separation of warring tribes or hostile ethnic groups—may be the only way of stopping conflicts in failed states. The reality is that this is exactly what happened in Bosnia and Kosovo despite efforts by the United States, United Nations, European Union, and North Atlantic Treaty Organization (NATO) to prevent it—another inconvenient truth. In African countries whose borders were set mostly arbitrarily by colonial powers, redrawn borders (a diplomatic taboo) and ethnic separation would seem to be acts of mercy. This is not something citizens of functioning multi-ethnic societies such as our own seem able to grasp. Since ethnic cleansing is often confused with genocide and cannot lose its bad connotations in modern minds, Peters inevitably backs off a bit on his support and leaves it as an idea to consider.

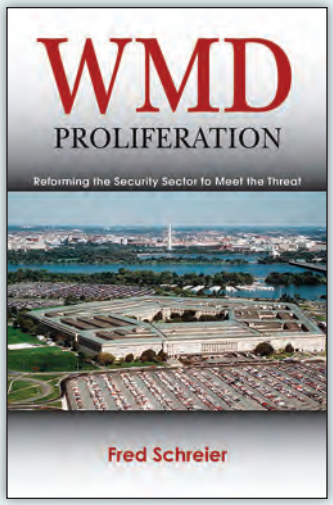
More entertaining, but with a serious point, is the essay "The Geezer Brigade," in which Peters outlines a method of recapturing operational knowledge and experience by allowing retired officers and noncommissioned officers to return to Active duty as advisors and mentors, albeit in a unique rank.

Despite the apparent strategic successes of the current commander of U.S. Central Command and commander of NATO/U.S. European Command, Peters rails against officers with Ph.D.s. His experience with Army officer Ph.D.s leads him to conclude that they are so wedded to academic theories with no validity in war that they have "learned to lose." I think he might think differently if he had met a Navy Ph.D., but a commitment to jointness prevents me from pursuing that further. Yet at the same time, Peters points out that being a good operator does not necessarily make one a good strategist, and he asks, "Where are the strategists?" The best source would seem to be a blend of operators who are war college graduates sprinkled with a few operationally experienced strategy-related Ph.D.s.

Other essays remain true to the author's commitment to demolishing myths and evangelizing the bloody truth about wars in which we must fight, and choices we need to make to defend our nation and its allies and partners. As profane as it might sound, his prose almost makes it fun to contemplate serious defense issues and controversies. Who else would describe the commander of U.S. Joint Forces Command as conducting an "over-the-beach assault" on effects-based operations? Peters skewers the wishful-thinking-as-strategy of the Donald Rumsfeld Pentagon and the George W. Bush administration, making "doing the right thing (removing Saddam) look like bullying justified by lies" by cramming "all of its justification eggs into one basket—then waiting for the WMD bunny to appear." One area of unstinting praise, however, is Peters's judgment and support for our troops engaged in the fight, and the dedication of the individual Servicemember.

Assessing convoluted and ultimately marginally successful strategies, Peters sets an initial standard for sound strategy that should always be kept foremost in mind: We need to be able to "define the mission in plain English." A great read, *Endless War* can hardly be considered plain writing, and it is its passion and engaging turns of phrase that give it a more profound impact than competing volumes. **JFQ**

**CAPT Sam J. Tangredi, USN (Ret.), is Director, San Diego Operations, for the planning-consulting firm Strategic Insight. He is the author of several books on defense strategies, including *Futures of War: A Consensus View of the Future Security Environment, 2010–2035* (Alidade Press, 2008).**




**WMD Proliferation: Reforming the Security Sector to Meet the Threat**
*By Fred Schreier*
Washington, DC: Potomac Books, Inc., 2009
352 pp. $60.00
ISBN: 978–1–59797–421–9

*Reviewed by*
JEFFREY L. CATON

Proliferation of weapons of mass destruction (WMD) remains a critical consideration in the security strategies of many countries. Once the property of only a few large states, the reality of WMD today is that some small countries and nonstate actors seek them to bolster their influence and perceived credibility, possibly by committing horrific acts with them.

In his preface, Fred Schreier states a relevant and timely thesis focused on how a state's security sector should reform "to counter the preeminent threats posed by the unholy trinity of proliferation of WMD, terrorism, and organized crime." Schreier, a consultant of the Geneva Centre for the Democratic Control of Armed Forces, has both the academic background and practical defense-related experience to examine this challenge. He tackles his thesis by organizing his book into two parts: Part I, "The WMD Threat," and Part II, "Reforming the Security Sector." Schreier is successful in describing the threat within the context of his proposed "unholy trinity," especially in conveying the complexity of the international security environment. He is less successful in offering solutions that are unique to WMD proliferation, and while he advocates logical approaches, his recommendations lean more toward business as usual rather than true reform.

Part I provides appropriate background on the various forms and technical nature of WMD, with chapters on nuclear, chemical, biological, and radiological weapons. Schreier argues that the goal of "new terrorists" is to pursue maximum damage and casualties, something avoided in the past to prevent negative international backlash. He connects this new paradigm to the ability, motivation, and willingness of international organized crime to facilitate the proliferation of WMD, thus providing persuasive evidence of his unholy trinity. Part I both describes specific WMD threats and touches on some of the dilemmas governments face in protecting citizens from attack, accurately attributing attacks, controlling dual-use technologies (such as medical radiology), and disarming the WMD of traditional military powers. The concise presentation of these subjects serves as a broad primer for the novice or as a quick review for readers already familiar with WMD. In either case, the endnotes offer a wealth of details and sources for further research.

Schreier dedicates most of Part II to addressing security measures required to meet the threat he describes. He notes that the intricate nature of less predictable menaces has forced states to shift their strategy from risk avoidance to risk management. He examines the National Security Council and its supporting committees as an example of an appropriate strategic decisionmaking construct. He then analyzes how the intelligence services should transform to meet the new threat, characterized by its clandestine nature, privatization of violence, exploitation of asymmetry, and transnational reach and impact. During the Cold War, intelligence services focused on solving puzzles—pursuing certain answers—but now the focus must be on solving mysteries—pursuing uncertain or changing answers. Parts of these answers are often embodied in resolutions and treaties; Schreier discusses how countries' legislative bodies in turn should translate such international agreements into domestic law. To be fully effective, all this must be in concert with national interests and policy; he outlines a structure with four strategy pillars—defeat, deter, diminish, and defend.

Turning to the modern security sector writ large, the author effectively imparts its intricacy to the reader, but diverges in his discussion on law enforcement, border management, and criminal activity without explicit connection to the WMD theme. In a chapter on homeland defense, he advocates approaches that leverage systems analysis and integration as well as private-public partnership, but unfortunately provides limited details that do not address WMD-unique issues. Schreier's final discourse analyzes five obstacles to international and interagency collaboration and advocates methods to overcome them, including a move from bilateral to multilateral intelligence-sharing. While he provides supporting facts, they are limited to applications in well-established fora in Western Europe (such as the North Atlantic Treaty Organization and European Union) and do not address the crucial issue of how to balance collaboration with sovereignty. A complete approach to the unholy trinity threat must include partnerships with countries on all continents.

In summary, Part II makes a good case for holistic approaches to security challenges, emphasizing collaboration at all levels to identify and address multifaceted threats such as WMD proliferation. However, the recommendations are largely generic with few specific WMD implications, and they do not address the full scope of the problem—such as what resources are available, what other security issues are competing for them, and how these needs are balanced and prioritized. At times, the text is difficult to read due to choppy organization and peripheral themes that detract from the content. The experienced security professional may want to skim these chapters and read the notes and bibliography in detail.

A reader who expects this book to reveal radically new methods for the international security sector to meet the threat of WMD proliferation will be disappointed. True reform suggests a different way of doing things, perhaps focused on the way the threat has evolved. This book offers mostly traditional bureaucratic "top down/bottom up" solutions that may work given unlimited time, resources, and a cooperative foe. However, the details provided may be useful for a reader who desires to gain an appreciation for the complexity of such challenges, or requires a contextual foundation to guide and inspire brainstorming toward new approaches to address WMD proliferation or similar security quandaries. Schreier's book may hold considerable merit for such an audience.

**Colonel Jeffrey L. Caton, USAF, is a faculty member and Defense Transformation Chair at the U.S. Army War College.**

# Joint Chiefs of Staff J7, Joint Education and Doctrine Division

*By* EDWARD L. PEARCE

As military professionals charged with the defense of the Nation, joint leaders must be true experts in the conduct of war. They must be individuals both of action and of intellect, skilled at "getting things done," while at the same time conversant in warfare. Every joint leader is expected to have a solid foundation in military theory and philosophy. Most have or should have studied Sun Tzu, Thucydides, Antoine-Henri Jomini, and Carl von Clausewitz. However, when asked, most would give differing definitions of *war* and *warfare*. The upcoming Joint Publication (JP) 1, *Doctrine for the Armed Forces of the United States*, will define war and warfare.

*War* is socially sanctioned violence to achieve a political purpose. History has demonstrated that war is an integral aspect of human culture and that its practice is not linked to any single type of political organization or society. The basic nature of war is immutable, although warfare evolves constantly.

Conflict is the normal state of global human relations. Thomas Hobbes stated that man's nature leads him to fight for personal gain, safety, or reputation. Thucydides said nearly the same thing in a different order, citing fear, honor, and interest as the precipitating causes for interstate conflict.

Nations, cultures, and organizations all have interests. Inevitably, some of those interests conflict with the interests of other nations, cultures, or organizations. Nearly all international and interpersonal relationships are based on power manifest through politics. Power and self-interests control the otherwise anarchic international environment. States exercise their power through diplomatic, informational, military, and economic means—they exercise statecraft. All forms of statecraft are important, but as conflicts approach the requirement for the use of force to achieve the state's interests, military means become predominant and war can result.

As an integral aspect of human culture, war has been defined and discussed in a myriad of contexts. As an element of statecraft, it has groundings in U.S. and international law and treaty. Classic scholars such as Sun Tzu and Clausewitz provide valuable perspectives necessary to a more complete understanding of the nature of war and both directly impact the manner in which the United States understands war.

Clausewitz believed that war is a subset of the larger theory of conflict. He defined war as a "duel on a larger scale," "an act of force to compel our enemy," and a "continuation of policy by other means." Distilled to its essence, war is a violent struggle between two (or more) hostile and independent wills, each trying to impose itself on the other. Simply put, war is a violent clash of wills. Clausewitz believed that war is characterized by the shifting interplay of a trinity of forces (primordial violence, hatred, and enmity) connected by principal actors that comprise a social trinity of the people, military forces, and the government. Clausewitz noted that the conduct of war combines obstacles such as friction, chance, and uncertainty. The cumulative effect of these obstacles is often described as "the fog of war." These observations remain true today and place a burden on the commander to remain responsive, versatile, and adaptive in real time to seize opportunities and reduce vulnerabilities. This is the art of war.

According to Sun Tzu, war is categorized as "a matter vital to the State; the province of life or death; the road to survival or ruin." To assess its essentials, he suggests that we analyze the five fundamental factors of war: moral influence (will), weather (fog of war), terrain (friction), command (leadership), and lastly, doctrine (organization, command and control, and planning). He further posits that "what is of supreme importance in war is to attack the enemy's strategy."

*War* is a noun. *Warfare*, however, feels like a verb. It is the mechanism, method, or modality of armed conflict against an enemy. It is "the how" of waging war. Warfare changes as rapidly as the means to wage war and the societies that wage war—that is to say, nearly continuously. Historian John Keegan has offered that war is a universal phenomenon whose form and scope are defined by the society that wages it. The changing "form and scope" of warfare give value to delineating the distinction between war and warfare.

Understanding the changing nature of warfare provides the context in which wars are fought. Context helps combatants make the right choices as to such essential matters as force structure, force preparation, conduct of campaigns and operations, and rules of engagement. The United States delineates two basic forms of warfare: traditional and irregular. The delineating purpose of each is the strategic focal point of each form. As war is a duality, all forms of warfare have offensive ("pushing an adversary") and defensive ("resisting an adversary's push") aspects.

*Traditional* warfare is defined as a violent struggle for domination between nation-states or coalitions and alliances of nation-states. This form is labeled traditional because it has been the dominant form of warfare in the West since the Peace of Westphalia (1648) reserved, for the nation-state alone, a monopoly on the legitimate use of force. The strategic purpose of traditional warfare is the imposition of our will on adversary nation-state(s) and to avoid their will being imposed upon us.

*Irregular* warfare is characterized as a violent struggle among state and nonstate actors for legitimacy and influence over the relevant population(s). This form is labeled irregular in order to highlight its non-Westphalian context. The strategic point of irregular warfare is to gain or maintain control or

**Lieutenant Colonel Edward L. Pearce, USA, is a Joint Doctrine Planner in the Joint Chiefs of Staff J7, Joint Education and Doctrine Division.**

influence over, and the support of, a relevant population.

The military profession demands lifelong learning. Doctrine provides a common taxonomy from which to baseline one's knowledge. Shortly after the Gulf War, General H. Norman Schwarzkopf was asked, "What qualities does a 21st-century leader need?" General Schwarzkopf replied, "Competence and character." Competence starts with an understanding of what we do (war) and how we wage war (warfare). **JFQ**

**For access to joint publications, go to the JDEIS Web portal at https://jdeis.js.mil (.mil users only). For those without access to .mil accounts, go to the Joint Electronic Library Web portal at http://www.dtic.mil/doctrine.**

## JPs Revised or Under Review

**JP 1**, *Doctrine for the Armed Forces of the United States*
**JP 1–0**, *Personnel Support to Joint Operations*
**JP 1–04**, *Legal Support to Military Operations*
**JP 2–01**, *Joint and National Intelligence Support to Military Operations*
**JP 2–01.2**, *Counterintelligence and Human Intelligence Support to Joint Operations*
**JP 2–03**, *Geospatial Intelligence Support to Joint Operations*
**JP 3–0**, *Joint Operations*
**JP 3–01**, *Countering Air and Missile Threats*
**JP 3–02.1**, *Amphibious Embarkation and Debarkation Operations*
**JP 3–03**, *Joint Interdiction*
**JP 3–05**, *Doctrine for Joint Special Operations*
**JP 3–07**, *Stability Operations*
**JP 3–07.2**, *Joint Tactics, Techniques, and Procedures for Antiterrorism*
**JP 3–08**, *Interagency, Intergovernmental Organization, and Nongovernmental Organization Coordination during Joint Operations*
**JP 3–09**, *Joint Fire Support*
**JP 3–13**, *Information Operations*
**JP 3–13.2**, *Psychological Operations*
**JP 3–13.3**, *Operations Security*
**JP 3–13.4**, *Military Deception*
**JP 3–15**, *Barriers, Obstacles, and Mine Warfare for Joint Operations*
**JP 3–15.1**, *Counter–Improvised Explosive Device Operations*
**JP 3–16**, *Multinational Operations*
**JP 3–22**, *Foreign Internal Defense*
**JP 3–31**, *Command and Control for Joint Land Operations*
**JP 3–33**, *Joint Task Force Headquarters*
**JP 3–34**, *Joint Engineer Operations*
**JP 3–41**, *Chemical, Biological, Radiological, Nuclear, and High-Yield Explosives Consequence Management*
**JP 3–50**, *Personnel Recovery*
**JP 3–61**, *Public Affairs*
**JP 3–68**, *Noncombatant Evacuation Operations*
**JP 4–01.2**, *Sealift Support to Joint Operations*
**JP 4–01.5**, *Joint Tactics, Techniques, and Procedures for Transportation Terminal Operations*
**JP 4–01.6**, *Joint Logistics Over-the-Shore (JLOTS)*
**JP 4–02**, *Health Service Support*
**JP 4–03**, *Joint Bulk Petroleum and Water Doctrine*
**JP 4–05**, *Joint Mobilization Planning*
**JP 4–06**, *Mortuary Affairs in Joint Operations*
**JP 5–0**, *Joint Operation Planning*
**JP 6–01**, *Joint Electromagnetic Spectrum Operations*

# The Joker Is Wild
# Managing Assumptions in Planning and Execution

*By* JEFFERY E. MARSHALL

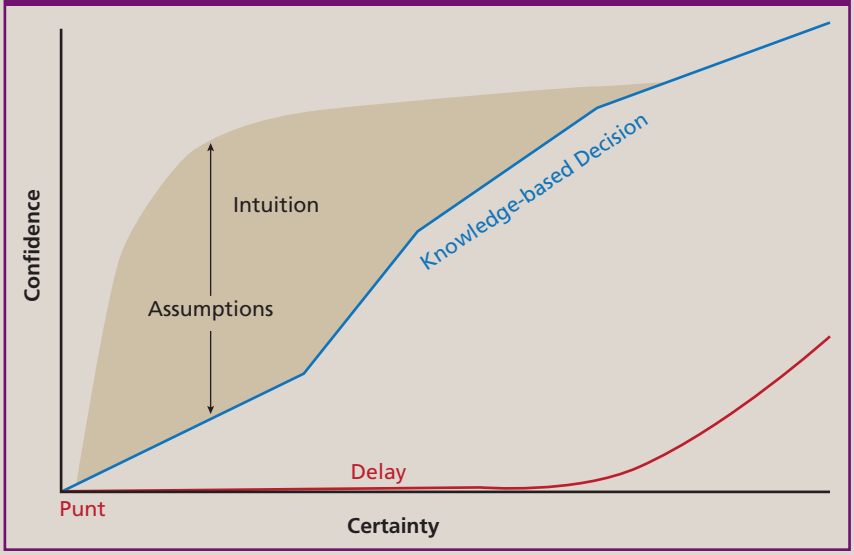
As the old adage goes: to *assume* is to make an *ass* out of *you* and *me*. It is equally applicable to the *development* of assumptions, and we should keep that in mind as we plan and make decisions. Assumptions that are misunderstood, not validated, and poorly managed will likely lead to havoc. In war, bad assumptions can do much more than make you look the ass—havoc kills the wrong people.

History is replete with examples of assumptions that were neither tested and validated nor balanced with a branch plan to execute if the assumptions proved incorrect. For example, in World War I, the German Schlieffen Plan assumed that the British would not intervene and that the French could be defeated in 6 weeks. The Germans were wrong on both counts. The British intervened, the French held on, and a bloodbath ensued. The untested assumptions in Operation *Iraqi Freedom*, such as the Iraqi populace welcoming the invasion force with open arms and the presence of weapons of mass destruction, are noteworthy as well.

Assumptions are more than just best-guess factors required to continue the planning process. As Joint Publication (JP) 5–0, *Joint Operation Planning*, points out, assumptions are suppositions that we require in the absence of facts in order to plan. In many cases, these suppositions drive operational success or failure, and the inability either to understand or to manage assumptions can open the door for significant problems, or even catastrophic failure.

Assumptions are a critical part of both the decisionmaking and decision execution processes. The new concept of operational design makes assumption management even more critical than the deliberate decisionmaking process. Operational design places emphasis on intuition and less structured, more creative decisionmaking and is absolutely critical for success in the complex joint interagency, intergovernmental, multinational (JIIM) environments that our forces will operate in. However, we must understand not only the explicit assumptions the commander and staff make during operational design, but also the implicit assumptions inherent in a less structured decision that are often unstated and perhaps not even recognized. These implicit assumptions could significantly impair an operation if they are not understood and managed properly.

**Figure 1. Decisionmaking under Uncertainty**




General James Mattis, in his introductory letter on operational design, discusses the need for creativity and critical thinking rather than mechanistic processes.[1] Figure 1 shows the relationship between intuition and knowledge-based, structured decisions. Intuitional decisionmaking requires the commander and staff to make assumptions to span knowledge gaps. The commander's intent must drive the entire process in order to guide and prioritize the staff's efforts.

Once the decision is made, however, a certain amount of structure is absolutely required to execute the decision effectively and continue to adapt to changing circumstances. The staff must use the science part of decisionmaking to understand the knowledge gaps that require assumptions and to develop required branch plans to hedge risk. This article focuses primarily on understanding both explicit and implicit assumptions and their management, and it provides a structure for their management.

As we develop the doctrine to support more effective assumption management, we must update the corresponding knowledge management (KM) doctrine and capabilities. This is not simply a technical process. It must entail a complete review of our approach to decision support that includes not only the technology, but also the organizational structure, processes, and doctrine. In other words, we need a complete doctrine, organization,

**Brigadier General Jeffery E. Marshall, ARNG (Ret.), was Deputy Director of Plans and Policy, J5, U.S. European Command and Executive Liaison to the State Partnership Program.**

training, materiel, leadership and education, personnel, and facilities review to ensure we can execute operational design.

So how do we currently define and manage assumptions? JP 5–0 states:

*A fact is a statement of information known to be true (such as verified locations of friendly and adversary force dispositions), while an assumption provides a supposition about the current situation or future course of events, assumed to be true in the absence of facts. Assumptions are necessary to enable the commander to complete an estimate of the situation and select the COA* [course of action]. *Assumptions that address gaps in knowledge are critical for the planning process to continue. For planning purposes, subordinate commanders treat assumptions made by higher headquarters as true in the absence of proof to the contrary. However, they should challenge those assumptions if they appear unrealistic. Assumptions must be continually reviewed to ensure validity.*[2]

The doctrinal definition is fine from a planning construct, but it leaves out a critical aspect of the operational construct: decisionmaking. The language in JP 5–0 treats assumptions as primarily a planning construct: "Although there may be exceptions, the staff should strive to resolve all assumptions before issuing the OPORD [operation order]."[3] If we are not careful, the inference is that making and managing assumptions cease once the plan is written and the staff moves into execution mode. At a bare minimum, assumptions should drive operational risk assessments, and the commander and staff must understand how unresolved assumptions may impact the operation.

Although the plan is critical, articulation of the plan and the follow-on execution including the input to the commander's decision cycle are paramount to success. Planners try to anticipate the critical decisions that the commander will need to make and construct a decision support matrix (DSM) to help identify when to make the decision. The Commander's Critical Information Requirements (CCIRs) are designed to gather the information required for a decision. The CCIRs are linked to anticipated decisions within the DSM.

However, within every anticipated decision, there is either an implicit or an explicit assumption—the conditions required to make the decision will be met. This implies that the CCIR will be completely answered and that there will be little or no uncertainty and ambiguity in the decision. In a perfect world, the commander will acquire complete knowledge and be able to make every decision based on this complete and accurate knowledge. War, however, does not exist in a perfect world. Decisions, particularly critical game-changing decisions, are often made without complete information.

When commanders need to make a decision without perfect information, they will do so based on assumptions as shown in figure 1. The shaded intuition area is a knowledge gap that must be spanned by assumptions until they are turned into facts.

In spite of the advances in command, control, communications, computers, intelligence, surveillance, and reconnaissance, there are still gaps—often large—in the knowledge that a commander needs to make critical decisions. Thus, commanders must use an intuitive approach based on their experience and understanding of the situation. The operational design process clearly recognizes the need to emphasize creative thinking and to move beyond purely structured decisionmaking processes in complex environments. Thus, these decisions will rest upon assumptions, either explicitly stated or implicit in the decision itself.

When decisionmakers are faced with uncertainty, they may take one of three actions: punt, delay, or make an intuitive decision using assumptions.

***Punt.*** The commander elects not to make a decision. However, the commander *has* made a decision: to ignore the conditions that generated the decision requirement. If the conditions are not critical, this may be fine. If the conditions could generate either an opportunity for success or the conditions leading to mission failure, however, punting the decision is an abrogation of command responsibility.

***Delay.*** The commander elects to delay the decision until he has greater knowledge and confidence. If the situation is not time sensitive, this action may be completely appropriate. But in dynamic situations, the commander may not have the luxury to wait

**Figure 2. Testing and Managing Assumptions**

**Testing Assumptions**

- Associate with decision point/ information requirements
- Develop branch plan if required
- Determine Red Team actions
- Prioritize knowledge management actions

} **Staff Actions**

**Validity Testing**

**Probability**
- Red: Improbable
- Orange: Unlikely
- Amber: Less likely
- Green: Likely
- Black: Uncertain

**Criticality**
- Red: Result in plan's failure
- Orange: Significant branch requirement
- Amber: Minor branch requirement
- Green: Negligible
- Black: Uncertain

**Operational Risk**
- Red: Mission failure
- Orange: Line of operation failure
- Amber: Mission impaired
- Green: Minor
- Black: Uncertain

**Sensitivity**
- Red: Small change yields a large shift
- Orange: Large change yields a large shift
- Amber: Large change yields a small shift
- Green: Negligible
- Black: Uncertain

**Time Window**
- Red: Immediate
- Orange: 24 hours
- Amber: 48 hours
- Green: 48+ hours
- Black: Uncertain

**Status/Knowledge Gap**
- Red: <50% answered
- Orange: 50% answered
- Amber: 75% answered
- Green: None
- Black: Uncertain

until the knowledge gap closes. Many, if not most, DSMs imply a delay until perfect or near-perfect knowledge. They identify the decision criteria, normally associated with answering specific aspects of the CCIR. Few, if any, DSMs note the risk associated with delaying a decision until specific elements of the CCIR are answered.

***Intuitive Decision.*** The commander elects to make a decision based upon less-than-perfect knowledge. These decisions can be either structured or unstructured. A *structured* intuitive decision occurs when the commander and staff make explicit assumptions about the missing knowledge and base the decision upon these assumptions. An *unstructured* intuitive decision occurs when the commander does not make formal assumptions about the missing knowledge and acts based upon experience. Intuitive decisionmaking is a by-product of experience and is framed within implicit assumptions that the commander specifically deems acceptable. These types of decisions often happen in time-sensitive situations. Effective staffs will start to define the implicit assumptions and work assumption management as soon as possible after the decision is made.

When commanders elect to make intuitive decisions, they must understand the implicit and explicit assumptions in the decision and rapidly engage the staff to fill in the knowledge gaps and develop branches in the event the assumptions are not valid. Operational design doctrine must address the assumptions that underpin creative thought and the requirement to validate and manage them. The staff's function is to help the commander take measured risks and hedge them in order to make effective intuitive decisions.

To understand an assumption, we must ask several questions:

***So What?*** This is a key, but often unasked, question. Will the lack of the assumption fundamentally change the decision or the plan? Just because a planner may need the assumption for a specific portion of the plan does not mean that the decisions based on the assumption will affect mission success and endstate.

***How Sensitive Is the Assumption?*** Will a small input change make a huge difference? If the assumption is relatively inelastic and does not change much as conditions change, then the risk may be far more containable.

***What Is the Risk If We Are Wrong?*** The current doctrinal literature, mainly in JP 5–0, contains a great deal of discussion on assumptions and their importance, as well as the need to manage the assumptions process. However, the literature provides little guidance on how to develop and manage assumptions. However, one key nugget in JP 5–0 does give a hint: "The information needed to verify or refute a planning assumption is an example of a CCIR."

CCIRs are linked to expected decisions, which rest either explicitly or implicitly on assumptions. Therefore, the information needed to verify or refute a planning assumption is not just an *example* of a CCIR, it is the very *nature* of a CCIR. CCIRs exist to plug knowledge gaps, which are covered by assumptions—either implicit or explicit—until the information is received.

## Making Valid Assumptions

Commander's intent is perhaps the most critical component of operational design. A well-crafted commander's intent clearly articulates the desired outcomes and changes to an environment that an operation should achieve and the key tasks required to reach this state. Commanders and staffs should carefully review the commander's intent to ensure that they understand any implicit assumptions and make them explicit.

But there are other areas that may help to identify implicit assumptions.

Perhaps the easiest place to start on assumptions is the DSM. Planners need to carefully review it and determine the underlying assumptions required in each decision for which there are open information requirements. As discussed above, each projected decision rests upon one or more assumptions. Often, these assumptions are implicit: we will either execute the decision or not. However, the implicit assumption that is often overlooked may lie at the core of the most critical decision. What happens if we do not execute the decision?

Essential and key tasks are another source of potential assumptions. Often, these tasks rest upon implicit assumptions about resources or partners. The key is to determine the anticipated conditions under which the task must be performed and determine whether they require an explicit assumption that must be validated through an information requirement.

The operating environment is another source of potential assumptions. JP 2–0, *Joint Intelligence*, discusses the need for a Red Team to review assumptions in the operating environment as part of joint intelligence preparation of the operating environment.

## An Integrated Example

Consider a noncombatant evacuation operation (NEO). The commander's intent may clearly articulate that the endstate is that all U.S. citizens and designated third party nationals are safely evacuated and the U.S. Embassy is secured and supported. Key tasks may include securing the Embassy, conducting the evacuation from designated collection points, establishing and maintaining a safe haven, supporting evacuees, and moving evacuees beyond the safe haven.

At this point, the intent and tasks rest on several key implicit assumptions:

- Evacuees can get to the collection centers. What happens if they cannot? Does the commander's intent mean that the evacuation force must go to the evacuees?
- The United States will be able to establish the planned safe haven. What happens if the safe haven is not available?
- How many designated third party nationals will the United States support? This could dramatically impact evacuee flow and the lift assets required.
- The United States will have the air- and/or sealift assets required for the evacuation. What happens if U.S. military forces are not sufficient and the plan calls for contracted lift? What happens if contracted lift is not available?

The situation in NEO planning can get even more complex as the planners review the various NEO conditions: permissive, uncertain, and nonpermissive. The assumptions and their ramifications may change between conditions. For example, contracted lift may not be available at all in a nonpermissive NEO operation.

Once the staff starts to develop assumptions, they must be tested to ensure validity. If valid, the staff then needs to determine what wargaming, analysis, and planning actions are required. Figures 2 and 3 provide a method to validate assumptions as well as to manage the actions required for valid assumptions.

JP 5–0 clearly states that assumptions must be valid. However, neither JP 5–0 nor any other doctrinal publication provides a method to determine whether an assumption is valid, much less a method to determine how critical it may be. The areas in the bottom half of figure 2 are a potential way to determine

validity and importance, which can then be built in a tracking matrix as shown in figure 3.

In addition to the metrics discussed above, two key metrics help to determine validity: probability and sensitivity. Both provide planners with a way to assess the likelihood of an assumption being correct and also the sensitivity of the assumption to changes in the inputs that ultimately drive the assumption. If the probability is either extremely likely or extremely unlikely, then the assumption may not be valid—at least as currently stated. In this event, planners should revisit the conditions that caused them to develop the assumption and ensure they have stated it properly. If the probability is extremely low, they may possibly eliminate the assumption altogether.

If the assumption is very inelastic—that is, if changes in inputs do not materially change outcomes, making the assumption far more containable—it carries less risk. A very elastic assumption can drastically change the impact of an incorrect assumption and carries more risk. Highly elastic assumptions may require more detailed branch planning, especially if the assumption is critical to the operation and poses significant operational risk. They should also be explicitly included in the CCIR.

As shown in figure 3, all of the metrics combine to determine both how valid and how important the assumption is to the operation. These metrics can then be used to prioritize both KM efforts as discussed above, as well as branch planning. They are more than simple stoplight charts. They provide staff with the framework to properly assess and categorize planning assumptions in order to:

- determine if the assumptions are valid
- understand how important they are to the operation
- determine the key inputs the assumption depends upon
- prioritize KM resources to fill in information gaps
- ensure a key assumption does not get lost in the often hectic process of plan execution.

Assumptions need to be integrated into the DSM. As noted earlier, virtually every decision in the DSM has at least an implicit assumption that may require branch planning. Figure 3 shows an Assumption Management Matrix that clearly associates the assumption with decision points and information requirements. Likewise, the command should consider adding a column to the DSM that shows the assumption numbers from the assumption matrix to cross-validate and track the list.

Any assumption that is valid and at least somewhat elastic should have a branch plan. The other metrics of risk, criticality, and time available can be used to prioritize planning.

If planners are uncertain about potential ramifications of incorrect assumptions or the sensitivity of the assumption, they may turn to the command's Red Team to explore various branches that could stem from the assumption. While this may be a different way to use the Red Team than that cited in JP 2–0, *Joint Intelligence*, it could provide a valuable analytical tool for the command's planners. A well-trained Red Team can potentially eliminate a great deal of time from planning requirements if it can explore potential branches and outcomes and assist planners in both prioritizing their efforts and focusing on the key areas that could most influence operational success.

The goal of assumption management is to provide commanders with the confidence to make intuitive decisions and take measured risk that can be hedged through effective management tools, targeted Red Team analysis, selected branch planning, and prioritized KM that quickly closes gaps.

## Recommendations

*Expand current doctrine to include more discussion on how to develop valid assumptions and, equally important, how to manage them as planning evolves to execution.* Operational design emphasizes the need for more creative decisionmaking with potentially less structure. This change is significant and reflects the complex JIIM environment in which virtually all military operations are conducted. But as we lessen the structural format for decisionmaking, we need to consider adding more analytical capability to ensure that we continue to make and execute effective decisions. The complexity of JIIM environments will almost certainly require more assumptions during the planning process. Furthermore, these assumptions are also likely to be far more elastic than in simpler environments. Therefore, doctrine needs to reflect the need for increased cross-functional analytical requirements and expand upon techniques to make valid assumptions and then manage them. The doctrine should reinforce the linkage between assumptions and decisions, as well as expand upon the need to develop branch plans for designated elastic assumptions.

In addition, the current doctrinal references to assumptions reside primarily in JP 5–0. While JP 5–0 should provide the overall guidance on assumptions, it cannot address the assumptions required in various functional areas. All families of joint publications should discuss assumption development and management at the "–0" level. In particular, JP 1–0, *Personnel Support to Joint Operations*, JP 2–0, JP 4–0, *Joint Logistics*, and JP 6–0, *Joint Communications System*, need to address the assumptions required in their particular functions and how to develop them and integrate them into an overall plan.

*Modify current doctrine to discuss the need for effective decision support and incorporate a decision support subparagraph into the Command and Signal paragraph of the joint orders format.* The current doctrine discusses CCIR in detail, especially in JP 3–0, *Joint Operations*. However, it never definitively states where the CCIR is published. Moreover, there are few references to decision support. JP 5–0 merely states decision support tools are important. This practice relegates the making of a critical decision to almost an afterthought in the orders process. Given the complexities in the JIIM environment and the requirements in operational design, decision support is critical to mission success.

A section on decision support to both JP 3–0 and JP 5–0 should be added. The excellent CCIR discussion in JP 3–0 should be incorporated into the new section and include expanded discussion of KM, the need to link KM, CCIR, and assumptions together, and their management. Likewise, the discussion in JP 5–0 should be included in a decision support section to make similar linkages between assumptions, CCIR, and KM. It should also discuss specific decision support techniques.

Finally, paragraph 5 of the standard operation order should be modified to include a new paragraph 5C governing Decision Support. Include:

- 5C1. Decision Points
- 5C2. CCIR
- 5C3. KM requirements.

*Develop and publish comprehensive Decision Support tactics, techniques, and procedures (TTPs) that reflect the relationships*

**Figure 3. Assumption Matrix**

| Assumption | Status | Decisive Point | Information Requirements | Probability | Criticality | Risk | Sensitivity | Branch | Red Team Action |
|---|---|---|---|---|---|---|---|---|---|
| Assumption 1 | | 1 | 1.1, 1.2, 1.3, 1.4 | | | | | Branch 1 | |
| Assumption 2 | | 2 | 2.1, 2.2 | | | | | Branch 2, 3 | |
| Assumption 3 | | 3 | 3.1, 3.2 | | | | | Branch 4 | |
| Assumption 4 | | 4 | | | | | | Not Valid | |
| Assumption 5 | | 5 | 5.1, 5.2, 5.3 | | | | | Fragmentary order issued to use Branch 5 | |
| Assumption 6 | | 6 | 6.1, 6.2, 6.3 | | | | | Assumption validated, no action required | |

*among decisions, assumptions, CCIR, and KM*. Include the metrics in figure 2. Develop TTPs to prioritize KM collection efforts. These TTPs should be standardized across the joint community and taught at the Joint Advanced Warfighting School and similar Service schools. Consider publishing a specific Decision Support joint publication that develops doctrine to integrate decisions, assumptions, CCIR, and KM.

*Add an Assumption Management Matrix to augment the standard DSM*. Include the Assumption Matrix in figure 3 as part of the DSM and staff briefings. Brief the matrix whenever the DSM is briefed. JP 3–0 discusses the need to review CCIR as part of assessments. Expand this section to include the DSM and the Assumption Matrix. A formalized assessment board that briefs during operations may facilitate a comprehensive review.

*Better integrate Red Teams into decision support and broaden their focus beyond that of the traditional intelligence role*. The Red Team is a tremendous asset to a commander and staff that can potentially be leveraged beyond an intelligence role. Trained Red Team members have a broad skill set in critical thinking, political-military analysis, wargaming techniques, cultural analysis, and other skills critical to the analysis required in operational design. Red Team members have the ideal skill sets to analyze a concept to determine the implicit assumptions that are inherent in the environment and tasks and then use the metrics in figure 2 to determine assumption validity and elasticity. They can then work with planners to wargame branch plans. Commanders may want to send key analysts to the Army's University of Foreign Military and Cultural Studies for the Red Team Leader Course and the Red Team Members Course.

Making assumptions is hard. Even experienced planners will often scratch their heads over what assumptions they need to make, and may completely miss the implicit assumptions they make and have not acknowledged. Unfortunately, implicit assumptions and poorly understood and managed assumptions can compromise a plan and lead to flawed execution and possibly failure.

Virtually every significant decision is made with some degree of uncertainty and missing knowledge. In many cases, the assumptions that mentally fill in these gaps are implicit. In other cases, the missing knowledge and uncertainty are not even recognized. In both cases, the commander and staff have made assumptions that could be critical to mission success. Sometimes the most obvious assumptions are not stated and managed because they seem so obvious.

Commands with effective Decision Support Matrices and synchronized data collection and rigorous decision support systems should lessen the impact of untested assumptions but still might not catch everything. Adding a deliberate assumptions analysis and management process could refine decisionmaking and help decisionmakers acknowledge all implicit assumptions made and analyze the risks associated with them.

This process should also help to better define asset requirements and branch plans. For example, if the J2 (intelligence) states a missile threat is negligible, there could well be an implicit assumption in the analysis. If that is the case, the J3 (operations) may need to add a branch plan that requires additional missile defense assets.

The recommendations above should help to add more discipline to the planning system at a small cost in extra planning resources. Teaching effective assumption making and management could also help to improve planning and reduce overall risk by reducing unacknowledged implicit assumptions. **JFQ**

## NOTES

[1] James N. Mattis, "Vision for a Joint Approach to Operational Design," memorandum for U.S. Joint Forces Command, October 6, 2009, available at <www.jfcom.mil/newslink/storyarchive/2009/aod_2009.pdf>.

[2] Joint Publication 5–0, *Joint Operation Planning* (Washington, DC: The Joint Staff, December 26, 2006), III–26.

[3] Ibid.

# Centers of Gravity from the "Inside Out"

*By* JAN L. RUESCHHOFF *and* JONATHAN P. DUNNE

For over two decades, U.S. military doctrine has insisted on pinning major aspects of its operational planning processes on Carl von Clausewitz's concept of the center of gravity (COG). Yet the lack of doctrinal guidance on developing and employing COGs wastes planners' time and provides few tangible benefits. Fortunately, doctrine's introduction of *Critical Factors* as the components of COG provides pillars upon which a process of COG identification and implementation can be built.

The purpose of this article is to extend a bridge between COGs and existing doctrinal guidance for operational planning. The concepts introduced in this article are not meant to challenge or change doctrine, but to clarify one of its most essential concepts.

## Review of COG

In the 1980s, American doctrine writers refocused on the Soviet army and the potential for war in Europe. As the American military was outnumbered and outgunned on the European continent, a departure from the largely defensive doctrine of the past was necessary. In its place, the Services sought to exploit the combination of mobility and firepower to overcome their numerical inferiority.

In the midst of this renaissance of American military theory, a term seized prominence in U.S. doctrinal publications—*center of gravity*. Clausewitz defined COG as "the hub of all power and movement, on which everything depends."[1] Victory, the Prussian argued, goes to the commander who focuses his energies against his adversary's COG while protecting his own.[2] While the Services may have reshaped Clausewitz's original concept of COG, the term has become a crucial part of American operational art. Yet the Army and Marine Corps took different paths to including COGs into their respective doctrines.

In 1986, Army doctrine asserted that the essence of operational art was the identification of the enemy's COG.[3] This theme has continued throughout Army doctrine up through its latest doctrinal revision describing COG as a "focal point" for campaigns and major operations.[4] While initially suggesting COG provided a method of pitting "strength against strength," the Army eventually adopted the term *decisive points* as a way of indirectly attacking an enemy's COG. This indirect approach would apply "combat power against a series of decisive points that avoid enemy strengths."[5]

Long holding to the importance of pitting strength against weakness, the Marine Corps approached the idea of COG cautiously. Marine doctrine warned there was "danger" associated with using the term COG; declaring the enemy's COG was not "a source of strength, but a [c]ritical [v]ulnerability (CV)."[6]

The 1989 edition of the Marine Corps Fleet Marine Field Manual (FMFM) 1, *Warfighting*, described CVs simply as "where and when we can hurt [the enemy] most."[7] The Marine Corps eventually relented to the idea of COGs. In the revision of the manual, the Marine Corps accepted COGs into its doctrine—but only if used as a partner to an enemy's critical vulnerabilities.

Whatever term the two Services use to describe the focus for indirectly attacking an adversary's COG, determining this point is admittedly not a simple process. The Army mandates a "thorough and detailed" analysis to determine its decisive points, but provides little insight on a process for that analysis.[8] The Marine Corps has been even more blunt, noting the identification of a CV may be so difficult that the Marine Corps may need to "adopt the tactic of exploiting any and all vulnerabilities" until uncovering a decisive opportunity.[9] It is interesting that doctrine would essentially disregard the principle of economy and suggest that one "hit anything that looks vulnerable and hope you get lucky." A more deliberate process was needed to identify this point.

## Critical Factors

In 1996, Dr. Joe Strange, a professor at the Marine Corps War College, set out to write a 13-page paper to link the Marine doctrinal terms of *critical vulnerability* and *center of gravity*.[10] He ended with a full-length monograph and a construct that has been adopted by militaries around the globe. Dr. Strange's framework introduced *critical capabilities* (CCs) and *critical requirements* (CRs) as the connective tissue between a CV and COG. By exploiting a CV, forces can deny a CR necessary for an enemy's CC. As the CCs are degraded or denied, the enemy's COG is also degraded or denied.[11]

In 2002, Strange's concept was adopted in U.S. Joint Forces Doctrine with the release of Joint Publication (JP) 5–00.1, *Joint Campaign Planning*,[12] and later in the 2006 edition of JP 3–0, *Joint Operations*, that referred to the individual components of COG—CCs, CRs, and CVs—as "Critical Factors."[13] North Atlantic Treaty Organization (NATO) doctrine also included this approach in its 2006 version of Allied JP 5–0, *Allied Joint Doctrine for Operational Planning.*

Neither the Army nor the Marine Corps, however, has revised its planning or operational doctrine to include a discussion of Critical Factors. This omission is unfortunate, as Critical Factors Analysis (CFA) provides a sound analytical framework to assist planners in the analysis and identification of COGs and to assist in operational planning.

## Identifying COGs

***The Problem.*** The American military's doctrinal guidance is insufficient in providing commanders and their staffs with a process to select a center of gravity. Planning teams can take hours—if not days—arguing over what is and is not the enemy's COG. This contest of wills is often decided by

**Lieutenant Colonel Jan L. Rueschhoff, USA, is an Intelligence Officer with operational tours in Iraq and Afghanistan. Lieutenant Colonel Jonathan P. Dunne, USMC, is an Artillery Officer with operational tours in Iraq.**

whoever is the strongest personality on the planning team, not through any established analytical process.

More troubling, without an objective approach to determine a COG, planners are vulnerable to faulty COG analysis. As Army Field Manual 3–0, *Operations*, warns, "Faulty conclusions drawn from hasty or abbreviated analyses can adversely affect operations, waste critical resources, and incur undue risk." The question, therefore, is how do planners select the correct COG?

The Army/Marine Corps' latest Intelligence Preparation of the Battlefield (IPB) doctrine states, "Threat/*adversary* templates . . . aid in the initial identification of the threat's/adversary's centers of gravity."[14] This essentially leaves a planner with a definition of COG in one hand and an enemy situational template in another—hoping he will make the right guess.

In 2002, the interim publication JP 5–00.1 provided an in-depth description of how COGs could be determined using Strange's framework.[15] However, JP 5–0, *Joint Operation Planning*, superseded JP 5–00.1 in 2006 and represented a step backward—deleting much of the guidance of the previous manual. JP 5–0 states that COGs are derived from systems analysis (see figure 1), but provides little guidance on the process of determining them. Instead, the manual refers readers to the Joint IPB manual for further guidance.[16] Yet any hope for concrete guidance in the Joint IPB manual quickly becomes forlorn. The manual's guidance is to analyze the various systems and determine from which elements the adversary derives its "freedom of action, physical strength or will to fight."[17] In other words, we take a definition in one hand and an enemy situational template in another, and hope we pick the right COG—and we are right back to the initial problem.

To its credit, JP 5–0 continued to incorporate Strange's concept of Critical Factors. Unfortunately, the manual depicted the process as a sequential, linear analytical method beginning with identifying a COG.[18] This linear, left-to-right approach is reinforced by other doctrinal and academic publications. These include a Joint Forces Staff College publication[19] (see figure 2) and guidance in the U.S. Joint Force Command's Joint Targeting Handbook, which states that the process "begins with the COG as a source of power."[20]

The problem with this left-to-right approach—beginning with identifying the COG—is that planners are once again left without any *process of determining* a COG. While the analysis of the Critical Factors provides the planning team with greater details to assist in targeting and operational planning, the difficulty involved in selecting the initial COG leaves the participants wanting to disassociate themselves from the process altogether. There is also no safeguard against picking the wrong COG.

***The Solution.*** Too many readers of Dr. Strange's monograph seem to have missed his advice that the process does not "have to be conducted in a precise or rigid sequential manner."[21] Proper analysis of a COG does not start with its identification. It is best accomplished from an "inside-out" approach of first identifying objectives and then the Critical Factors—namely the critical capabilities—that support the objectives (see figure 3).

In his 2004 *Military Review* article, Colonel Dale Eikmeier, USA, acknowledged the importance of first identifying objectives, then identifying Critical Factors.[22] Yet the Navy's Planning Manual is the only doctrine that calls for identifying Critical Factors before COGs—although the Navy focuses on what it calls "critical strengths" to identify COGs.[23] Why Critical Factors—particularly critical capabilities—should precede COGs is best explained by reviewing the definitions of *critical capability*:

- a means that is considered a crucial enabler for a center of gravity to function as such and is essential to the accomplishment of the specified or assumed objective(s)[24]
- primary abilities that merit a center of gravity to be identified as such in the context of a given scenario, situation, or mission.[25]

While the joint definition reveals that critical capabilities are what allow a COG to function as such, Strange's use of the term *identified* gets to the point of the issue. It is through an adversary's CCs that an analyst may identify a COG. While COGs may seem amorphous, capabilities are much more concrete and discernable. Joint and Service doctrine has long included the identification of enemy capabilities as a crucial step in the IPB process. Armed with a list of capabilities necessary for a force to achieve its objectives, an analyst may now make an assessment of what may be providing the "source of power" to these capabilities—the COG.

**Figure 1. JP 5–0 Concept of COG**

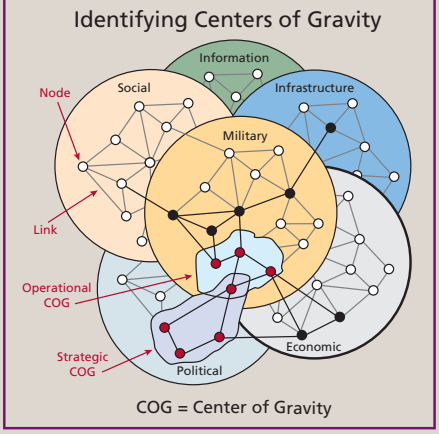
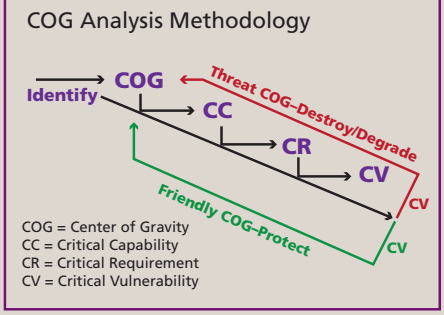



**Figure 2. Depiction of a Linear Analytical Methodology**

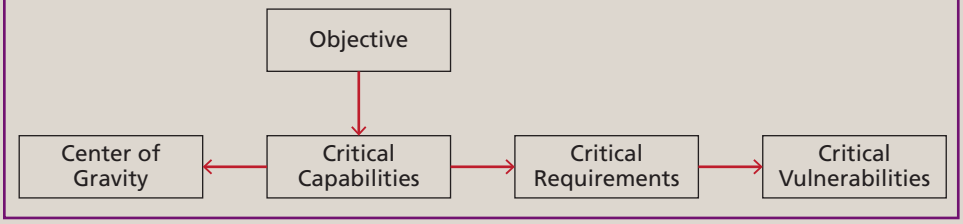



## The "Unspecified" COG

While there may be times when a COG is abundantly clear, often the true COG will be difficult to determine. Take the example of a staff that identifies 10 CCs. The staff attempts to find a singular source of power for each of the 10 CCs believed vital for the accomplishment of the enemy's mission. After determined analysis, their best COG candidate can only satisfy seven of the CCs. Another source provides the last three. Are there, therefore, two COGs?

The answer may very well be yes, but it depends upon which doctrine the staff is following. Despite the individual Services' acceptance of multiple COGs, joint doctrine is clear that there is only one COG for each level of war.[26] So what should a staff do if they have two possible COGs and are operating under joint doctrine—constricting the staff to only one COG? Should the staff continue looking for a better COG candidate? Should they simply discard the three CCs that cannot be linked to the proposed COG?

**Figure 3. COG Analysis from the "Inside Out"**




We recommend the staff do neither. The objective of COG analysis is not to provide a magic name of a COG by which the commander may speak and slay his foe. The objective is to identify weaknesses the commander may exploit that will uncover and eliminate the foe's ability to resist.

If the staff is able to identify and then devise an operational plan to exploit CVs, thereby denying CRs and eliminating the abilities of a CC, is not the force still attacking an "unspecified" COG? We believe this to be the case. The time spent in a fruitless pursuit of the perfect description of the enemy's COG is better used providing detail to the Critical Factors.

## Operational Planning

***Working "To the Right of CCs."*** Regardless of whatever is named the COG—or even if one is specified at all—with the identified CCs, the analyst may begin identifying CRs and CVs. While CCs are the critical actions or functions—think verbs—necessary for the enemy to meet his objectives, CRs are assets or conditions—think nouns—required to enact the CCs. For instance, if the CC is *deliver indirect fires*, the CRs may be *observers, munitions, artillery pieces, gun crews, radio communications,* and *being within range of desired targets.*

Critical vulnerabilities identify the aspects of CRs that are vulnerable or already deficient. Too often, analysts simply restate vulnerable CRs as CVs. However, to get the most out of the analysis, the planner should attempt to determine not only *if* a CR is vulnerable, but *how* the CR is vulnerable.

While the analyst will usually identify CRs and CVs after determining CCs, the process does not always need to be in this order. There may be times when discovering a vulnerability or requirement may result in the identification of a CC. For example, an intelligence report reveals that an adversary has purchased amphibious landing craft. From this report, an analyst could assess that the landing craft is a possible CR for a new CC—conducting amphibious operations. In turn, this may indicate that the adversary may also be adjusting his objectives.

While "conventional" military examples are fairly straightforward, the CFA process is also applicable to counterinsurgency (COIN) operations. The complexity of the COIN battlefield demands more detailed analysis. In conducting a thorough analysis of an adversary's CRs, the planner may run into a Russian "nesting doll" effect of subnested requirements. By subnesting requirements, the planner keeps intact the linkage of CRs and CCs. A sub-CR could support more than one CC or CR.[27] Identifying these multiple relationships allows planners to formulate priorities based upon which targets would have the greatest impact on the adversary. The CFA framework also facilitates identifying nonlethal targeting opportunities—stopping insurgent attacks—that would normally be associated with lethal targeting efforts.

CFA applied to COIN demonstrates how this type of analysis can contribute to planning across lines of operation and in depth of time and space. From this example, we realize that CFA is essential in the development of operations. The importance of determining how to attack a COG is, according to joint operations doctrine, the "essence of operational art."[28] One of the key operational elements in this planning is decisive points (DPs). Interestingly, while the Army fully embraces DPs in its doctrine, Marine Corps doctrine uses the term sparingly, emphasizing CVs instead. Yet both Services use their respective terms for the same purpose: to provide an indirect means to attack an enemy's center of gravity.

So are DPs restated CVs? Some argue that this is the case. Lieutenant General Paul Van Riper, USMC (Ret.), wrote, "The terms *vulnerability* and later *critical vulnerability* entered the military vocabulary in the late 1980s as sort of a synonym for decisive point."[29] Joint doctrine seems to echo this when it states, "Decisive points can be thought of as a way to relate what is 'critical' to what is 'vulnerable.'"[30]

The link between DPs and Critical Factors is further strengthened by the joint definition that states a DP can be a geographic place, specific key event, Critical Factor, or function. The examples given in JP 3–0—airbases, overflight permissions, civilian infrastructure[31]—all describe elements that could be CRs to an adversary's CC. JP 5–0 seems to close the discussion when it states, "Understanding the relationship between a COG's critical capabilities, requirements, and vulnerabilities can illuminate direct and indirect approaches to the COG. It is likely that most of these Critical Factors will be decisive points."[32]

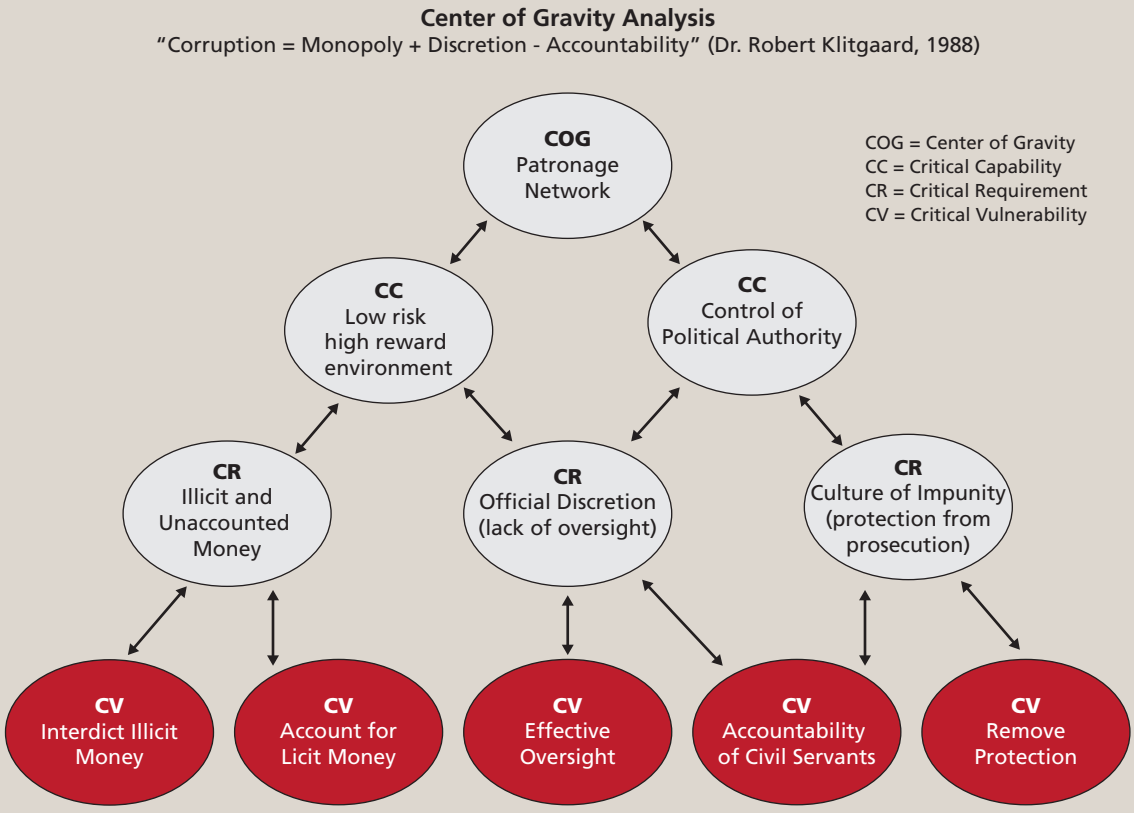
Yet it may be more helpful to follow NATO doctrine's lead: "Decisive Points are logically *derived* from Critical Requirements and Critical Vulnerabilities."[33] Planners derive DPs through CFA, but DPs are not synonymous with Critical Factors.

Planners identify the Critical Factors of their adversaries, their own forces, and third parties. They then determine which vulnerable CRs need to be affected—attacked or protected—in order to achieve their own objectives and endstate. Just as CVs describe how a CR may be vulnerable, DPs describe the key locations, systems, capabilities, or events from which a commander may exploit or protect the vulnerabilities that CFA identifies. Essentially, DPs are the springboard by which planners effect the CVs necessary to achieve one's objective.

It is easy to focus on the adversary's COG, but planners must not disregard their own COG. By applying the same CFA model to friendly forces, planners will identify CCs necessary to accomplish their objectives, CRs necessary to enable those CCs, and how they might be deficient or vulnerable. Thus, some DPs may be identified that protect or reinforce friendly CRs at the same time planners use DPs to affect the CRs of their adversaries.

***Third Party Actors.*** As observed in current conflicts, modern forces do not only share the battlefield with one's adversaries. Other parties such as nongovernmental organizations, the host nation, various tribes, and

**Figure 4. ISAF COG Analysis of Corruption**




*Source:* ISAF Stability Division Corruption Annex briefing to OPLAN, June 21, 2010.

criminal groups all contribute to the operational environment. An evaluation of each of these third parties using CFA aids the staff's ability to understand the systems of each group and how they interact.

The concept of evaluating civilian entities based upon their capabilities is already captured in Service doctrine. The Army/Marine Corps IPB manual expresses the need to identify the capabilities when assessing civil considerations.[34] Identifying these groups, their objectives, and associated Critical Factors—including capabilities—necessary to achieve their endstate provides the operational planner with vital analysis of the operational environment.

Planners may find critical requirements are shared by more than one party. There also may be sets of inverse relationships of Critical Factors among the different groups where the presence of a particular condition may be a CR for one party and the absence of that particular condition is a CR of another.

Identifying these shared and inverse Critical Factor relationships allows operational planners to identify and prioritize DPs that would have the greatest impact on neutralizing opposing Critical Factors and reinforcing Critical Factors tied to shared objectives within the operational environment. By applying CFA to third party actors, planners can begin to determine which party's CRs they may choose to reinforce and protect and whose CRs they wish to disrupt in order to meet their own objectives.

***Future Critical Factors.*** Much of the emphasis in American campaign planning doctrine is focused on identifying an adversary's present vulnerabilities and capabilities. Unfortunately, the exclusive focus on present capabilities stifles our ability to develop a plan poised to react to future threats—much less prevent those future threats from emerging. The planning for the transition between phase three and phase four operations is where the concept of Future Critical Factors may have the most relevance.

Through phase three, planners are usually focusing on an enemy with a relatively well-defined objective and set of Critical Factors. The staff dutifully identifies the decisive points necessary to attack their adversary's COG and sequences them into their operational planning, which will culminate with defeat of the adversary's COG and accomplishment of friendly objectives.

With a defeated adversary, there could be the temptation to dismiss the use of CFA to identify DPs in phase four. Yet just as planners use phases to denote a change in objectives, it is important to assume a defeated adversary's objectives have also changed. Likewise, it is possible that other groups may see the defeat of our adversary as an opportunity to act on their objectives— which may not be congruent with our own—even if they do not yet have the capabilities to act toward achieving their objectives.

The lack of capabilities does not invalidate the use of CFA. Rather, the staff should focus on the CCs that their adversary would need to develop to reach their objectives. The CRs become the conditions, resources, and means by which an adversary would develop their necessary CCs.

Focusing on future CCs allows the planning team to anticipate problems during the transition to phase four and to be proactive in dealing with these challenges before they are able to impact their own CVs—preventing achievement of the endstate.

### Current Operations

One of the best examples of how CFA is contributing to current operations is the International Security Assistance Force (ISAF) efforts to support the government of Afghanistan in combating corruption. Despite sincere proclamations of the government's leaders desiring to clamp down on corruption, the social fabric of the country complicates confronting some of the country's most malign actors and their networks directly. ISAF planners realized an indirect approach to corruption that changed the conditions in which these networks operated was needed. The best way to do this was to attack the CVs and CRs of the patronage networks.[35]

The planners started with a simple COG analysis, which concluded with the identification of five critical vulnerabilities (see figure 4). The planners admit their initial COG analysis was too simplistic and note that several of the Critical Factors are not consistent with doctrinal definitions. However, what sets this analysis apart from so many other COG analysis efforts is the planners actually *used* this analysis to help guide their operational pursuits.

For each of the CVs, planners identified actions by which these could be influenced. For example, to influence the CV Interdict Illicit Money, planners identified providing better border control and instituting merit-based hiring as potential actions to be taken. These and other actions were designated as decisive points and arrayed in a synchronization matrix depicting the sequence in which they were to be engaged.

In some cases, the best way to influence the malign actor network's COG was to reinforce a CR of the Afghan government. To help make this distinction, the decisive points were segmented into three categories: ISAF Can Do, ISAF Can Facilitate, and ISAF Can Advocate. The categories were a realization that not only did the COG of malign actor networks need to be considered, but also that the COGs of ISAF and the Afghan government needed to be considered—utilizing the concept of third party actor CFA described earlier.

While these initial analyses are simplistic, the process has continued to add more detailed analysis. In August 2010, the ISAF Joint Command (IJC) provided a mission analysis briefing on its anticorruption efforts. The briefing detailed 27 CCs and 77 CRs that IJC found in its COG analysis of malign networks and friendly forces. A number of the associated CVs were identified as being exploitable to achieve decisive conditions.[36]

### Operational Design

Operations in Iraq and Afghanistan have prompted spirited discussions pitting operational planning against operational design—in many cases, arguing traditional planning processes are outdated when facing the complexities of the modern battlefield. While the previous segments in this article have demonstrated how Critical Factors Analysis can be a significant contributor to operational planning, the question may be asked: what is CFA's applicability to operational design?

If existing doctrine is to be used as a guide, CFA is applicable to operational design. JP 5–0 states, "One of the most important tasks confronting the [joint force commander's] staff in the operational design process is the identification of friendly and adversary COG."[37] In fact, the discussion of COG and Critical Factors occurs in JP 5–0's design chapter, not its planning chapter. The Army has long held COGs are elements of operational design, reinforced in the Army's newest version of FM 5–0.[38] Even the Army Training and Doctrine Command's pamphlet on operational design specifically speaks of CCs and CRs in its section on mission analysis.[39]

Beyond doctrine, CFA's utility in operational design is illustrated by the ISAF example. The ISAF and IJC staff has used CFA to help craft the foundation of its anticorruption campaign. It was no accident that the IJC briefed their anticorruption CFA results under the banner of "operational design."[40] So perhaps the question is not whether CFA is applicable to operational design, but how it should be applied.

CFA assists in identifying options by which forces can engage an adversary. These options include both lethal and nonlethal methods. They may be for immediate execution or sequenced far in the future. They may be prioritized by which points impact the most adversary capabilities or by those that aid an ally while harming a foe. But CFA is not a crystal ball that tells a commander that engaging a potential adversary is consistent with the commander's strategic endstate. Other tools in design's framing process may be helpful in assisting a commander with that judgment. However, once a commander's endstate is defined, CFA is a powerful tool in helping a commander and staff in campaign design and translating that design into action.

Over the past 20 years, American military doctrine has adopted and adapted Clausewitz's concept of center of gravity into its own operational art. However, guidance for identifying COGs and the points by which commanders can indirectly attack those COGs has been elusive in American doctrine. Critical Factors Analysis provides a clear, analytical method of determining the points that American forces should affect—a far cry from recent guidance that in essence suggested Marines should "hit anything that looks vulnerable and hope they get lucky."

CFA is not a process that stands alone in the operational process. Rather, it is the connective tissue between many other doctrinal processes. While COG analysis may once have been no more than an exercise in putting ideas on a PowerPoint slide, CFA provides the staff with a continuous, iterative process that capitalizes on COG analysis to help design campaigns and drive operations.

CFA provides a tool to identify what is critical about one's adversary or third party and to determine where commanders can best affect that point through both lethal and nonlethal means. A better understanding of Critical Factors Analysis within our doctrine will allow staffs to develop plans that are both more effective and efficient. **JFQ**

#### NOTES

[1] Carl von Clausewitz, *On War*, trans. and ed. Michael Howard and Peter Paret (Princeton: Princeton University Press, 1984), 485–486.

[2] Ibid., 595–596.

[3] Field Manual (FM) 100–5, *Operations* (Washington, DC: Headquarters Department of the Army, 1986), 179–180.

[4] FM 3–0, *Operations* (Washington, DC: Headquarters Department of the Army, 2008), 6–8.

[5] Ibid., 5–10.

[6] Fleet Marine Field Manual (FMFM) 1, *Warfighting* (Washington, DC: Headquarters Department of the Navy, 1989), 85.

[7] Ibid., 36.

[8] FM 3–0 (2008), 6–8.

[9] FMFM 1, 36.

[10] Joseph L. Strange, interview with authors, February 12, 2008.

[11] Joseph L. Strange, "Centers of Gravity & Critical Vulnerabilities: Building on the Clausewitzan Foundation So That We Can All Speak the Same Language," *Perspectives on Warfighting* 4, no. 2 (1996), 3.

[12] Joint Publication (JP) 5–00.1, *Joint Campaign Planning* (Washington, DC: Joint Chiefs of Staff, 2002), II–6—II–10.

[13] JP 3–0, *Joint Operations* (Washington, DC: Joint Chiefs of Staff, 2006), IV–10.

[14] U.S. Army/U.S. Marine Corps, FM 2–01.3/Marine Corps Reference Publication 2–3A: *Intelligence Preparation of the Battlefield/Battlespace* (Washington, DC: Headquarters Department of the Army/Headquarters Department of the Navy, 2009), A–1.

[15] JP 5–00.1, II–6—II–10.

[16] JP 5–0, *Joint Operation Planning* (Washington, DC: The Joint Staff, 2006), IV–8—IV–15.

[17] JP 2–03.1, *Joint Tactics, Techniques, and Procedures for Joint Intelligence Preparation of the Battlespace* (Washington, DC: Joint Chiefs of Staff, 2000), II–45.

[18] JP 5–0, IV–11, IV–13.

[19] Joint Forces Staff College, *Campaign Planning/Operational Art Primer AY 07: Joint Operation Planning Process* (Norfolk, VA: National Defense University, 2007), 58.

[20] Joint Warfighting Center, *Joint Fires and Targeting Handbook* (Suffolk, VA: U.S. Joint Forces Command, 2007), I–26.

[21] Strange, *Centers of Gravity & Critical Vulnerabilities*, 141.

[22] Dale C. Eikmeier, "Center of Gravity Analysis," *Military Review* (July–August 2004), 4.

[23] U.S. Navy Warfare Publication 5–01, *Navy Planning* (Washington, DC: Headquarters Department of the Navy, 2007), 2–8, annex C.

[24] JP 3–0.

[25] Strange, *Centers of Gravity & Critical Vulnerabilities*, 3.

[26] JP 3–0, IV–10.

[27] Developed based upon email discussions between Dr. Strange and authors in September 2009.

[28] JP 5–0, IV–18.

[29] Paul K. Van Riper, *Planning For and Applying Military Force: An Examination of Terms* (Carlisle Barracks, PA: Strategic Studies Institute, 2006), 10.

[30] JP 3–0, IV–12.

[31] Ibid.

[32] JP 5–0, IV–16.

[33] North Atlantic Treaty Organization (NATO), Allied Joint Publication 5, *Allied Joint Doctrine for Operational Planning* (Brussels: NATO Standardization Agency, 2006), 3–11. Emphasis added.

[34] FM 2–01.3/MCRP 2–3A, 3–15.

[35] Email interview with Nathan Hoepner, who served as the Anti-Corruption Officer in the International Security Assistance Force (ISAF) Stability Division, September 10, 2010.

[36] ISAF Joint Command (IJC), Anti-Corruption Analysis Brief to CJIATF–SHAFAFIAT, August 24, 2010, slides 31–39.

[37] JP 5–0, IV–8.

[38] FM 5–0, *The Operations Process* (Washington, DC: Headquarters Department of the Army, 2010), D–1.

[39] U.S. Army Training and Doctrine Command (TRADOC) Pamphlet 525–5–500 (Fort Monroe, VA: TRADOC, 2008), 28.

[40] HQ IJC, slides 31–39.

# Evidentiary Validation of FM 3–24
# Counterinsurgency Worldwide, 1978–2008

*By* CHRISTOPHER PAUL *and* COLIN P. CLARKE

The Joint Doctrine section of *JFQ* 58 (3d Quarter 2010) contained a lively exchange between Colonel Gian Gentile, USA, and Dr. John Nagl over the principles advanced in Field Manual (FM) 3–24, *Counterinsurgency*, and how those principles were developed and codified into doctrine.[1] One of the issues raised in this exchange was the extent to which current counterinsurgency (COIN) doctrine was debated and discussed prior to the manual's publication. We have nothing to contribute to that part of the discussion. Where we do wish to contribute is with regard to concerns raised about the demonstrated efficacy of the COIN principles embodied in FM 3–24.

Insurgency has been the most prevalent form of armed conflict since at least 1949.[2] Countering insurgents, or supporting the counterinsurgency efforts of allies and partners, is the primary focus of ongoing operations in both Iraq and Afghanistan. Such operations are also likely to remain the U.S. emphasis should the Nation become involved (or further involved) in places such as Somalia, Yemen, and Pakistan. Because of growing disparities between the capabilities of conventional and unconventional forces, insurgents, terrorists, and militias are likely to become increasingly common foes.[3] U.S. doctrine for countering insurgencies matters now and is likely to continue to matter.

Colonel Gentile contends that FM 3–24 relies on "unproven theories and assumptions about insurgencies and how to counter them,"[4] criticizes the empirical and theoretical foundation of the doctrine as based on wars of independence that happened over 40 years ago,[5] and concludes that FM 3–24 principles and methods "have not been shown to work in past and current operational practice."[6]

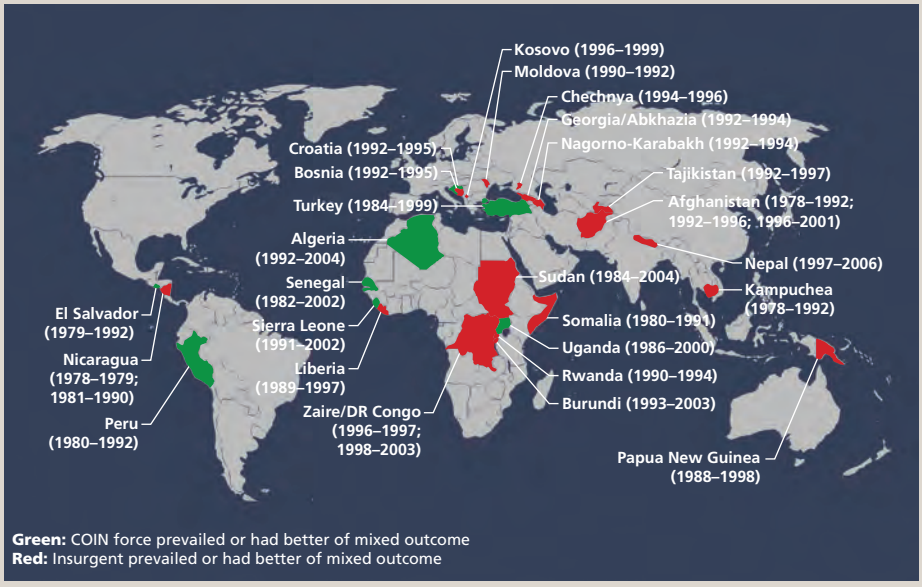
But the question remains: Whether it was sufficiently debated or not, and whether it was formulated on the basis of a small number of older cases or not, *how have the principles espoused in FM 3–24 performed in recent history?*

Neither party to the discussion above offered much beyond references to general history or perhaps to one or two arbitrarily selected cases in support of his views.[7] Here, we bring the weight of substantial and systematic historical evidence to bear. We find that the record of recent history (insurgencies worldwide from 1978 to 2008) supports the principles espoused in FM 3–24. The vast majority of governments and COIN forces that adhered to multiple tenets of the manual prevailed over the insurgencies they opposed. In the preponderance of insurgencies in which COIN forces did *not* follow the principles of FM 3–24, they lost.

## The Evidence

These findings are based on data collected for and published as part of a recent RAND study, *Victory Has a Thousand Fathers: Sources of Success in Counterinsurgency*.[8] In it, we compiled detailed case studies for the 30 most recent resolved insurgencies.[9] This proved to be all insurgencies worldwide started and concluded from 1978 to 2008. Individual cases were compiled from multiple secondary sources and are quite rich and detailed. The cases, their date ranges, and their global distribution are depicted in the map below.

**Map of Studied COIN Case Dates, Countries, and Outcomes**




*Source:* Figure 2.1 in Christopher Paul, Colin P. Clarke, and Beth Grill, *Victory Has a Thousand Fathers: Sources of Success in Counterinsurgency*, MG–964–OSD (Santa Monica, CA: RAND, 2010). Used with permission.

**Dr. Christopher Paul is a Social Scientist at the RAND Corporation. Colin P. Clarke is a Project Associate at RAND and a Ph.D. candidate in the Graduate School of Public and International Affairs at the University of Pittsburgh.**

In 8 of the 30 cases, the COIN force prevailed or had the better of a mixed outcome. These areas are shaded green in the map. In the remaining 22 cases, the insurgents prevailed or had the better of a mixed outcome; these areas are shaded red. Note that in all countries that hosted more than one insurgency during the time span, the insurgents won in every case (so the red shading accurately applies to all cases in those countries).

■ The majority of the population in the area of conflict supported or favored the COIN force.

■ The COIN force avoided culturally offensive behaviors and messages.

The balance of these factors proved a powerful predictor of COIN case outcomes between 1978 and 2008. Seven of the eight cases in which the COIN force prevailed had at least three of the nine FM 3–24 factors present in the decisive phase. In contrast, in only one of the cases in which the insurgents prevailed (Kampuchea, 1978–1992) did the COIN force realize at least three of the nine factors. *This represents a remarkably strong correlation between the application of FM 3–24 principles and success in COIN.*

*while killing or capturing insurgents is an important element of any effective COIN operation, our research demonstrates the importance of preserving the legitimacy of the use of force*

As part of the case-study analysis, we scored the presence or absence of 77 different factors potentially related to COIN outcomes for each phase of each insurgency case.[10] Subsets of these factors were specifically identified as representative of competing approaches to COIN. The approaches tested included FM 3–24 explicitly.[11]

**Test of History**

In our analysis, the application of FM 3–24 was represented by the presence or absence of nine factors in each phase of each of the 30 insurgencies shown on the map. The factors were as follows:

■ A perception of security was created or maintained among the population in areas that the COIN force controlled or claimed to control.

■ Government corruption was reduced or good governance increased since the onset of the conflict.

■ Insurgent-claimed grievances were substantially addressed since the onset of the conflict.

■ The COIN force sought to engage and establish positive relations with the population in the area of conflict.

■ The COIN force provided or ensured the provision of basic services in areas that it controlled or claimed to control.

■ There were short-term investments, improvements in infrastructure or development, or property reform in the area controlled or claimed by the COIN force.

■ The COIN force received substantial intelligence from a population in the area of conflict.

**On Firepower**

In addition to railing against the "unproven" assumptions underpinning the principles espoused in FM 3–24, Colonel Gentile attacks the operational emphasis on restraint in firepower that results. Because of the "stock mantra" that the greater the number of civilians killed, the greater the number of insurgents made, he argues, "firepower . . . has come to be viewed as something dirty, bad, and to be avoided."[12]

While killing or capturing insurgents is an important element of any effective COIN operation, our research unambiguously demonstrates the importance of avoiding repressive tactics and preserving the legitimacy of the use of force.

In our analysis, the repression-based "crush them" approach to COIN is represented by two factors:

■ The COIN force employed escalating repression.

■ The COIN force employed collective punishment.

In the 30 insurgencies fought between 1978 and 2008, fully 20 included the COIN force employing both escalating repression and collective punishment in the decisive phase. Of those 20, only 2 were wins for the COIN force (Turkey, 1984–1999, and Croatia, 1992–1995), and in both those cases, the COIN force engaged in a substantial number of positive COIN practices that offset the impact of repression.[13]

Worse, we found evidence that repression can appear to give the COIN force the upper hand temporarily while decreasing long-term prospects for success. In 19 intermediate phases in the cases (that is, *not* the decisive phase), the COIN force had the upper hand but ultimately lost in a later phase (so they won the phase and lost the case). Seventeen of those 19 winning phases on the way to a case loss included COIN force employment of both escalating repression and collective punishment. Many of the detailed narratives follow this general progression: Once the government decides to take an insurgency seriously, it sends in its military with few restraints. This COIN force smashes the insurgents *and* the population, dealing a heavy blow to the insurgents while significantly alienating the population in the area of conflict. In a later phase, the insurgents recover and gain strength and effectiveness through the (now dramatically increased) support of the population.

Our analysis also considered the legitimacy of the use of force in insurgencies over the past 30 years. Legitimate use of force was represented by five factors:

■ The COIN force avoided excessive collateral damage, disproportionate use of force, or other illegitimate applications of force.

■ COIN force collateral damage was *not* perceived by the population in the area of conflict as worse than that of the insurgent.

■ In the area of conflict, the COIN force was *not* perceived as worse than the insurgents.

■ The perception of security was created or maintained among populations in areas that the COIN force claimed to control.

■ The COIN force was *not* viewed as an occupying force in the area of conflict.

The presence of these factors was also correlated with COIN success. Six of 8 winning COIN forces realized at least 3 of the 5 legitimacy-of-force factors in the decisive phase of their case compared to only 3 of 22 losing COIN forces.

Bottom line: Repression reliably wins phases, not cases. When force is used, care must be taken to ensure that it is legitimate

and that civilian casualties are minimized. After all, COIN is complex and not a zero-sum game. Combined arms prowess and effective restraint both belong in the doctrinal toolbox.

So the principles in FM 3–24 showed strongly in insurgencies worldwide over the past 30 years, not just ambiguously in wars of independence more than 40 years ago, as Colonel Gentile argued. While the details of FM 3–24, like all doctrine, should be subjected to continuing scrutiny and refinement based on operational experience, there appear to be no grounds in the past 30 years of insurgency worldwide for any attack on the core principles of FM 3–24. Similarly, firepower need not be wholly eschewed in COIN, but the record of history suggests that victory over the long term is much more likely to go to those who are judicious in their application of force. **JFQ**

## NOTES

[1] See Gian P. Gentile, "Time for the Deconstruction of Field Manual 3–24," *Joint Force Quarterly* 58 (3d Quarter, 2010); John A. Nagl, "Constructing the Legacy of Field Manual 3–24," *Joint Force Quarterly* 58 (3d Quarter, 2010); Gian P. Gentile, "Freeing the Army from the Counterinsurgency Straightjacket," *Joint Force Quarterly* 58 (3d Quarter, 2010); John A. Nagl, "Learning and Adapting to Win," *Joint Force Quarterly* 58 (3d Quarter, 2010).

[2] Thomas X. Hammes, "Why Study Small Wars?" *Small Wars Journal* 1, no. 1 (April 2005).

[3] Michael T. Klare notes that of the 50 armed conflicts that broke out in the 1990s, only 4 entailed combat between 2 or more states, and only 1, the Persian Gulf War, involved all-out fighting among large numbers of ground, sea, and air forces. See Michael T. Klare, "The New Face of Combat: Terrorism and Irregular Warfare in the 21st Century," in *The New Global Terrorism: Characteristics, Causes, Controls*, ed. Charles W. Kegley, Jr. (Upper Saddle River, NJ: Prentice Hall, 2003), 29.

[4] Gentile, "Time," 116.

[5] Ibid., 117.

[6] Gentile, "Freeing," 121.

[7] Colonel Gentile has written repeatedly on the topic of COIN doctrine. All of his articles on the subject follow the same basic themes: He attacks the creators and proponents of population-centric COIN or FM 3–24 as conspirators of some kind, argues that the doctrine they have promoted is not only wrong but also actually dangerous, and advances the view that more firepower, not less, is the real solution to an insurgency. However, beyond some case detail from Vietnam and Iraq and general references to the American Civil War and World War II, he offers virtually no evidence to support his criticisms or his own claims. For examples of these arguments, see Gian P. Gentile, "A (Slightly) Better War: A Narrative and Its Defects," *World Affairs* (Summer 2008), available at <www.worldaffairsjournal.org/articles/2008-Summer/full-Gentile.html>; "Our COIN Doctrine Removes the Enemy from the Essence of War," *Armed Forces Journal* (January 2008), available at <www.armedforcesjournal.com/2008/01/3207722>; "Misreading the Surge Threatens U.S. Army's Conventional Capabilities," *World Politics Review* (March 4, 2008); "Not So Big of a Tent," March 4, 2008, available at <http://smallwarsjournal.com/blog/2008/03/not-so-big-of-a-tent/>; "The Death of the Armor Corps," April 17, 2010, available at <http://smallwarsjournal.com/blog/journal/docs-temp/416-gentile.pdf>; "Gaining the Initiative in Afghanistan," September 2, 2009, available at <http://smallwarsjournal.com/blog/journal/docs-temp/288-gentile.pdf>; "A Strategy of Tactics: Population-Centric COIN and the Army," *Parameters* (Autumn 2009), 5–17.

[8] Christopher Paul, Colin P. Clarke, and Beth Grill, *Victory Has a Thousand Fathers: Sources of Success in Counterinsurgency*, MG–964–OSD (Santa Monica, CA: RAND, 2010).

[9] Based on a list developed by Martin C. Libicki, "Eighty-Nine Insurgencies: Outcomes and Endings," in *War by Other Means: Building Complete and Balanced Capabilities for Counterinsurgency*, ed. David C. Gompert et al., MG–595/2–OSD (Santa Monica, CA: RAND, 2008), 373–396. The initial case list with which Libicki began was drawn from James D. Fearon and David D. Laitin, "Ethnicity, Insurgency, and Civil War," *American Political Science Review* 97, no. 1 (February 2003).

[10] For details on the factors, their scoring, and how the phases were identified, see Paul, Clarke, and Grill, *Victory Has a Thousand Fathers: Sources of Success in Counterinsurgency*. For a detailed narrative of the case and the scores of the 77 factors for all phases of each case, see Christopher Paul, Colin P. Clarke, and Beth Grill, *Victory Has a Thousand Fathers: Detailed Counterinsurgency Case Studies*, MG–964/1–OSD (Santa Monica, CA: RAND, 2010).

[11] For a detailed discussion of and evidence for all 20 approaches to COIN considered in the research, see Paul, Clarke, and Grill, *Victory Has a Thousand Fathers: Sources of Success in Counterinsurgency*.

[12] Gentile, "Freeing," 122.

[13] See chapter five in Paul, Clarke, and Grill, *Victory Has a Thousand Fathers: Sources of Success in Counterinsurgency*.


## From NDU Press

# PRISM

### A Journal of the Center for Complex Operations

National Defense University announces publication of *PRISM* 2, no. 1 (December 2010). Entering its second year of publication, *PRISM* remains fresh in its outlook on the expanding field of complex security operations. Among the feature articles in this issue: Congressman Samuel Farr examines current efforts to stand up the Civilian Response Corps, drawing upon lessons learned from the establishment of the Peace Corps; William Durch examines exit strategies for complex peace support operations; and Corri Zoli and Nicholas Armstrong explore how U.S. Army doctrine is affecting national security strategy. The "From the Field" article, by William Caldwell and Nathan Finney, is a firsthand report on the problems of the multilateral approach to building police capacity in Afghanistan, while "Lessons Learned" by William Bowers reviews the U.S. earthquake relief operations in Pakistan as an example of leveraging humanitarian missions for strategic success. Closing out the issue are interviews with Senator Jim Webb and U.S. Training and Doctrine Commander GEN Martin Dempsey and several book reviews.

*PRISM* explores, promotes, and debates emerging thought and best practices as civilian capacity increases in order to address challenges in stability, reconstruction, security, counterinsurgency, and irregular warfare. Published by NDU Press for the Center for Complex Operations, *PRISM* welcomes articles on a broad range of complex operations issues, especially civil-military integration. Manuscript submissions should be between 2,500 and 6,000 words and sent via email to prism@ndu.edu.

# Call for Entries for the 2011

## Secretary of Defense National Security Essay Competition and Chairman of the Joint Chiefs of Staff Strategic Essay Competition

Are you a Joint Professional Military Education (JPME) student? Imagine your winning essay in the pages of a future issue of *Joint Force Quarterly*. In addition, imagine a chance to catch the ear of the Secretary of Defense or the Chairman of the Joint Chiefs of Staff on an important national security issue. Recognition by peers and monetary prizes await the winners.

**Who's Eligible:** Students at the JPME colleges, schools, and programs, including Service research fellows and international students.

**What:** Research and write an original, unclassified essay in one or more of the various categories. May be done in conjunction with a course writing requirement. Must be selected by and submitted through your college.

**When:** Essays may be written any time during the 2010–2011 academic year, but students are encouraged to begin the process early and avoid the end-of-academic-year rush that typically occurs each spring. JPME colleges are free to run their own internal competitions to select nominees but must meet these deadlines:

**April 27, 2011:** colleges submit nominated essays to NDU Press for first round of judging.

**May 17–18, 2011:** final judging and selection of winners.

National Defense University Press conducts the competitions with the generous support of the NDU Foundation. For further information, see your college's essay coordinator or go to:

***www.ndu.edu/press/SECDEF-EssayCompetition.html***
***www.ndu.edu/press/CJCS-EssayCompetition.html***

JFQ

**JOINT FORCE QUARTERLY**

Published for the Chairman of the Joint Chiefs of Staff by National Defense University Press
National Defense University, Washington, DC

NDU Press


## From NDU Press

# PRISM

### A Journal of the Center for Complex Operations

National Defense University announces publication of *PRISM* 2, no. 1 (December 2010). Entering its second year of publication, *PRISM* remains fresh in its outlook on the expanding field of complex security operations. Among the feature articles in this issue: Congressman Samuel Farr examines current efforts to stand up the Civilian Response Corps, drawing upon lessons learned from the establishment of the Peace Corps; William Durch examines exit strategies for complex peace support operations; and Corri Zoli and Nicholas Armstrong explore how U.S. Army doctrine is affecting national security strategy. The "From the Field" article, by William Caldwell and Nathan Finney, is a firsthand report on the problems of the multilateral approach to building police capacity in Afghanistan, while "Lessons Learned" by William Bowers reviews the U.S. earthquake relief operations in Pakistan as an example of leveraging humanitarian missions for strategic success. Closing out the issue are interviews with Senator Jim Webb and U.S. Training and Doctrine Commander GEN Martin Dempsey and several book reviews.

*PRISM* explores, promotes, and debates emerging thought and best practices as civilian capacity increases in order to address challenges in stability, reconstruction, security, counterinsurgency, and irregular warfare. Published by NDU Press for the Center for Complex Operations, *PRISM* welcomes articles on a broad range of complex operations issues, especially civil-military integration. Manuscript submissions should be between 2,500 and 6,000 words and sent via email to prism@ndu.edu.

# Call for Entries for the 2011

## Secretary of Defense National Security Essay Competition and Chairman of the Joint Chiefs of Staff Strategic Essay Competition

Are you a Joint Professional Military Education (JPME) student? Imagine your winning essay in the pages of a future issue of *Joint Force Quarterly*. In addition, imagine a chance to catch the ear of the Secretary of Defense or the Chairman of the Joint Chiefs of Staff on an important national security issue. Recognition by peers and monetary prizes await the winners.

**Who's Eligible:** Students at the JPME colleges, schools, and programs, including Service research fellows and international students.

**What:** Research and write an original, unclassified essay in one or more of the various categories. May be done in conjunction with a course writing requirement. Must be selected by and submitted through your college.

**When:** Essays may be written any time during the 2010–2011 academic year, but students are encouraged to begin the process early and avoid the end-of-academic-year rush that typically occurs each spring. JPME colleges are free to run their own internal competitions to select nominees but must meet these deadlines:

**April 27, 2011:** colleges submit nominated essays to NDU Press for first round of judging.

**May 17–18, 2011:** final judging and selection of winners.

National Defense University Press conducts the competitions with the generous support of the NDU Foundation. For further information, see your college's essay coordinator or go to:

***www.ndu.edu/press/SECDEF-EssayCompetition.html***
***www.ndu.edu/press/CJCS-EssayCompetition.html***

JFQ

**JOINT FORCE QUARTERLY**

Published for the Chairman of the Joint Chiefs of Staff by National Defense University Press
National Defense University, Washington, DC

NDU Press