

A full-page photograph of two soldiers in camouflage uniforms and helmets, holding rifles, in a desert environment. The soldier in the foreground is a woman with a focused expression, wearing a helmet with a '32' patch and 'A POS' text. An American flag patch is visible on her sleeve. The background soldier is slightly out of focus.

JFQ

Joint Force Quarterly

Issue 75, 4th Quarter 2014

Joint Logistics Innovations

Chinese Cruise Missile
Developments

2014 Essay
Competition Winners

Report Documentation Page				Form Approved OMB No. 0704-0188	
Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.					
1. REPORT DATE OCT 2014		2. REPORT TYPE		3. DATES COVERED 00-00-2014 to 00-00-2014	
4. TITLE AND SUBTITLE Joint Force Quarterly. Issue 75, 4th Quarter 2014				5a. CONTRACT NUMBER	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S)				5d. PROJECT NUMBER	
				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) National Defense University, Joint Force Quarterly, 260 Fifth Avenue, Building 64, Fort Lesley J. McNair, Washington, DC, 20319				8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)				10. SPONSOR/MONITOR'S ACRONYM(S)	
				11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION/AVAILABILITY STATEMENT Approved for public release; distribution unlimited					
13. SUPPLEMENTARY NOTES					
14. ABSTRACT					
15. SUBJECT TERMS					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT Same as Report (SAR)	18. NUMBER OF PAGES 152	19a. NAME OF RESPONSIBLE PERSON
a. REPORT unclassified	b. ABSTRACT unclassified	c. THIS PAGE unclassified			

Joint Force Quarterly

Founded in 1993 • Vol. 75, 4th Quarter 2014
<http://ndupress.ndu.edu>

GEN Martin E. Dempsey, USA, Publisher

AMB Wanda L. Nesbitt, Interim President, NDU

Editor in Chief

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

Executive Editor

Jeffrey D. Smotherman, Ph.D.

Production Editor

John J. Church, D.M.A.

Internet Publications Editor

Joanna E. Seich

Photography Editor

Martin J. Peters, Jr.

Art Director

Marco Marchegiani, U.S. Government Printing Office

Advisory Committee

COL Michael S. Bell, USA (Ret.), Ph.D./College of International Security Affairs; Maj Gen Brian T. Bishop, USAF/Air War College; LTG Robert B. Brown, USA/U.S. Army Command and General Staff College; BG Guy T. Cosentino, USA/National War College; Brig Gen Thomas H. Deale, USAF/Air Command and Staff College; Col Keil Gentry, USMC/Marine Corps War College; Lt Gen David L. Goldfein, USAF/The Joint Staff; BG Gen Thomas A. Gorry, USMC/Dwight D. Eisenhower School for National Security and Resource Strategy; Col Steven J. Grass, USMC/Marine Corps Command and Staff College; MG William E. Rapp, USA/U.S. Army War College; RDML John W. Smith, Jr., USN/Joint Forces Staff College; LtGen Thomas D. Waldhauser, USMC/The Joint Staff

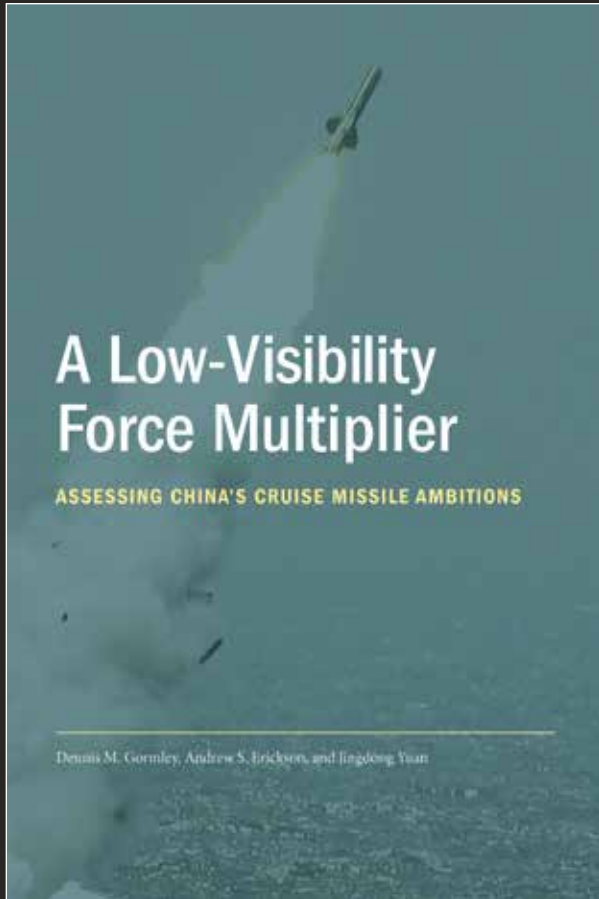
Editorial Board

Richard K. Betts/Columbia University;
Stephen D. Chiabotti/School of Advanced Air and Space Studies;
Eliot A. Cohen/The Johns Hopkins University;
COL Joseph J. Collins, USA (Ret.)/National War College;
Mark J. Conversino/Air War College;
Thomas P. Ehrhard/Office of the Secretary of Defense;
Aaron L. Friedberg/Princeton University;
Col Thomas C. Greenwood, USMC (Ret.)/Office of the Secretary of Defense; Douglas N. Hime/Naval War College;
Mark H. Jacobsen/Marine Corps Command and Staff College;
Col Jerome M. Lynes, USMC (Ret.)/The Joint Staff;
Kathleen Mahoney-Norris/Air Command and Staff College;
Thomas L. McNaugher/Georgetown University;
Col Mark Pizzo, USMC (Ret.)/National War College;
James A. Schear/Office of the Secretary of Defense;
LtGen Bernard E. Trainor, USMC (Ret.)

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

Cover 2 images (top to bottom): Marine takes cover behind berm during firefight in Helmand Province, Afghanistan, July 2014 (U.S. Marine Corps/Joseph Scanlan); Sailor performs maintenance on F/A-18F Super Hornet aircraft assigned to Strike Fighter Squadron 213 aboard aircraft carrier USS *George H.W. Bush* (DOD/Brian Stephens); Airmen with 455th Expeditionary Aircraft Maintenance Squadron work on C-130J Super Hercules engine at Bagram Air Field, Afghanistan (U.S. Air Force/Kayla Newman)





NEW from NDU Press

A Low-Visibility Force Multiplier: Assessing China's Cruise Missile Ambitions

By Dennis M. Gormley, Andrew S. Erickson, and Jingdong Yuan

China's military modernization includes ambitious efforts to develop antiaccess/area-denial (A2/AD) capabilities to deter intervention by outside powers. Highly accurate and lethal antiship cruise missiles and land-attack cruise missiles carried by a range of ground, naval, and air platforms are an integral part of this counter-intervention strategy. This comprehensive study combines technical and military analysis with an extensive array of Chinese language sources to analyze the challenges Chinese cruise missiles pose for the U.S. military in the Western Pacific.

"Cruise missiles are key weapons in China's A2/AD arsenal, providing a lethal precision-strike capability against naval ships and land-based targets. The authors use hundreds of Chinese language sources and expertise on cruise missile technology to assess China's progress in acquiring and developing advanced antiship and land-attack cruise missiles and to consider how the People's Liberation Army might employ these weapons in a conflict. Essential reading for those who want to understand the challenges China's military modernization poses to the United States and its allies."

—**David A. Deptula**, Lieutenant General, USAF (Ret.),
Senior Military Scholar, Center for Character and Leadership
Development, U.S. Air Force Academy

"This volume is a major contribution to our understanding of Chinese military modernization. Although China's ballistic missile programs have garnered considerable attention, the authors remind us that Beijing's investment in cruise missiles may yield equally consequential results."

—**Thomas G. Mahnken**, Jerome E. Levy Chair of
Economic Geography and National Security, U.S. Naval War College

"This book provides an excellent primer on the growing challenge of Chinese cruise missiles. It shows how antiship and land-attack cruise missiles complicate U.S. efforts to counter China's expanding A2/AD capabilities and are becoming a global proliferation threat. The authors also demonstrate just how much progress China has made in modernizing and upgrading its defense industry, to the point of being able to develop and produce world-class offensive weapons systems such as land-attack cruise missiles. This book belongs on the shelves of every serious observer of China's growing military prowess."

—**Richard A. Bitzinger**, Coordinator, Military Transformations Program,
S. Rajaratnam School of International Studies, Singapore

Available online at ndupress.ndu.edu/Portals/68/Documents/Books/force-multiplier.pdf

In this Issue

Dialogue

- 2 From the Chairman
4 True and Steady,
Inspection Ready
*By Bryan B. Battaglia
and Curtis L. Brownhill*

Forum

- 6 Executive Summary
8 An Interview with
Raymond T. Odierno
13 Theater Airlift Modernization:
Options for Closing the Gap
By Robert C. Owen
19 The Afghanistan National
Railway: A Plan of Opportunity
*By Lawrence J. Pleis, Richard
Llitas, David A. Wood, Matthew D.
Bain, and Steven J. Hendrickson*
28 The USCENTCOM Train: The
Deployment and Distribution
Operations Center Turns 10
By Mark A. Brown

Essay Competitions

- 32 2014 Winners
34 Deterrence with China: Avoiding
Nuclear Miscalculation
By David S. Forman
43 The Limits of Cyberspace
Deterrence
By Clorinda Trujillo
53 Opportunities in Understanding
China's Approach to the
Senkaku/Diaoyu Islands
By Bradford John Davis

JPME Today

- 57 Cyber Security as a Field of
Military Education and Study
*By Eneken Tikk-Ringas, Mika
Kerttunen, and Christopher Spirito*
61 Why Military Officers Should
Study Political Economy
By Rebecca Patterson and Jodi Vittori
70 Low Cost, High Returns:
Getting More from
International Partnerships
*By Russell S. Thacker and
Paul W. Lambert*

Commentary

- 77 Asymmetry Is Strategy,
Strategy Is Asymmetry
By Lukas Milevski



About the Cover

Soldiers of 92nd Engineer Battalion stand guard during force protection exercise at Forward Operating Base Hadrian in Uruzgan Province, Afghanistan, March 2013 (U.S. Army)

- 84 Is Military Science "Scientific"?
By Glenn Voelz
91 The Best Man for the Job?
Combatant Commanders and
the Politics of Jointness
By R. Russell Rumbaugh

Features

- 98 A Potent Vector: Assessing
Chinese Cruise Missile
Developments
*By Dennis M. Gormley, Andrew S.
Erickson, and Jingdong Yuan*
106 Blurred Lines: Cultural Support
Teams in Afghanistan
By Megan Katt
114 Determining Hostile
Intent in Cyberspace
By Ramberto A. Torruella, Jr.
122 Understanding the Enemy: The
Enduring Value of Technical
and Forensic Exploitation
*By Thomas B. Smith and
Marc Tranchemontagne*

Recall

- 129 Challenges in Coalition
Unconventional Warfare:
The Allied Campaign in
Yugoslavia, 1941–1945
*By J. Darren Duke, Rex L. Phillips,
and Christopher J. Conover*

Book Reviews

- 135 You Cannot Surge Trust
Reviewed by Dov S. Zakheim
136 Engineers of Victory
Reviewed by Bryon Greenwald
137 Next-Generation
Homeland Security
Reviewed by Katie Kuhn

Joint Doctrine

- 139 Implementing Joint Operational
Access: From Concept to
Joint Force Development
By Jon T. Thomas
143 Dealing with Corruption: Hard
Lessons Learned in Afghanistan
*By Richard J. Holdren, Stephen F.
Nowak, and Fred J. Klinkenberger, Jr.*
148 Joint Doctrine Update

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. All published articles have been vetted through a peer-review process and cleared by the Defense Office of Prepublication and Security Review.

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

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

Submissions and Communications

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

Editor, *Joint Force Quarterly*

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

Telephone: (202) 685-4220/DSN 325

Email: JFQ1@ndu.edu

JFQ online: www.dtic.mil/doctrine/jfq/jfq.htm

4th Quarter, October 2014

ISSN 1070-0692



Chairman speaks with U.S. military officers before ISAF and U.S. Forces–Afghanistan change of command ceremony August 26, 2014, in Kabul, during which Marine Corps General Joseph F. Dunford, Jr., relinquished command to Army General John F. Campbell (DOD/Sean K. Harp)

From the Chairman

Commitment to Service

Representing America to the rest of the world is something that we all take great pride in. We know what a privilege it is to represent our country overseas. Of course, representing our nation is not an experience entirely unique to the military.

I recently had the honor of presiding over a dog tag exchange with our country's best basketball players as they were preparing for the 2014 International Basketball Federation World Cup. Servicemembers from across the joint force presented a set of dog tags to each member of Team USA. Sergeant

Major Bryan Battaglia, USMC, presided over a similar ceremony in June for the national soccer team as it was departing for Brazil. In both instances, the athletes and Servicemembers were honored and excited to be a part of the ceremony.

Dog tags are an iconic symbol of the military and have been representative of the sacrifices inherent in military service since their debut on the battlefields of the Civil War. For the men and women who wear them, dog tags are a personal and profound reminder of what it means to represent the United States of America. They are a symbol of courage and a

representation of the trust we share with our teammates, our leaders, and the Nation that supports us.

On the front of these particular dog tags are the American flag and the words "Leadership, Service, and Teamwork." While these are values we hold dearly in the Profession of Arms, they are also shared values that are important to all Americans.

Service has always been fundamental to being an American, and the greatness of our nation stems from our collective willingness to serve others. Across our country, police officers, firefighters,

teachers, coaches, pastors, Scoutmasters, business people, and many others serve their communities every day. No matter the uniform, the desire to contribute permeates every corner of the United States. Exchanging these dog tags highlights that common commitment to our country and its ideals.

Serving Together

Over the past decade, the American people have provided unwavering support to our military family. For that strong support, I am extremely thankful. Looking ahead, we need to think about how we will continue to connect with America. The American people appreciate what we do when we are called on to fight in faraway places. Less understood are the ways we continue to serve in our communities when we take off our uniforms—whether at the end of the day or at the end of our careers.

These dog tag exchanges are the first step in a Department of Defense initiative to inspire an enduring commitment to service and to enrich local communities across America through the influence of the U.S. military and the popularity of American sports. Through this Commitment to Service, athletes and members of the military will work together—on panels, workshops, and service projects—to make a difference in our communities.

Commitment to Service tips off this Veterans Day with service projects conducted in partnership with the National Basketball Association. This initiative with the NBA is one way we can help others better understand the military and find innovative ways to address the needs of the communities in which we live and work.

These efforts will showcase the pride that all of us have in representing our country, whether in athletic attire or a military uniform. Servicemembers and athletes will work side by side to serve their communities and demonstrate the value of not only military service, but also service that aims to better our country and contribute to the common good.

Sparking a Commitment to Service

This is not a military appreciation program focusing on what Americans can do for Servicemembers. Rather, Commitment to Service focuses on what we can do with our fellow citizens *for* America. It is a program of appreciation by the military for our great nation and the communities that support us. Through Commitment to Service we can continue to serve others and help foster a broader spirit of service across the country.

Every day I am honored to put on my uniform and represent the Servicemembers who make up today's joint force. For the last 3 years, it has been my privilege to tell the story of your military service to the American people. Often untold, however, is the story of your commitment to our local communities and your willingness to continue service, even out of uniform. Over the course of the next year, I will be highlighting the contributions, beyond their military service, that Servicemembers and Veterans make to our communities. The Commitment to Service initiative is one way of showcasing those contributions.

I hope you will join me in this effort. JFQ

MARTIN E. DEMPSEY

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



New from NDU Press

for the Center for Strategic Research

Strategic Forum 288

The Rising Terrorist Threat in Tanzania: Domestic Islamist Militancy and Regional Threats

by Andre LeSage



In this paper, Dr. Andre LeSage argues that the growing number of militant Islamist attacks in Tanzania

demonstrates a nascent terrorist threat that can undermine peace and stability in yet another East African country. Local and regional dynamics—including foreign fighter returns from Somalia, disputes over the Zanzibar Islands, and national elections in 2015—could create a “perfect storm” that would exacerbate the threat. If its issues remain unaddressed, Tanzania is likely to experience the same security trends as Kenya, where, with the help of external support, local capabilities have been developed to conduct increasingly deadly attacks that affect U.S. and other foreign interests. In response, the United States needs to focus policy-level attention on the situation in Tanzania and invest additional intelligence, law enforcement, and strategic communications efforts to combat the spread of violent extremism.



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



Retired Army 1st Sgt. William Staude of Elliott, Pennsylvania, salutes Soldiers from 316th Expeditionary Sustainment Command stationed in Coraopolis, Pennsylvania, as they march past him during Veterans Day parade in downtown Pittsburgh, November 2011 (U.S. Army/Michael Sauret)

True and Steady, Inspection Ready

The global security environment in which the U.S. Armed Forces must operate, manage, and influence presents many challenges to our all-volunteer force. Moreover, shifting societal norms (domestic and abroad) often compete directly and indirectly with the professional norms that shift over time. The effect of variances in societal and professional norms can and often does induce friction points and challenges us to stay on the right course, defined by the qualities of honor, respect, duty, service, courage, commitment, loyalty, and integrity, as well as the virtues of decency, fairness, honesty, humility, integrity, and valor through actions. The standards

required to sustain the Profession of Arms must always be maintained.

The American people have always understood that their external security and their guarantees of inalienable rights largely rest on the shoulders of the U.S. military. Indeed, they support the raising, funding, and sustainment of the Armed Forces because without them, our nation's safety and security would decline. Given the importance of the Armed Forces, its special relationship to the American people, and the notion that *the few protect the many*, young men and women from all walks of life are encouraged to serve and contribute to something larger, deeper, and more profound than one's own self.

There is an enduring obligation on the part of the members of the Profession of Arms not only to keep the Nation safe and secure, conduct and execute well-planned military operations, and provide responsible management of national resources, but also to inspire others and meet or exceed the expectations of the American people. Every profession has, in effect, a compact with the larger society. Society grants the profession certain powers, privileges, and prerogatives not normally granted to others; in exchange, the profession provides reliable and longstanding service to society. More particularly, members of the profession are granted wide discretionary latitude in performance of their specialized duties.

Given the nature of the Profession of Arms, it embodies high standards fostered through an unwavering dedication to duty, an ethical and moral high ground, and a rigorous code of conduct. In the purest sense, *all* members of our profession, regardless of rank or status, *live a life ready for inspection*.

Living in such a way begins in the earliest part of the military career. Fresh from society writ large, new recruits become exposed to a life different from any other. Trained, tested, and developed, only then are they afforded an official membership into the profession. From that point forward, irrespective of tenure, true members of the profession instinctively conduct themselves in a manner that exemplifies confidence, integrity, obedience, and courage to all who view them. It is an internal disciplining mechanism that triggers our ability to sidestep unethical temptations and potential points of corrosion.

Living a life ready for inspection requires strength in purpose and frequent introspection. It means sharpness in duty and squared away in conduct. It is not a checklist approach to one's professional conduct or actions; rather, it is a behavioral compass that keeps a true azimuth. Indeed, course corrections are within each of us. So perhaps a good way to portray the virtues of living a life ready for inspection is to consider the oaths of commissioning and enlistment; both deliver the obligation to support and defend the Constitution against all enemies, foreign and domestic. That obligation, however, deserves a deeper consideration.

We understand that a threat to national security often requires overseas deployment and engagement in multiple postures, from combat to partnership-building. However, there are additional forms of threats to our nation and the Profession of Arms that each Servicemember is responsible for deterring, dissuading, or defeating. For instance, institutionally and individually, we defend opportunity for all—to ensure all have the same rights and no one is institutionally held back from achieving his or her goals and desires based on race, creed, or religion. We fight to defeat

prejudice, and we defend human rights. We do not condone unethical behavior or less than honorable actions within our ranks. We ensure command climates and duty environments are free of intolerance and are not overly permissive. We instill a sense of unity, purpose, good order, and discipline and compliance with standards, tradition, culture, customs, and courtesies. We police our ranks and are willing to undergo scrutiny when we fail in the eyes of our teammates, our units, our profession, and the society we serve. Furthermore, when one's service to the Nation comes to a close, we give back to society a stellar model citizen who understands that actions have cause and effect and that living a life ready for inspection is a foundation gained from military service.

As part of choosing to serve our country, we unselfishly sacrifice many of the comforts and luxuries normally afforded to an average individual or American family. Through varying lenses and under constant evaluation, we execute our duties as the Nation's defenders and are prepared to hold accountable those who are less than ready for inspection. In many regards we are role models for our youth, warriors to our enemy, and ambassadors of our country.

The quality of the reciprocal relationship between the military and the American society it serves goes back to the citizen soldier of the Revolutionary War. Over the centuries and decades, through conscription or through a volunteer force, the Nation continues to provide its sons and daughters the opportunity to serve in this admired profession. For that, we owe it a life ready for inspection. JFQ

BRYAN B. BATTAGLIA

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

CURTIS L. BROWNHILL

Chief Master Sergeant
U.S. Air Force (Ret.)

New from NDU Press

for the Center for the Study of
Chinese Military Affairs

China Strategic Perspectives 7
*"Not an Idea We Have to Shun":
Chinese Overseas Basing
Requirements in the 21st Century*
by Christopher D. Yung and Ross
Rustici, with Scott Devary and
Jenny Lin




China's expanding international economic interests are likely to generate increasing demands for the People's

Liberation Army Navy (PLAN) to operate out of area to protect Chinese citizens, investments, and sea lines of communication. How will the PLAN employ overseas bases and facilities to support these expanding operational requirements? In this study, main authors Dr. Christopher D. Yung and Ross Rustici's assessment is based on Chinese writings, comments by Chinese military officers and analysts, observations of PLAN operational patterns, analysis of the overseas military logistics models other countries have employed, and interviews with military logisticians.



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



During rescue mission, HH-3E Jolly Green helicopter code-named "Banana," carrying 14 Green Berets, deliberately crash landed inside walls of North Vietnam's Son Tay POW camp, November 20, 1970 (USAF)

Executive Summary

As we mark this 75th issue of *Joint Force Quarterly*, I am reminded of the wisdom I gained some years ago when I was seeking to become a teacher. My faculty mentor at the time offered some advice as I took up the task of teaching history. I asked him, "Does history repeat itself?" His response was useful but not easily digested. "History does in fact repeat but not in detail or on a schedule," he said. "We as teachers need to identify both the similarities and differences of events past and present in order to have our students learn." Recent events that fit this model of the past repeating itself, but not in detail, include rioting in Missouri surrounding the violent death of an African American teenager, a failed special forces raid into Syria

to rescue an American reporter held hostage, airliners shot down by military forces, mass migration of people seeking security in a foreign land, deadly disease spreading in Africa, and the withdrawal of U.S. combat forces from an unpopular war—to name a few in today's headlines.

Despite all of the advances in medicine, technology, education, and political systems, change has yet to completely impact the one biological fact my mentor gave me. The human brain remains as it has been for over 50,000 years. What we put into it makes the difference in how we live our lives. Put another way, investing time and energy into education is the best means to affect any kind of change in the human condition. The question is what kind of education can move us

forward to reduce the cycle of violence, both domestically and globally, that seems to continually reappear. Many who read this may not be old enough to remember the past events that mirror those of today (Selma, Alabama; the Son Tay and *Desert One* rescue missions; the downing of Korean Airlines Flight 007 and the Iranian Airbus; Vietnamese and Cuban refugees; Ebola again), but careful study can help us see what important work remains unfinished and what new challenges lie ahead. Our readers are in luck as *JFQ* continues to offer opportunities to learn from the past to prepare for the future with change for the better in mind.

The Forum opens with an interview of U.S. Army Chief of Staff General Raymond T. Odierno. Discussing a range of topics from force drawdown to

modernization, General Odierno lays out the future for the Army and its relationship to the joint force. Identifying critical shortfalls ahead, Robert Owen then provides a range of options to modernize theater airlift, a critical capability as recent operations have shown. One of the more interesting and not well-known success stories from Afghanistan is its railroad system. Lawrence Pleis, Richard Lliteras, David Wood, Matthew Bain, and Steven Hendrickson, who were involved in its construction, offer a fascinating look into how it was built with international assistance. Next, Mark Brown discusses another type of train, a joint one, that recently celebrated a birthday of sorts. He discusses how U.S. Central Command's Deployment and Distribution Operations Center has been delivering the mail and a whole lot more for over a decade in support of U.S. operations in that theater.

As we do each year, we next present the winning essays from the 2014 8th Annual Secretary of Defense and 33rd Annual Chairman of the Joint Chiefs of Staff Essay Competitions. This year's competition once again has yielded some outstanding writing on timely topics. The judges from across the joint professional military education (JPME) community all commended the students for their critical thinking skills and writing talent. In the winning Secretary of Defense essay, Commander David Forman, USN, discusses how to consider the future of China's military in terms of deterrence. Lieutenant Colonel Clorinda Trujillo, USAF, won in the Chairman's strategic research paper category with an insightful discussion of deterrence in cyberspace. In the Chairman's strategic article category, in which the author must develop and defend a thesis in only 1,500 words or less, Lieutenant Colonel Bradford John Davis, USA, offers some interesting ideas on the issue of territorial claims to the Senkaku/Diaoyu Islands.

Our essay competitions this year indicate that all things cyber are at the top of the list of issues in international security circles. Eneken Tikk-Ringas, Mika Kerttunen, and Christopher Spirito lead off our JPME Today section by considering the value of studying cyber

security as an element of professional military education. Of note, the recently updated curriculum here at the National Defense University is taking the authors' advice with a number of lessons dedicated to cyber issues having been added or enhanced from previous instruction. Other PME institutions are doing so as well. From the faculty of the world's newest JPME-qualified school, NDU's College of International Security Affairs, faculty members Rebecca Patterson and Jodi Vittori advocate adding political economy to PME. From NDU's International Student Management Office, Russell Thacker and Paul Lambert discuss how to continue benefiting from relationships with international officers long after they have graduated from PME classrooms. Surprisingly, their research shows that we are not taking sufficient strides to do so.

Our Commentary section has three distinct authors and ideas to consider. Returning to the pages of *JFQ*, Lukas Milevski develops an important discussion of asymmetry and strategy, which may seem simple enough. If the last decade or more of war has taught us, however, nothing in the world of strategy is easily learned. Another important argument comes from Glenn Voelz on the concept of "military science." Every student of Carl von Clausewitz knows of the tension that comes from the desire to create order out of chaos, but in the end, is it art or science, or both, that tips the scale in military affairs? If you are a frequent reader of *JFQ*, you may have read Admiral Samuel Locklear's response to my question about whether U.S. Pacific Command would begin rotating among the Services for its leadership. Russell Rumbaugh provides us a full appreciation of the history and decisionmaking involved in who has been selected to command at the top of U.S. joint forces around the world.

From China's growing antiaccess/area-denial capabilities to determining hostile intent in cyberspace, the Features section serves up some of the best of today's thinking and writing in these areas and more. Adding to their recently published NDU Press book on the subject, Dennis Gormley, Andrew Erickson,

and Jingdong Yuan describe important developments in Chinese cruise missiles to date. By detailing the experience of dealing with cultural differences in Afghanistan, Megan Katt adds to the continuing discussion of how the joint force deploys new kinds of teams to deal with complex operations. Adding significantly to what is becoming the leading collection of cyber related writing, Ramberto Torruella, Jr., helps us understand the difficulty involved in finding the responsible person or persons behind a cyber attack. Lastly, Thomas Smith and Marc Tranchemontagne show that the military's pursuit of terrorist organizations requires a dedicated effort to exploit the traces left behind by these groups.

Our Recall article, by J. Darren Duke, Rex Phillips, and Christopher Conover, examines the highly successful United Kingdom-U.S. joint unconventional warfare campaign in Yugoslavia during World War II.

As always we bring you three fine book reviews to further assist your efforts to find good works to add to your library.

Joint Doctrine offers two important discussions aimed at shaping doctrine in two important areas: the implementation of the Joint Operational Access Concept and how to effectively deal with corruption in those places where the joint force employs. These important articles along with the Joint Staff J7 Joint Doctrine Update should lead to a good amount of discussion on emerging areas that should improve existing—and possibly make new—doctrine.

Lastly, this issue marks retirement of the last two remaining "plank holders" of the original *JFQ* staff from the journal's 1993 launch: Mr. Calvin B. Kelley and Mr. Martin "Jimmy" Peters, Jr. We who remain have learned a great deal from these gentlemen who helped build and sustain the Chairman's Journal for more than 20 years and 75 issues. We wish them great happiness in their lives ahead. *JFQ*

WILLIAM T. ELIASON
Editor in Chief



staying in the Service; they're not leaving en masse to do other things. So we have an incredible force, and I want to build on that. We have a wealth of experiences from junior to senior officers that we've never had before, and we have to learn how to exploit the experiences gained in joint, multinational, interagency, and intergovernmental environments, and I think that's key to the future.

I do see three major challenges for the Army: First, as we sit here today, we still have over 60,000 people deployed around the world, so we have to make sure that these Soldiers are prepared to do the missions that we're asking them to do. Second, we have to figure out how to keep these Soldiers prepared while, with the fiscal realities of today, we're in the process of downsizing the Army. I need to make sure that I balance that and I need to make sure that I'm taking the Army down in such a way in which we are still meeting our operational commitments and requirements, taking care of our Soldiers, but also taking a stand in order to meet the budget pressures. Third, we have to ask ourselves what we want the future Army to look like. The world around us is changing rapidly, and I tell everyone it might not be the most dangerous time, but it's the most *uncertain* time that I've seen. And we have to have an Army that is capable of adapting to the new realities. We have to have an Army that is looking forward and implementing what we've learned in the past but also looking forward to see what we have to develop for the future.

JFQ: What are your priorities for meeting those challenges?

General Odierno: As I look around the world today, I ask how can the Army contribute across the full range of operations in order to prevent conflict, shape the environment for the combatant commanders to ensure access to build partner capacity, and then, if necessary, win. Maintaining a highly trained and professional all-volunteer force is the number one priority; moreover, we have to develop leaders who can operate in complex environments. I want to sustain

An Interview with Raymond T. Odierno

Joint Force Quarterly: After more than a decade of combat around the world, what can you tell us about the challenges facing today's Army?

General Raymond T. Odierno is the Chief of Staff of the U.S. Army. JFQ Editor in Chief Dr. William T. Eliason interviewed General Odierno at the Pentagon. NDU Press Internet Publications Editor Ms. Joanna E. Seich transcribed the taped interview.

General Raymond T. Odierno: We're starting from an incredible position of strength because of the experience that the Army has. This is the first time after a long period of war that Army leaders are

the advantages we have now, and I think that we have an asymmetric advantage both in our noncommissioned officers and officers and in their ability to operate in a joint, interagency, and multinational environment. We have to continue to develop these Soldiers as we move forward. We have to optimize performance; we have to optimize our management of our talent. To me, that's number one by far.

We also have to be globally responsive and regionally engaged. By globally responsive, I mean that in the future, we're going to have many more "no-notice" small contingencies, and we have to be responsive in such a way that we can tailor and scale our response to not only the place we're going, but also the mission. When I talk about the need for decisive landpower as part of the joint force, that doesn't necessarily mean decisive landpower to fight wars—that means decisive landpower to build partner capacity, to respond to humanitarian assistance and disaster relief, and to build interoperability and multinational capability. We look to solve problems. Decisionmaking will probably be much more decentralized in the future, and we have to ensure that our young men and women are prepared for that. "Globally responsive" means responding quickly and understanding the region in order to be responsible for it.

In fact, there are two recent examples where we've done this. The first is the deployment of four companies to Eastern Europe to assure our allies after Russia's recent actions in the Ukraine. The second is the quick deployment of an assessment force to Iraq—a majority of that being the Special Operation Army Conventional Capability. They are two small examples of how I see the future. We have to possess that capability and we have to continue to build it as we move forward. That's what we're doing regarding setting our priorities for the future.

JFQ: How do you propose to incorporate lessons learned from combat in Iraq and Afghanistan into the future force?

General Odierno: First, a strategic response is going to be much more

decentralized and it's going to be done at a lower level. Also, it's going to be done in a smaller footprint, which is exactly how we operated both in Iraq and Afghanistan where we decentralized responsibilities to lower levels of commands.

Second, we've learned that there will never again be an operation that's purely a military operation. It's going to be one that's conducted in a joint, interagency, intergovernmental, multinational context. So we have to prepare ourselves to operate in that environment.

Third, which is almost counterintuitive, since we're going to have to operate in this joint interagency, intergovernmental, multinational environment, we have to ensure that we are preparing our headquarters to do that.

Last, our adversaries have learned that they must do everything they can to take away our technological advantages. So we have to be capable of operating in a diverse, hybrid environment that will have a combination of conventional capabilities, an environment of terrorist activity [in counterterrorism], as well as an environment of opportunists, insurgents, and criminal activity. No matter where we operate, we are going to have the potential for these environments.

JFQ: How is the Army dealing with the fiscal constraints of recent years, and what kind of planning have you requested should the full impact of sequestration become a reality? In particular, can you discuss the likely effects on the total force?

General Odierno: We're conducting significant planning in these areas, and our assumption right now is that the law of the land is sequestration and that it'll be full sequestration. There will be several impacts on the Army, but really on the joint force. I'll speak to the Army first.

We've done our planning in order to do the things I've already mentioned. But there are three things to balance. You have to balance end strength, readiness, and modernization. Because of the sharp acts of sequestration, however, the next 4 to 5 years will not be in balance. So upfront, because we have to take end

strength down over a 5-year period due to the operational commitments that we have, we are taking some risk in readiness and modernization. That means we're out of balance and we might not obtain appropriate readiness levels. We are delaying modernization, too, which might not allow us to keep our edge in mobility, lethality, and survivability. That's the short, midterm problem.

Once we get rebalanced again, which looks like the 2019, 2020, or 2021 timeframe, we have another problem, which I've testified to. We'll have a smaller force. It'll be ready and we'll begin to reintroduce modernization, but I think we will be too small to meet the current national security strategy. So we have to readjust the goals we have in national security because we will not be able to meet the requirements we currently have in leading and building security and stability in all the regions around the world. That's the longer term challenge.

JFQ: In recent talks, you have mentioned your view that the Army needs to become globally responsive. What ways do you believe the Army needs to change to meet that goal?

General Odierno: We have to think a bit differently, and again I think it ties to how we're going to operate in the future. Over the last 12 or 13 years, we've gotten very used to moving into areas with mature infrastructures. For example, we've built up Iraq and Afghanistan so when we fall in, there are basecamps, there is support that's already set up, there's life support, equipment support, and training support, which is what we normally would do if we were somewhere for a long period of time. But in the future, we're going to be required to go in quickly, and probably into remote areas that have little infrastructure, so we have to get back to understanding that when we deploy somewhere, we have to be able to sustain ourselves for fairly significant periods of time organically.

We have to build packages that are small, that meet the requirement, and that can be moved very quickly—whether by



Chief of Staff gives remarks during promotion ceremony at headquarters, 4th Infantry Division, Fort Carson, Colorado (U.S. Army/Teddy Wade)

air or sea—and we have to be cognizant of this early on. One of the things all Army leaders have talked about is our ability to build these small packages to respond.

There are several important things along this line of thought that we have to be able to do. Thus, as we talk about being globally responsive, we have to make sure we're able to acquire and maintain a level of information awareness, even as we're deploying. We have to have robust command and control communications, but with small packages that require us to have less support. We have to increase mobility and survivability, but in smaller packages. What the Army brings to the joint force is a variety of capabilities that no other Service brings: We can send light, medium, or heavy airborne capabilities, or we can mix the three together. We can also provide task forces from 200 troops to 50,000. We can support ourselves, so we can build packages that are uniquely organized to meet a required need—whether it is for

humanitarian assistance or operations. We have to build that capability and make sure that we can do it in the right size, get there with the right speed, and be able to accomplish the right mission. I believe the Army is the Service that can do things at many speeds, many sizes, and many different types of activities.

***JFQ:** A number of social issues have been affecting all the Services, such as repeal of the “Don’t Ask, Don’t Tell” policy, integration of women into combat specialties previously barred to them, sexual assault and suicides, and senior officer misconduct, to name a few. What is the Army’s approach to working these issues?*

General Odierno: For the Army, it is important to bring in the best, most qualified talent that’s available, and it is about talent management. To do that, we have to make sure that we create an environment in which all Soldiers not only

believe they can increase their own personal capabilities, but also contribute to the greater good and the team capabilities we have. We have to create an environment where many different people with many different beliefs can operate effectively and are not discriminated against and can reach their full potential. That’s the underpinning of everything we do.

We have been able to implement the repeal of “Don’t Ask, Don’t Tell,” frankly, with only very small issues—and almost no issues at all. It is important that we continue to integrate and make everybody feel comfortable.

Increased opportunities for women in the Army is another priority. The Army has more women than any other Service in terms of numbers, and it’s important they get all the opportunities they can meet. We have to be able to ensure that they feel comfortable in the environment we’re in, so we take sexual assault seriously. It is our number one priority, and we have made some good progress.

Number two is making sure if something does happen, we have advocates who allow victims to go through the process and feel comfortable that people are concerned about them. The third piece is holding people—the predators who are targeting women, and in some cases men—accountable. Also, holding commanders accountable for creating the right environment where people believe they can [talk] openly. We're working aggressively at that.

All this comes under the Army profession, which gets to the other points you were referring to in terms of senior leader misconduct and other things. We are the most respected profession, and it is important that we sustain that. People have a lot of trust and confidence in us, so it is important that we sustain that confidence.

But there are a couple things we've learned that are necessary for us to continue to build the profession. For instance, we're implementing programs that do 360-degree assessments for all commanders, and now we're starting that program when people first come into the Service. It's a self-development tool, but it's also an awareness tool for command climate and how things are being done. It also lets us know where we should expand that particular program. We have implemented a significant amount of training in all of our professional military schools that concentrate on the responsibilities that Soldiers have as leaders and the ethical/moral requirements that we expect of leaders. The foundation of everything is trust: We talk about trust between Soldiers, trust between Soldiers and leaders, and then trust among Soldiers, leaders, and the institution, and finally trust between the institution and the American public.

We also talk about three basic characteristics that we expect all our Soldiers to have: competence, commitment, and character. We expect our Soldiers to be competent, which is building expertise and constantly learning to improve that expertise. We expect commitment: commitment to your Soldiers, commitment to your unit, commitment to the mission, commitment to the institution.

Most important is character. Character is what defines us. Character is about understanding the moral and ethical values that we represent, as well as the ethical dilemmas that we face throughout our careers. These dilemmas start out small and it's how we deal with them early on that sets our character and how we deal with difficult problems as we grow in responsibility. We are focused on ensuring that we emphasize competence, commitment, and character to the institution. This is ingrained in every one of our training programs. I recently attended a symposium of Army leaders that talked specifically about the profession and ethics. We're taking this discussion very seriously as we move forward.

Finally, as we look at talent management, it is important to look where all Soldiers can serve. We want to open up positions based on standards, not based on preconceived notions of sex—male or female—or other biases we want to eliminate. We want to make the Army a standards-based organization, so we've worked hard on developing standards that we think are right for every MOS [military occupational specialty]. This is why we are doing significant work to make sure we have underpinning information that will allow us to move forward and open as many positions as possible to women in the future.

JFQ: All the Services have programs for helping their wounded warriors and their families. As the Army has the largest population of recent combat veterans in and out of uniform, can you discuss your program called Soldiers for Life, as well as other programs that make up how the Army is working to help veterans?

General Odierno: There are two specific programs that relate to this question. One is the Soldier for Life program, which I put into place 2½ years ago when I became the Chief of Staff of the Army. It's important for Soldiers to understand and believe that from the time they come into the Army and for the rest of their lives, we consider them to be Soldiers who served honorably and who deserve

the care and attention necessary. This covers not only wounded warriors, but also Soldiers who have served honorably and now decided to go into civilian life. We will assist them as they move forward in integrating back into civilian society. Because we believe they are great people to hire, we believe they can be great representatives of and contribute greatly to society both locally and nationally.

The second piece is that we must never forget what our Soldiers and wounded warriors have sacrificed, including the families who have sacrificed loved ones. One of my major concerns today is that even though people do understand the importance of providing care—and we get lots of external support, both private and public—we have to ensure that this same care is available in 5, 10, or 15 years, especially to Soldiers who have been wounded and families who have lost loved ones. We have to make sure that we recognize their sacrifices. So we are building programs that will allow us to do this.

The second program that is important is the Ready Resilient program, which builds mental and physical abilities to become more resilient. As we continue to ask our Soldiers to operate in complex situations, we want them to build resilience that enables them to deal with difficult issues. It's about not only proving individual capabilities but also reducing the risk of suicide and other issues that we've faced.

The last program is one we are working on with Veteran's Affairs. As we hand over our Soldiers from the Army to Veteran's Affairs, we want that process to go as smoothly as possible—and we still have a lot of work to do in that area. Although we've made some progress, we have not yet made the progress necessary to have visibility as we move forward.

JFQ: What is the Army's role within the Joint Force 2020 and beyond? Specifically, what role does jointness play in your efforts to achieve that force?

General Odierno: As I think about all the missions we have, whether we're

detering conflict or building capability with our partners, we must have a balanced joint force. We have to have a capability in the Navy, Air Force, Marine Corps, and Army that not only enables us but also ensures that our adversaries understand we have this capability that can deter and compel them not to make misjudgments or miscalculations that could lead to conflict.

As mentioned earlier, the Army provides specific and unique capabilities that no other Service can. For example, the Army provides the majority of support to the joint force and combatant commanders in terms of enablers. Whether it's [intelligence] support, engineer support, logistics support, command and control capability, we are the largest provider to the joint force to include the combatant commanders, and so I think that's an important mission.

I also believe in the notion of strategic landpower. I often joke that we know 72 percent of the world is water, but I always say 100 percent of the people live on land. To create security and stability requires the ability to interact with individuals on land, and we do that in several ways. The United States does it diplomatically, but it also does it through [military-to-military] relationships, and the Army plays a significant role in this. Understanding the human dimension of conflict and the human domain and how that impacts our ability to interact and build relationships in every region of the world is very important. This gets to the point of regional forces and our ability to align forces to combatant commanders that allows them to meet their missions and to be an integral part of the joint force. Doing so establishes what I consider a global landpower network. It is a small footprint, but it still allows us to respond. This network can have Marine capability, special operation forces capability, and Army capability. We are in the process of establishing this network, and the Army will continue to be an integral part of the joint force.

We have to be careful that all the Services do not focus on domain warfare, which takes us away from jointness. The Services are too worried about the



Soldier scans surrounding area for potential enemy movement during mission in Saberi district of Khowst Province, Afghanistan (U.S. Army/Justin A. Moeller)

land domain or the air domain or the space domain or the cyber domain or the sea domain. We cannot get focused on individual domain warfare. We have to stay integrated because every one of those domains intersects at one time or another, and it's crucial to have the ability to operate jointly when those domains intersect. We have to stay focused on that idea, but I am a bit worried that we're headed away from that. We have to remind ourselves that we have to operate together. For the Army, the intersection of the land, sea, air, and cyber domains is critical. An integrative approach to these domains, to include the human domain, proves a strength that no one else has. If we do not take an integrative approach, we are going to lose synergy. One of the real advantages that we have is our ability to do that—and we have to make sure we stay focused on that.

JFQ: *What has the experience of being Chief of Staff meant to you, and what will you tell your eventual successor about the job?*

General Odierno: Being the Chief of Staff of the Army is the most humbling experience I've ever had. I have the opportunity to help shape and ensure that this institution keeps moving forward.

We have incredible Soldiers, and I have the opportunity to see them and what they do every single day. As we awarded the Medal of Honor to Staff Sergeant [Ryan] Pitts only yesterday, I was reminded of not only the incredible sacrifice, but also the capability and the trust that these young men and women have in the Army. It's my responsibility to ensure that we continue to build an Army that comes forward at these levels. The lesson I learned is that we represent many different people; we represent our Soldiers in the Active and Reserve components, as well as the National Guard. We also represent our civilians, and it's incumbent on the Chief of Staff of the Army to ensure that the Army continues to prepare itself for the future while meeting current operational commitments. The most important job that the Chief has is to maintain continuity, and we have to make sure that we move forward in a consistent manner. Understanding that the next Chief will have to make some adjustments is a given, but we must stay focused on where we want to take this Army in the future. JFQ

Halvorsen loader pulls away from C-130J Super Hercules at Bagram Air Field, Afghanistan, where Airmen from aerial port and airlift squadrons support operations 24/7 at DOD's busiest single runway airfield (U.S. Air Force/Brian Wagner)



Theater Airlift Modernization

Options for Closing the Gap

By Robert C. Owen

America's renewed strategic emphasis on state-on-state conflict highlights significant gaps in the country's theater airlift capabilities, particularly in the Asia-Pacific region. Quantitatively, there likely will not be enough airlift capacity available to cover major conflict requirements. Qualitatively, the current program-of-record (POR) airlift fleet (what

the Nation has and what it expects to acquire) presents serious shortfalls in the ability to maneuver land forces on the scale, to the destinations, or in the timeframes desired by Army planners. Air commanders also have reason for concern since the core aircraft of the theater fleet, the C-17 and C-130, pose capacity and operational risks in their abilities to support high-volume combat operations at forward bases when threatened or damaged by attack.

Given these gaps between capabilities and requirements, this article considers two questions. First, it begins by asking

whether the POR airlift fleet will be adequate to the demands likely to be placed on it. The discussion then turns to the question of whether affordable opportunities exist to mitigate the gaps identified.

Requirements

Many organizations articulate versions of airlift requirements based on subjective guesses about future scenarios. Moreover, the details of the more authoritative Department of Defense (DOD) studies are classified. Therefore, this article asserts only that the steady reduction of airlift planning goals over

Dr. Robert C. Owen is a Professor in the Department of Aeronautical Science at Embry-Riddle Aeronautical University.



Thirty-sixth Airlift Squadron co-pilot flies C-130 Hercules during training mission as part of Readiness Week at Yokota Air Base, Japan, providing rapid tactical airlift support throughout Pacific theater (U.S. Air Force/Raymond Geoffroy)

the past four decades makes shortages practically certain. In 1981, for example, defense planners accepted a fleet capacity of 66 million ton/miles per day (MTMD) as a “fiscally responsible” target, even though their planning scenarios required as much as 124 MTMD.¹ Ten years later, DOD reduced its airlift capacity to 54.5 MTMD, which conveniently matched the force structure actually on hand at the time.² This number raised high-level concerns over the methodology of the study and the adequacy of its findings.³ Most recently, the DOD *Mobility Capabilities and Requirements Study 2016* tacitly lowered the planning baseline to 30.7 MTMD and declared that the C-130 fleet was larger than needed.⁴ These findings and the methodologies that produced them drew immediate criticism from the Gov-

ernment Accountability Office.⁵ Thus, if baseline airlift studies have a theme, it is that their force structure goals reflect budgetary concerns as much as they do actual requirements.

As in the case of quantitative assessments of airlift shortfalls, qualitative assessments must be parsed from a collection of formal requirements documents, strategies, and Service visions. At the highest level, President Barack Obama’s *Sustaining U.S. Global Leadership: Priorities for 21st Century Defense* calls for the “ability to project power in areas in which our access and freedom to operate are challenged.”⁶ The DOD *Joint Operational Access Concept* expands on this guideline, calling for forces capable of “deploying and operating on multiple . . . lines of operations,” “maneuver[ing] directly against key operational objectives

from strategic distance,” and supporting “forces that may be in multiple locations with multiple objectives.”⁷ Joint forcible entry operations doctrine calls for forces to “seize and hold lodgments against armed opposition . . . [making] the continuous landing of troops and materiel possible and . . . [gaining] maneuver space for subsequent operations.”⁸ Thus, the weight of defense policy implies a need for airlift forces able to support air and land combat operations at almost any location and in the face of substantive threats.

The mounted vertical maneuver (MVM) vision further articulates the Army’s maximal airlift requirements. MVM has passed through several conceptual stages since the mid-1990s, but at its heart calls for “the maneuver and *vertical* insertion of *medium weight armored forces* into areas in close proximity to their

battlefield objectives without the need for fixed airports, airfields, or prepared airheads.⁹ To make the MVM vision practical, proponents call for development of a large vertical takeoff and landing (VTOL) aircraft. As the MVM vision has matured, the expected payloads of these joint heavy lift (JHL) aircraft have increased from 26- to 30-ton *Stryker* or Future Combat System vehicles to Bradley fighting vehicles up to 36 or more tons in weight. MVM visionaries expect that these aircraft will enable a revolutionary increase in the combat power and survivability of air maneuvered forces.¹⁰

The Air Force has not developed a conceptual equivalent to mounted vertical maneuver, but it probably should. In the past, most Air Force airlift support concepts have presumed that transport aircraft would operate under the umbrella of American air dominance to reach the main bases used by the combat units they supported. However, deeper thought about the possibility of major conflicts in the Asia-Pacific suggests that the United States may not always enjoy unbroken air dominance and invulnerable bases in future conflicts and that potential foes may plan to target American airlift forces at the beginning of any future conflicts.¹¹ There is a need, therefore, to articulate expeditionary strategies that presume that the Service's airlift forces may be called on to operate at bases that are damaged or under current or imminent attack.

Land maneuver and air operations at degraded airfields will demand high throughputs from airlift forces at austere or off-runway locations. Even in support of JHL-based operations, fixed-wing transports will be needed to move large quantities of vehicles and supplies into MVM bases or operating locations established deep in contested territories or otherwise beyond land lines of communication. Given the vulnerabilities of transport aircraft at forward bases, local commanders may want to push their operations out to unpaved areas of main bases or even to remote fields. Such relocations would reduce the likelihood that cargo aircraft could be destroyed during their predictable ground movements or at their parking areas. They also would

minimize the chance of collateral losses of personnel and nearby aircraft in the event of detonations of aircraft loaded with tons of munitions or other hazardous cargo.

The Air Force POR Fleet

In terms of gross capacity, the program-of-record fleet is in good shape. The Air Force fields about 213 C-17s and 428 C-130s, which comprise its core theater airlift capabilities. The Air Mobility Command (AMC) manages all of these aircraft logistically, but they are assigned to AMC, geographic combatant commands, and the Air Reserve Components (the Air Force Reserve and Air National Guard). Production of C-17s has ended, but a program to replace older C-130s with C-130Js is under way. Conflict tested for the past 20 years, this fleet remains the only force capable of moving brigades, divisions, wings, air forces, and their sustainment anywhere on the planet. Additionally, the Army and Marines field hundreds of CH-47 and CH-53 battlefield airlift aircraft, while the Navy and Marines also conduct airlift operations with about 50 C-130s of their own.

Importantly, the capacity of the Air Force's theater transport fleet diminishes quickly when it is called on to operate in austere or degraded airfield environments. Under sea level atmospheric conditions and depending on their loaded weights, the maximum effort takeoff distances of the C-130 range from 1,700 to 3,200 feet.¹² Under similar conditions, C-17s need between 3,000 and 7,000 feet.¹³ Presuming that runways of suitable length are available, the limiting operational factor becomes the load-bearing strength of their surfaces. A C-17, for example, will rut, gouge, and render unusable runways rated at a California bearing ratio of 10 (graded soil and gravel) in just 30 passes (30 landings and 30 takeoffs). Lighter C-130s could make 1,500 passes on the same surface.¹⁴ Thus, in situations where airstrips or the undamaged sections of main runways are short, the most capacious aircraft in the fleet will not be able to get in, while the smaller aircraft could get in but would be

limited in their throughput. The impact of runway strength becomes clearer when one considers that a C-17 flying an unrefueled 2,800 nautical mile (nm) round trip from the main U.S. airbase on Guam in support of Army operations on the Philippine island of Luzon could carry up to 60 tons of cargo, while a C-130 would deliver only 6 tons. Furthermore, C-130s could not deliver any of the armored combat vehicles or other outsize items required by most maneuver brigades.¹⁵

The limitations of the C-17/C-130 team trouble proponents of MVM. Illustrating the impact of these limitations, a 2008 Army study determined that a C-5/C-17 fleet would in most cases be obliged to set down MVM units 50 kilometers (km) or more from their objectives or points of need/effect (PON/E).¹⁶ C-130s, once brought into such a distant theater, could ease the access problem, but they would be incapable of delivering much of the equipment required. These limitations, therefore, render the MVM vision moot.

In summary, the POR airlift fleet presents theater warfighters with three capabilities/requirements gaps. Historical experience suggests that there always will be shortfalls in capacity versus requirements. Also, the C-17/C-130 combination is capable but restricted in its ability to deliver high tonnages and mechanized ground units into degraded or austere airfield environments. Last, the fleet on the books has little to no capability to satisfy the Army's MVM vision of conducting air assaults with medium mechanized units near or at their PON/Es. While this last gap does not relate to a concept endorsed for funding by DOD, it still has relevance to airlift planners since the Army, historically the biggest user of airlift, favors it.

Options for Closing the Gaps

In broad terms, there are three approaches to closing these theater airlift gaps: buy more of the same aircraft, buy off-the-shelf aircraft offering desired capabilities, or develop completely new aircraft. Each of these approaches offers its own mix of cost and operational features as capability

gap fillers. Consequently, this brief analysis focuses on three criteria for assessing these gap-filler approaches: the likelihood that a given option actually will close some or all the gaps, lifecycle costs, and general impact or opportunity costs on other mission areas.

Numerous studies have been done on at least some elements of this issue. In 2007, DOD issued an initial capabilities document (ICD) for a JHL aircraft with either super-short takeoff and landing (SSTOL) or VTOL capabilities. By SSTOL, the ICD meant an aircraft able to take off from an unprepared surface and climb over a 50-foot obstacle in 1,000 feet or less. The concept aircraft also was to be capable of carrying a 28-ton medium armored vehicle over a 250 nm mission radius to within either 25–50 km of desirable points of need (if SSTOL capable) or less than 25 km (if a VTOL design).¹⁷ Sensitive to its other airlift support obligations, the Air Force in 2010 eased the takeoff- obstacle-clearance distance requirement to 1,500 feet to gain some trade space to increase the notional aircraft’s mission radius to 1,000 nm and thereby improve its ability “to satisfy a wide variety of airlift mission requirements.”¹⁸ More recently, the U.S. Transportation Command and Air Mobility Command conducted studies focused on satisfying mounted vertical maneuver needs.¹⁹

The Air Mobility Command’s Joint Future Theater Lift (JFTL) Technology

Study, released in February 2013, addressed gaps in the command’s ability to operate into austere landing areas, support the maneuver of medium-weight armored vehicles, and transport medium-weight forces and their logistics over strategic and operational distances directly to their PON/E.²⁰ The technology options it studied included the C-17s, C-130s, and CH-47s of the “baseline fleet,” a conventional takeoff and landing (CTOL) turboprop-powered aircraft, a CTOL turbofan-powered aircraft, a short takeoff and landing (STOL)-capable turboprop, a STOL turbofan-powered aircraft of planform design, a VTOL tiltrotor, and a VTOL hybrid airship. In the end, AMC concluded that a new heavy-lift tiltrotor would be the “most operationally effective of all the options.” New design STOL turboprops, planform turbofans, and hybrid airships also offered useful, but not maximal, operational values in the scenarios examined.²¹ Given the characteristics of those scenarios, the JFTL found the turboprop CTOL option as “high risk.”²²

The JFTL also estimated the 30-year lifecycle costs of a force of each aircraft capable of carrying a medium-armored brigade over strategic distances into a theater, carrying a “primarily medium weight” brigade task force in a forcible entry operation, moving a medium-weight battalion within a theater, and supporting the logistics of these operations (see table).

Assessing the Options

We turn now to analysis of options for closing the theater airlift gap. Option 1—buying more of the same aircraft already in the POR fleet—likely will be unattractive to theater and Service planners. Most important, buying additional C-17s and C-130s will not close any of the three airlift gaps. They might make a contribution to the shortfall in gross capacity, but they would have little impact on the Air Force’s ability to deliver high cargo volumes and outsize vehicles into damaged and austere airfields, and they would leave MVM unsupported. In terms of opportunity costs, acquisition of such aircraft could make airlift capacity available to otherwise unserved users, but its \$62.1 billion price tag also would siphon funds away from other programs. In addition, the Air Force has stated that it has plenty of C-17s and C-130s, so making a politically and financially compelling case for more would be difficult.²³

Option 2—acquiring an off-the-shelf aircraft—is a more complex proposition than expanding the existing fleet. The only mid-sized airlifter on the market that could address the Air Force’s airlift gaps would be the Airbus A400M, an aircraft similar to the turboprop CTOL aircraft discussed in the JFTL. With a maximum payload of 40.5 tons and the ability to carry a Bradley fighting vehicle for 2,400 nm, this aircraft could contribute to gross long-range lift capacity. Moreover, the A400M has airfield length and strength requirements close to those of the C-130, giving it significant ability to sustain high throughput into airfields not suitable for the C-17.²⁴ The A400M also could deliver medium-weight armored units closer to their PON/E than could a C-5/C-17 fleet. Thus, if the Army and Air Force remain unable to attain DOD authorization and funding to pursue a VTOL option, an off-the-shelf turboprop CTOL could be an affordable second approach to at least improving joint aerial maneuver capabilities.

It is worth noting here that the lifecycle costs of the medium CTOL option likely would be lower than those estimated in the JFTL. Those numbers

Table. JFTL Technology Study Lifecycle Cost Estimates

Alternative	Number of Aircraft	Lifecycle Cost of Budget Year 2012 (in \$ billions)
Baseline	63 (C-130) 36 (C-17) 20 (CH-47)	62.1
CTOL Turboprop	49	36.4
CTOL Turbofan	84	111.1
STOL Turboprop	93	110.7
STOL Turbofan	93	120.8
VTOL Tiltrotor	98	128.4
VTOL Hybrid Airship	92	84.3

Source: Air Mobility Command, *Joint Future Theater Lift: Technology Study Final Report*, February 20, 2013, 125.

Key: CTOL = conventional takeoff and landing; STOL = short takeoff and landing; VTOL = vertical takeoff and landing.



Air Force C17 Globemaster takes off from old Israeli airstrip in Sinai Peninsula of Egypt to provide airlift support for Soldiers from Aviation Company, 1st Support Battalion, Task Force Sinai (U.S. Army/Thomas Duval)

were based on an unaugmented fleet of 49 CTOLs needed to meet the gross lift requirements of its chosen scenarios.²⁵ But in reality, the Air Force likely would buy only enough new CTOL aircraft to augment the existing C-130 fleet's ability to deploy and sustain forces into airfields too short or soft for C-17s. For example, C-130s would be capable of moving the personnel, supplies, and about half of the 300 or so vehicles possessed by a mechanized infantry battalion. Consequently, the Air Force would need to field only enough new medium CTOL aircraft, such as the A400M, to move the other, heavier vehicles in the battalion. More practically, however, the Air Force might want to acquire enough medium CTOLs to make such moves alone, since they would greatly increase movement velocities and the flow of sustainment in forward airfields or at degraded air bases.

This brings the discussion to the final option for addressing theater airlift gaps—developing and acquiring a completely new aircraft. If DOD pursued this costly option, the only reasonable choice would be the VTOL tiltrotor. The

other options discussed in the JFTL are unrealistic, and their merits in relation to the theoretical capabilities of a new tiltrotor and the real capabilities of, say, the A400M would be too marginal to justify their costs. Given its inherent performance limitations, the tiltrotor would make little or no contribution to the general airlift shortfall over strategic distances. Over distances of a few hundred miles, VTOL tiltrotors could increase the flow of forces into austere airfields because more of them could land in a given area. But their ability to sustain high throughputs at those locations, in comparison to what fixed-wing transports could do, bears close examination. Historically, rotary-wing aircraft have not been able to generate the flight hours over time or the ton-mile productivity of fixed-wing transports. Of course, the attraction of a heavy-lift VTOL would be its maximal contribution to the aspirations of MVM advocates.

The assertion that tiltrotors would be inherently unable to generate fixed-wing-like throughputs bears some expansion. Suffice it here to offer a simple

comparison of the current MV-22 tiltrotor and the C-130J fixed-wing transports. An MV-22, with total engine power of 12,300 horsepower, cruising at 240 knots with its maximum 8-ton payload, produces 0.12 ton-miles of useful lift per hour *per engine horsepower available*.²⁶ A C-130J, with total power of 19,364 horsepower, cruising at 350 knots with a less-than-maximum payload of 20 tons, will produce 0.36 ton-miles per available horsepower.²⁷ This comparison is inexact, but in its magnitude, it offers compelling and relevant insights into the operational offsets of VTOL capabilities.

Recommendations

In its examination of theater airlift gaps and mitigation options, this article has highlighted two broad conclusions. First, gaps do exist in general long-range airlift capacity, the C-17/C-130 team's ability to achieve high throughputs into austere landing areas, and the POR fleet's ability to satisfy the maximal requirements of the MVM vision. Second, there are numerous mitigation options for these shortfalls. But as likely

as the gross lift shortfalls will be, they are unlikely to spur additional spending on airlift forces. The shortfall in austere airfield capabilities, in contrast, should trouble combatant commanders and fortunately can be addressed through modest investments in existing aircraft designs. Addressing the MVM requirement, if it ever gains DOD funding approval, will be both an expensive undertaking and one with significant implications for other mission areas.

The first step toward mitigating these theater airlift gaps will be to settle the MVM issue, at least for the moment. Because MVM is the long pole in theater airlift planning and has dominated recent studies, combatant commanders need to determine how badly they want it. The estimated cost of \$128 billion or more represents a large commitment, particularly when the JFTL indicates that MVM will shorten the closure time of a maneuvering battalion by only 21 hours in comparison to current capabilities of the POR fleet.²⁸ Perhaps the time has come for the Army to accept less “precise” maneuver for its medium forces or to develop an MVM concept based on lighter units that can be lifted by a modestly augmented POR fleet and helicopters.

The second step should be to develop an affordable strategy for enhancing the ability of combatant commands to deploy ground forces to austere locations and support combat air operations from degraded airfields. This is an immediate requirement affecting land force mobility and air combat capabilities. If an appropriate fixed-wing aircraft is chosen to mitigate this requirement, acquiring it in appropriate numbers probably will not break the bank. Moreover, since such new planes will be augmenting the existing fleet, their costs can be offset by reducing buys or deferring the service-life extensions of other transports. The imperative, in any case, is to begin taking concrete steps to understand and address theater airlift shortfalls in the very near future, rather than let them worsen until they unhinge future combat operations. JFQ

Notes

¹ Duncan McNabb, “Point Paper, Subject: Congressionally Mandated Mobility Study (CMMS),” Headquarters MAC/XPPB (Scott Air Force Base, IL: Air Mobility Command History Office, February 12, 1986); John Shea, interview by Robert C. Owen, August 8, 1990, tape 3A, index 409.

² Office of the Secretary of Defense (OSD), “Executive Summary,” *Mobility Requirements Study 2005 (MRS)* (Washington, DC: OSD, December 2000), 4.

³ “GAO: Military 30% Short of Airlift Requirement for War,” *Defense Week*, December 18, 2000, 1; “Ryan: ‘We Will Never Have Enough Lift’ for Two Regional Wars,” *Aerospace Daily*, June 22, 2000, 1.

⁴ Carl Lude and Jean Mahan, “Executive Summary,” *Mobility Capabilities and Requirements Study 2016* (Washington, DC: OSD, 2010), 1–8; John A. Tirpak, “The Double Life of Air Mobility,” *Air Force Magazine* (July 2010), 31.

⁵ U.S. Government Accountability Office (GAO), *Defense Transportation: Additional Information is Needed for DOD’s Mobility Capabilities and Requirements Study 2016 to Fully Address All of Its Study Objectives*, GAO Report 11-82R (Washington, DC: GAO, December 8, 2010), 3–12 and throughout; GAO, *Mobility Capabilities: DOD’s Mobility Study Limitations and Newly Issued Strategic Guidance Raise Questions about Air Mobility Requirements*, GAO Report 12–510T (Washington, DC: GAO, March 7, 2012), 9.

⁶ *Sustaining U.S. Global Leadership: Priorities for 21st Century Defense* (Washington, DC: Department of Defense, January 2012), 4.

⁷ *Joint Operational Access Concept (JOAC), Version 1.0* (Washington, DC: The Joint Staff, January 17, 2012), ii, 32.

⁸ Joint Publication 3-18, *Joint Forcible Entry Operations* (Washington, DC: The Joint Staff, November 27, 2012), I-1.

⁹ U.S. Army and U.S. Marine Corps, *Gaining and Maintaining Access: An Army-Marine Corps Concept*, March 2012, 10. Emphasis added.

¹⁰ Brigadier General Robin P. Swan and Lieutenant Colonel Scott R. McMichael, “Mounted Vertical Maneuver: A Giant Leap Forward in Maneuver and Sustainment,” *Army* (January–February 2007), 52–62. The Bradley concept is based on discussions by the author and Army proponents of the MVM concept.

¹¹ OSD, *Military Power of the People’s Republic of China 2007*, Annual Report to Congress (Washington, DC: Department of Defense, 2008), 17; and Roger Cliff et al., *Entering the Dragon’s Lair: Chinese Antiaccess Strategies and Their Implications for the United States* (Santa Monica, CA: RAND, 2007), 60–62.

¹² Lockheed Martin Corporation, “C-130J Super Hercules: Whatever the Situation, We’ll

Be There,” 27–28, available at <http://cc-130j.ca/wp-content/pdfs/Spec_Book.pdf>.

¹³ Boeing Corporation, “Background: C-17 Globemaster III,” February 2014.

¹⁴ The California bearing ratio (CBR) measures the resistance of unpaved surfaces to compression and rutting. A CBR of 100 equates to a surface of crushed California limestone, almost equivalent to pavement in its strength. A CBR of 10 equates to one of wet sand and soil, while anything less delineates wet tilled soil or plain mud. For discussions of C-17 and C-130 effects on soft fields, see Air Force Civil Engineer Support Agency, “Engineering Technical Letter 97-9; Criteria and Guidance for C-17 Contingency and Training Operations on Semi-Prepared Airfields,” November 25, 1997, 10; and Lockheed Martin, “C-130J Super Hercules.”

¹⁵ Lockheed Martin, “C-130J Super Hercules,” 29.

¹⁶ U.S. Army Concepts Integration Command, “Global Deployment Assessment: Examining Deployment Considerations within the Arc of Instability,” PowerPoint briefing, July 7, 2008, slides 15–24.

¹⁷ Joint Requirements Oversight Council, “Initial Capabilities Document for Joint Heavy Lift (JHL),” October 12, 2007, 8, 22.

¹⁸ Air Force, Chief of Staff, “Initial Capabilities Document for Joint Future Theater Lift (JFTL),” October 27, 2009, 5, 6, 9.

¹⁹ U.S. Transportation Command (USTRANSCOM), *Future Deployment and Distribution Assessment: Mobility Lift Platforms, Final Report, Volume 1* (Scott Air Force Base, IL: USTRANSCOM, 2011); and Air Mobility Command, *Joint Future Theater Lift: Technology Study Final Report*, February 20, 2013 (hereafter “AMC JFTL”).

²⁰ AMC JFTL, 17–18, 31.

²¹ *Ibid.*, 10–14, 125–126.

²² *Ibid.*, 77–86.

²³ Lude and Mahan, 6; and David Ignatius, “No clipping these wings,” *The Washington Post*, July 5, 2013, available at <http://articles.washingtonpost.com/2013-07-05/opinions/40390066_1_planes-c-130s-cuts>.

²⁴ EADS North America, “Joint Future Theater Lift (JFTL) Technology Study Capability RFI (C-RFI) Response,” December 22, 2012, 44.

²⁵ AMC JFTL, 125.

²⁶ All MV-22 data in this paragraph are extracted from U.S. Marine Corps, *V-22 Osprey Guidebook 2011–2012* (Washington, DC: Department of the Navy, 2011), 5, 44, 59.

²⁷ All C-130J data in this paragraph are extracted from Lockheed Martin, “C-130J Super Hercules.”

²⁸ AMC JFTL, 125.



New train track 75 kilometers long between Afghanistan border and Mazar-e-Sharif provides hundreds of jobs to local Afghans and means of importing and exporting goods (DOD/Michael Reinsch)

The Afghanistan National Railway

A Plan of Opportunity

By Lawrence J. Pleis, Richard Lliteras, David A. Wood, Matthew D. Bain, and Steven J. Hendrickson

Steam railroading is important not because it represents some nostalgic past that, in truth, never was. Steam railroading is important because it was a human tool that radically transformed a continent, affecting everyone.

—WILLIAM L. (BILL) WITHUHN, CURATOR EMERITUS,
Smithsonian Institution

Colonel Lawrence J. Pleis, USMC (Ret.), is Chief of the Strategy and Policy Office (SPO) in the Directorate of Logistics and Engineering at U.S. Central Command (USCENTCOM). Colonel Richard Lliteras, USA (Ret.), is Deputy Chief of SPO. Colonel David A. Wood, USA (Ret.), is a Senior Associate with Booz Allen Hamilton. Major Matthew D. Bain, USMC, is a Logistics Strategist in the Directorate of Logistics and Engineering at USCENTCOM. Mr. Steven J. Hendrickson is an Associate with Booz Allen Hamilton.

In support of the State Department's "New Silk Road" initiative, U.S. Central Command (USCENTCOM) formed a planning team of subject matter experts spanning the Department of Defense (DOD), the interagency community, academia, and the U.S. railroad industry to provide recommendations that advance the development of a national railway system for the Government of the Islamic Republic of Afghanistan (GIROA). The Afghanistan National Railway Plan (ANRP) was provided to the Afghanistan Railway Authority (ARA) in August 2013.

The ANRP was developed on the basis of Afghanistan's urgent need for a national transportation system as a precursor of economic development and political stability. Expansion of the existing 75-kilometer rail line could ultimately allow Afghanistan to export minerals and agricultural products, significantly enhance its position as a regional trading partner, improve domestic commerce, and link products, consumers, and markets across Eurasia and beyond.

Assessing the economic viability and technical and financial feasibility of a national railway system for Afghanistan, as well as the regional connectivity imperatives, to develop recommendations for large capital-investment infrastructure projects was a nontraditional assignment for USCENTCOM. The railroad expertise formerly resident in the U.S. Army Reserve has been significantly reduced to tactical-level repair, operations, and advisory capability. Notwithstanding these planning challenges, USCENTCOM partnered closely with the Task Force for Business and Stability Operations, U.S. Transportation Command's Joint Distribution Process Analysis Center, the Surface Deployment and Distribution Command's Afghanistan Railway Assessment Team, the Center for Joint and Strategic Logistics at National Defense University (NDU), and United States Forces-Afghanistan to collectively plan, model, assess, and validate the recommendations in the ANRP. Invaluable to DOD planners was the voluntary technical assistance provided over the 18-month planning process by the Department of Transportation, Federal Railroad Administration, Department of State, and Treasury Department, as well as the largely pro bono support from rail, mining industry, and cultural experts from Columbia University, George Mason University, and Michigan State University. While these organizations formed the core planning team, several other stakeholders, including other DOD organizations, were critical to reviewing and refining the ANRP.

The planning effort culminated in February 2013 at a stakeholder review workshop, co-hosted by the Near East South Asia Center for Strategic Studies at NDU and USCENTCOM, when 56 representatives from 24 organizations conducted a detailed assessment of the draft plan. Highlighting the workshop was the participation of the Afghanistan Railway Authority, established under the Afghan government's Ministry of Public Works in September 2012, and the Ministry of Mines. Guidance, discussion, and buy-in from these key Afghan representatives were critical to reshaping

the preliminary ANRP into an actionable plan reflecting the requirements and priorities most relevant for Afghanistan.

Why Rail?

Afghanistan is blessed with billions of dollars' worth of accessible mineral wealth (primarily copper and iron ore) but does not currently have a railway capable of transporting high volumes of these lucrative exports. Similarly, the country relies on relatively inefficient trucking routes for vital imports such as wheat, cement, fertilizer, consumer goods, and petroleum. The absence of a railway system dampens trade and inhibits the landlocked nation's economic growth and trade with its neighbors and global markets. A railway could facilitate commercial exchange and promote stability, serving as a regional hub for Central and South Asia. The potential for significant revenue enabled by rail could aid in reducing poverty and improving the standard of living of the Afghan people. A railway is also critical to the country's security, with select rail corridors supporting national defense. The potential of these benefits has drawn railway development support from the Central Asia Regional Economic Cooperation (CAREC) program, South Asian Association for Regional Cooperation, and Afghanistan-Pakistan Border Region Prosperity Initiative, which was launched by the G-8.

Regional Support

Regional railway integration has drawn support from Afghanistan's neighbors, including Uzbekistan, Kazakhstan, Turkmenistan, and Tajikistan, and regional trading partners such as India and China. Long reliant on northern routes to the Baltic Sea for access to the global economy, the Central Asian Republics are developing the potential to transport goods through Afghanistan to Indian Ocean ports at lower costs and shorter distances. The economies of Afghanistan and regional partners could also benefit from trade borne by trains traversing Afghanistan since its neighbors Pakistan (26 percent), India (26 percent), and Tajikistan (10 percent)

constitute the biggest export destinations. Rail transport is a key component of the reemerging Silk Road, a comprehensive concept to expand trade, transit, and supply route networks from the Indian Ocean to the Ural Mountains. As Kazakhstan's Foreign Minister Yerzhan Kazykhanov explained in 2012, regional investment in Afghanistan will pay dividends: "We must look beyond 2014 and help Afghans help themselves."

The Business Case

Sustainable growth is the best way for Afghanistan, a largely agrarian country, to reduce dependence on foreign aid. The country is eager to leverage its vast iron ore and copper deposits, mines that could generate a total of \$78 billion in corporate taxes and royalties by 2040. Geological surveys also indicate the country possesses exploitable reserves of valuable elements such as lithium. In Afghanistan, rail and mining development are integrally linked; mining requires rail to transport ore efficiently to market, and rail is reliant on revenue generated by exporting ore. Competitive analysis indicates that current low-cost global producers of iron ore, including Brazil and Australia, are able to extract, rail, and ship to Asian markets for as little as \$39 per metric ton (2012 equivalent). To successfully compete in the global iron ore market, Afghanistan must approach this level of efficiency. Delivering hundreds of millions of metric tons of minerals to market at competitive rates will require expeditious rail routes linking mines with seaports and Standard gauge track able to support heavy-haul loads. The ANRP forecasts 75 percent of the country's estimated rail freight traffic between 2017 and 2040 will be mineral transport. The rest of the traffic will represent shipments of agricultural products, raw materials, and finished goods to and from the country, shipments that will grow as Afghanistan's society modernizes and accumulates wealth.

A Wealth of Minerals

Afghanistan's mineral abundance, widely dispersed throughout the

country, could ultimately exceed \$1 trillion. The country has been known since antiquity for gemstones such as lapis lazuli and emeralds, but the greatest potential for wealth generation consists of bulk quantities of copper and iron ore available close to the Earth's surface. Seven iron and copper mining "areas of interest" would produce the majority of the country's export earnings: Haji Gak, Syadara, and Zarkashan for iron and Aynak, Balkhab, Dushanbe, Kundulan, and Zarkashan for copper. According to forecasts, mining operations would yield about 58 million metric tons of ore annually, almost all of it requiring rail transport. Production totals could approach 1.4 billion metric tons between 2017 and 2040. Minerals from Haji Gak, acclaimed as one of the world's largest iron reserves, account for most of the anticipated freight demand for a proposed southern line. Haji Gak's output is expected to be four times that of all the other mining areas combined. Afghanistan offers many advantages as a source for minerals to supply the teeming markets of fast-developing South Asia.

Emerging Rail Routes

Economic feasibility, including the need to negotiate Afghanistan's challenging terrain, dictates the location of proposed rail routes. The national railway concept envisions a southern mineral freight line of Standard gauge that would approach Indian Ocean ports in Iran and Pakistan. The prohibitive cost of traversing the Hindu Kush, the mountainous interior of Afghanistan, suggests the southern rail line would initially function largely independently of the northern line. The northern commercial freight line consisting of the wider Russian gauge would link to the existing 75-kilometer line in the city of Mazar-e-Sharif and join a network serving the Central Asian states. Major Afghanistan commercial centers such as Kabul, Kandahar, Herat, and Mazar-e-Sharif will serve as hubs of this transportation network. It is necessary to note that medium-term CAREC program priority projects through 2020 include

supporting Afghan railway goals for a route from Tajikistan to Turkmenistan through Afghanistan:

- Turkmenistan: construction of railway line Atamurat–Imamnazar–Aqina (estimated cost of construction \$200 million; implementation period of the project 2012–2015)
- Afghanistan: construction of railway line Aqina–Andkhoy–Sheberghan–Naibabad–Kholm–Kunduz–Sherkhan Bandar (estimated cost of construction \$525 million; implementation period of the project 2012–2015)
- Tajikistan: construction of railway line Kolkhozabad–Dusti–Panji Poyon–Afghanistan border (estimated cost of construction \$90 million; implementation period of the project 2012–2015).

These projects would link northern Afghanistan rail lines, via Turkmenistan, to the Caspian Sea, which would expand Afghanistan's commercial opportunities to a new part of the world.

The Plan

The ANRP is underpinned by the Commercial Market Feasibility Analysis (business case), Terrain and Freight Rail Corridor Feasibility Analysis (technical and financial feasibility and risk analysis), and Legal and Regulatory Framework (proper governance and facilitation of economic viability). The plan supports the achievement of Afghanistan's strategic priorities, which are to enhance economic growth and economic development, facilitate regional cooperation and development, and better connect the people of Afghanistan. The ANRP supports these strategic priorities by providing analysis and recommendations for four sequential key decisions to effectively expand Afghanistan's existing railway and identifies the critical path for timely and integrated railway development, operation, and sustainment to achieve the best possible, most financially viable national rail system over time.

The key decisions are to finalize the primary and supporting railway purposes, determine the preferred rail system design,

determine the most suitable railway ownership model(s) and management structure, and determine regional connectivity requirements. These four decisions are foundational to ensuring successful railway development and implementation.

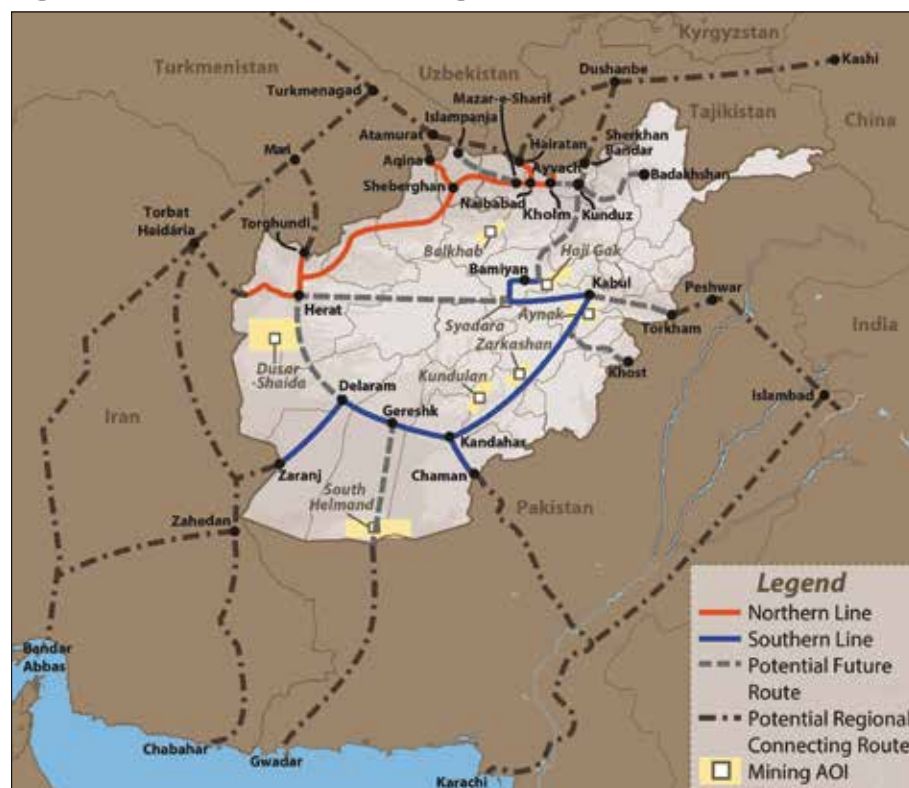
Key Decision 1

Finalize the Primary and Supporting Railway Purposes.

Afghanistan railway development will be driven primarily by transport of iron ore and, to a much lesser degree, by copper cathode, merchandise, and transit traffic transport. Cumulative mineral, merchandise, and transit traffic shows potential for approximately 1.8 billion net metric tons of freight available for railway transport between 2017 and 2040. Mining is expected to generate approximately 76 percent of potential railway freight traffic demand. Merchandise traffic, including mine-driven imports required for mine development and commercial imports (grain, fertilizer, petroleum, cement, machinery, and other equipment), is expected to generate approximately 17 percent and transit traffic, 7 percent.

The greatest potential for wealth generation consists of bulk quantities of copper and iron ore. The best prospects for near-term revenue generation center on the seven mining areas of interest: Haji Gak, Syadara, and Zarkashan for iron and Aynak, Balkhab, Dushanbe, Kundulan, and Zarkashan for copper. Estimated net tonnage of minerals from Afghanistan's mining areas of interest exceeds 58 million metric tons per year, on par with some of the largest freight operations in the world. Output from the Haji Gak iron ore area of interest is estimated to account for 80 percent of all mineral traffic and 60 percent of all freight traffic. To successfully compete in the global iron ore market, Afghanistan will need to approach the level of efficiency achieved by low-cost producers in Australia and Brazil at \$39 per metric ton (2012 equivalent). If ore is not moved competitively to market by utilizing the shortest and most efficient railway route to seaport, the railway will lack the revenue to expand and sustain itself. Enabling regional connectivity and establishing a regional transportation

Figure 1. Recommended ANR Design



- Prioritize and develop the Haji Gak mining area of interest first.

Key Decision 2

Determine the Preferred Rail System Design. Economic feasibility, including the need to negotiate Afghanistan's rugged terrain, inevitably dictates the length and location of proposed railway corridors. The Terrain and Freight Rail Corridor Feasibility Analysis evaluated the technical and financial feasibility of developing a national rail system. Employing a three-phased approach, seven assumption-driven construction and operating scenarios were examined to determine a preferred design. Results of the analysis indicate the cost to build rail lines over steep mountainous terrain, which significantly increases the number of bridges and tunnels, is approximately \$9.3 million per kilometer, compared to \$1.9 million per kilometer for flat and undulating terrain. Therefore, constructing and operating a rail line traversing the Hindu Kush in the immediate future is not cost effective. The recommended railway design consists of two separate, purpose-built rail lines with potential for future expansion to unify the two lines and support emerging economic sectors at some time in the future, as shown in figure 1.

The two lines consist of a southern, mineral freight-focused, Standard gauge line, which primarily supports transport of bulk mineral ore to seaports in Pakistan and/or Iran for onward shipment to global markets at the lowest possible overall (rail and sealift) transit cost; and a northern, commercial freight-focused, Russian gauge line, which expands the existing 75-kilometer line running between Hairatan and Mazar-e-Sharif, connects the Central Asian Republics and Iran via Afghanistan, and supports the recent memorandum of understanding for the establishment of railway transport infrastructure linking Turkmenistan, Afghanistan, and Tajikistan.

The financial metrics and risk score for the recommended national railway design are included in table 1. These financial metrics reflect railway operations

Table 1. Recommended ANR Design: Financial and Risk Metrics

Total Cost	\$42,135.40
Total Revenue	\$68,726.20
Profit	\$26,590.80
Cost Present Value	\$19,533.60
Revenue Present Value	\$18,135.40
Net Present Value†	(\$1,398.20)
Internal Rate of Return	8.7%
Operating Ratio	52.3%
Risk Score‡	Medium (9)

All dollar values based on 2012 US\$ millions for 2017–2040

†Based on 10 percent discount rate

‡Risk score based on scale of 1–20, with 1 being low risk and 20 being extremely high risk

hub that facilitates trade, industry development, and commercial-based traffic, and eventually passenger transit to better connect the Afghan people, are important supporting purposes of expansion of the railway system.

Recommendations to GIROA:

- Finalize the primary and supporting purposes of the national rail system. The primary purpose is to enable self-sustainability and economic independence via mineral-based traffic to provide regional connectivity and serve as a regional transportation hub, with supporting purposes of trade facilitation, industry development, commercial-based traffic, and eventually passenger transit to better connect the Afghan people.
- Support development of mining areas of interest to meet transport demand thresholds needed for profitable railway operations.

exclusively and do not include the positive financial impacts estimated for potential mining operations.

The combined southern and northern rail lines of the recommended national railway design do not achieve a positive net present value (NPV) and 10 percent internal rate of return (IRR), though the calculated operating ratio of 52.3 percent reflects a generally favorable revenue-to-operating cost ratio once rail lines are operational.

To more fully analyze the two primary rail lines comprising the national railway design, the planning team considered both the southern and northern lines as independent railways. The southern mineral freight-focused line generates a positive \$635.6 million NPV, an IRR exceeding 10 percent, and an operating ratio of 53.6 percent. The northern commercial freight-focused line is less economically viable with a negative \$2.3 billion NPV, an IRR less than 10 percent, and an operating ratio of 47.6 percent. Table 2 presents the financial metrics associated with the recommended railway design of southern and northern lines.

Figure 2 reflects the cumulative cost, revenue, and profit projections for the recommended Afghanistan national railway design over the designated railway lifecycle, 2014 to 2040, and the southern and northern line break-even points, where cost is recovered by sufficient revenue generation.

The combination of the southern and northern rail lines is projected to reach the cost/revenue break-even point in 2026. Viewed independently, the southern line is projected to reach its break-even point in 2024, and the northern line is projected to reach this point 9 years later in 2033. The impact of these varying profitability profiles may drive GIRoA to leverage the potential revenue generation of the southern mineral freight-focused railway to offset construction and operations of the less profitable northern railway.

Recommendation to GIRoA: Develop and implement the preferred Afghanistan national railway design, the most financially feasible alternative with an acceptable level of risk. It is further

Figure 2. Recommended ANR Design: Cumulative Cost, Revenue, and Profit Projections

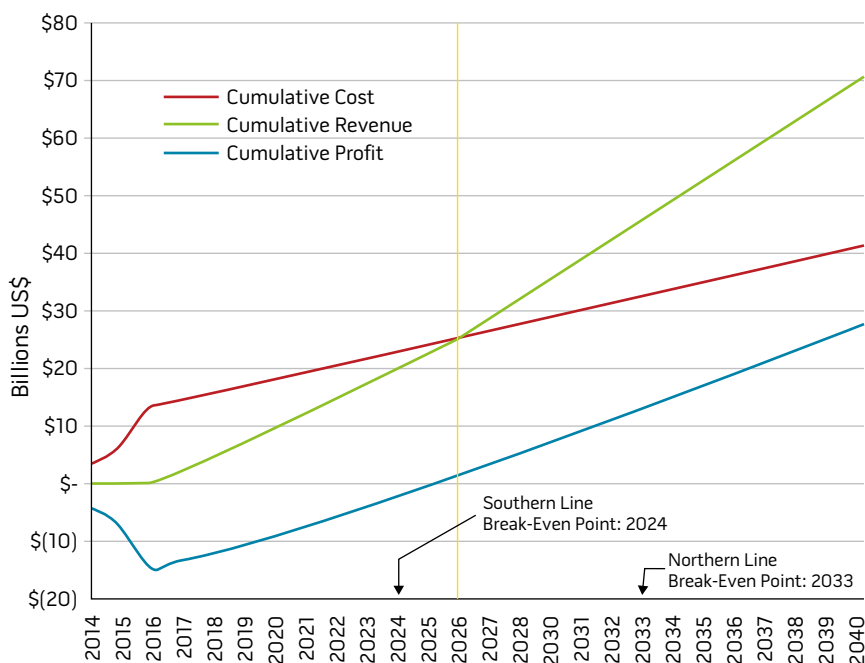


Table 2. Southern and Northern Lines Financial Metric Comparison

Financial Metrics	Southern Line	Northern Line
Total Cost	\$33,988.6	\$8,563.6
Total Revenue	\$56,147.2	\$12,579.0
Profit	\$22,158.6	\$4,015.4
Cost Present Value	\$14,473.1	\$5,349.8
Revenue Present Value	\$15,108.7	\$3,026.7
Net Present Value†	\$635.6	(\$2,323.1)
Internal Rate of Return	10.9%	3.8%
Operating Ratio	53.6%	47.6%

All dollar values based on 2012 US\$ millions for 2017–2040

†Based on 10 percent discount rate

recommended that GIRoA consider increasing the assumed mineral freight rate from \$0.030 to \$0.033 per net ton kilometer to potentially yield a positive NPV and IRR above 10 percent. Additional analysis is required to determine an appropriate mineral revenue rate once a railway operating plan has been developed.

Key Decision 3

Determine the Most Suitable Railway Ownership Model(s) and Management Structure. The ARA is

responsible for developing and instituting policies, laws, and regulations needed for the safe, efficient, and reliable operation of a national railway. Four general railway ownership models and associated management structures were examined to determine the most suitable ownership model and associated management structure for the Afghanistan national railway:

- **Model 1: 100 Percent Public Ownership.** The government owns railway assets, including land and infrastructure, and operates and maintains the

Table 3. Strengths and Weaknesses of Railway Ownership Models

Model	Strengths	Weaknesses
Model 1: 100 Percent Public Ownership	<ul style="list-style-type: none"> Increased government control promotes achievement of GIROA defined-objectives and priorities (for example, enhance economic growth and independence, facilitate regional cooperation and development, and better connect the people of Afghanistan) 	<ul style="list-style-type: none"> Significant capital expenditures require GIROA funding Public model does not facilitate concurrent generation of mining and railway revenue Large government-generated tax revenues are required for Afghanistan railway development and operation Lack of competition has historically fostered inefficient and uncompetitive railway operations
Model 2a: 100 Percent Private Ownership, General Purpose	<ul style="list-style-type: none"> Little or no GIROA investment or subsidies required for development and operations Strong operator incentives exist to operate efficiently, invest, and develop markets and could generate higher revenues from taxes and royalties for GIROA than public model 	<ul style="list-style-type: none"> May require GIROA introduction of railway competition to stimulate competitive transportation rates Insufficient or inappropriate GIROA control and oversight could result in a rail line that does not correspond to Afghanistan railway requirements
Model 2b: 100 Percent Private Ownership, Purpose Built	<ul style="list-style-type: none"> Little or no GIROA investment or subsidies required for development and operations Strong operator incentives exist to operate efficiently, invest, and develop specific markets and could generate higher revenues from taxes and royalties for GIROA than public model 	<ul style="list-style-type: none"> Single purpose operation could constrain future Afghanistan railway expansion options Lack of sufficient GIROA oversight at a prescribed level could result in a rail line that does not meet Afghanistan railway requirements
Model 3: Mixed Public-Private Ownership	<ul style="list-style-type: none"> Provides for railway competition between above rail operators, which may foster more efficient operations Distributes capital risk between the above and below rail operators Allows for integration of future passenger service, particularly with GIROA ownership of track 	<ul style="list-style-type: none"> Requires unique regulation of infrastructure and access rates to satisfy both GIROA and private stakeholders Limited GIROA control over rate setting could cause insufficient return on investment for publicly funded portions of the railway Deferred GIROA support of infrastructure maintenance and planning could lead to unreliable rail operations for private stakeholders
Model 4: Hybrid Ownership	<ul style="list-style-type: none"> Increased flexibility enables railway to be more adaptable to changing political and economic environments Able to provide solutions to unique railway ownership challenges Can support multiple rail purposes Allows for GIROA participation in development and/or operation of specific rail lines, which may help sustain overall railway financial feasibility 	<ul style="list-style-type: none"> Inadequate management of responsibilities for funding, development, and operation, and control of the railway could increase the potential for capital risk, instability, and/or insufficient return on investment

railway with government employees or contractors.

- Model 2: 100 Percent Private Ownership. A private, self-funded corporation owns, operates, and maintains railway assets. Operating decisions are based mainly on market demands and profitability. Two subcategories of this model exist:

- Model 2a: General purpose (mixed freight)
- Model 2b: Purpose-built (bulk mineral freight from mines)

- Model 3: Mixed Public-Private Ownership. The government owns “below rail” assets, including land and infrastructure such as tracks, while a private entity owns, operates, and maintains “above rail” assets and

infrastructure, including locomotives, rolling stock, and control systems.

- Model 4: Hybrid Ownership. The hybrid model contains elements of the above models and accommodates dynamic railway ownership requirements. This model could provide the flexibility to focus government participation on some, but not all, rail lines.

The strengths and weakness of the four railway ownership models are shown in table 3.

Overall, the hybrid model is best suited for GIROA adoption initially. This model best supports implementation of a southern rail line primarily focused on supporting mineral extractive industries and a northern rail line primarily focused on commercial transit traffic and regional trade. Given the flexibility of the hybrid

ownership model, the model could evolve and adapt to dynamic political and economic situations, which may be more suitable for Afghanistan. To support implementation, management, and oversight of a hybrid ownership model, a detailed management structure was also developed for the ARA.

Recommendations to GIROA:

- Adopt a hybrid ownership model as the initial national railway model.
- Refine and implement the initial hybrid ARA management structure. Furthermore, this recommendation includes formally approving a minimum 3-year operating budget.
- Adopt relevant policies, laws, and regulations to support safe, efficient, reliable, and profitable railway operations within Afghanistan.

Key Decision 4

Determine Regional Connectivity Requirements. A key driver of railway profitability is the avoidance of costly transloading operations due to track gauge changes. Because Afghanistan is surrounded by countries whose rail-ways have three different track gauges, regional rail connectivity is a major challenge to operational efficiency. Potential Afghanistan rail freight would be required to traverse multiple Central and South Asian countries with differing track gauges including Standard (1435 millimeters [mm]), Russian (1520 mm), and Indian Broad (1676 mm). Details are shown in figure 3.

The gauge of new rail lines is best determined by the gauge of its connecting lines. Since Iran uses Standard gauge and the Central Asian Republics use Russian gauge, selection of the preferred rail system design establishes a separated system of a southern, mineral freight-focused Standard gauge line linking to Iran and Pakistan, and a northern, commercial freight-focused, Russian gauge line linking to Iran, Turkmenistan, Uzbekistan, and Tajikistan.

Iran is a primary destination for mineral exports traversing the southern line, offering the most expeditious routing to port, with Pakistan providing an alternate route to mitigate the risk of only one outlet to port. Implementation of Standard gauge for the southern line mitigates the requirement for transloading operations for freight en route to Iran. To address potential requirements to export ore through Pakistan, implementation of a Standard gauge railway within Pakistan or a dual gauge railway should be considered.

Northern line operations are commercial, freight-focused, and depend heavily on trade with the Central Asian Republics, all of which operate Russian gauge lines. Implementation of Russian gauge leverages the existing rail line from Hairatan to Mazar-e-Sharif and minimizes the requirement for transloading operations and facilities, with the possible exception of Herat. A transload facility near Herat could support the transport of commercial goods through Afghanistan

Figure 3. Regional Track Gauges



Table 4. Evaluation of Risk Factors for National Rail System

Risk Category	Ranking (1: Greatest Impact to Railway Success)	Scaled Risk Category Score
Investment and Funding	1	Medium
Political (Internal to Afghanistan)	2	Medium
Security	3	Medium
Operations	4	Medium
Development	5	Medium
Political (External to Afghanistan)	6	Medium
Legal and Regulatory	7	Medium
Overall Risk Score: Medium (9)		
Low 1–5	High 11–15	Medium 6–10
		Extremely High 16–20

to Iran, assuming Iran adopts Standard gauge to connect with Herat.

Recommendations to GIROA:

- Implement Standard gauge for the southern rail line.
- Implement Russian gauge for the northern rail line.

Risk Assessment

Though there is substantial support for expansion of Afghanistan's current,

single rail line, there are challenges in developing and operating a national rail system. The planning team evaluated risk associated with the preferred design scenario through a broad assessment that weighed 37 risk factors organized in 7 risk categories to account for these challenges and the assumptions used for planning (see table 4).

1. Investment and Funding. As GIROA does not have the required resources to finance the construction of



New track from Uzbekistan border to just beyond Mazar-e-Sharif lets Afghan traders import and export goods (DOD/Michael Reinsch)

the national railway on its own, sufficient financing is essential from both the international financial community and private sector. To encourage investment by financiers, GIRA must ensure that capital and operating cost estimates for projects are accurate; the appropriate laws, policies, and regulations are in place; and an overall project manager is appointed to plan and manage initial development. Land grants could also serve as a means to finance national railway construction.

2. Political (Internal to Afghanistan). GIRA instability following the drawdown of North Atlantic Treaty Organization forces in 2014 could halt the development of railway and mining operations. National, regional, and local governments are encouraged to work collectively to ensure a sufficient level of governance during and after foreign troop withdrawal.

3. Security. Insufficient security measures could lead to theft, vandalism, and/or terrorist attacks on railway

and mining property, infrastructure, equipment, and personnel, resulting in schedule delays and loss of railway and mining revenues. GIRA should work with regional and local governments and tribes to develop and implement a security plan that encourages regional and local governments and tribes to participate in, and support, security operations. Local employment for security forces, land grants, and revenue sharing could be leveraged as incentives.

4. Operations. Due to a lack of experience, industry experts must be recruited for the startup of operations and to train local labor. GIRA should also consider sending some people to train on neighboring railways and explore opportunities in railway management education offered at the university level. Afghanistan rail operations must be coordinated closely with neighboring countries to ensure efficient interchange of operations and traffic. Safety and operating standards for equipment, track,

and personnel must be developed and promulgated to ensure safe, reliable, and efficient operations.

5. Development. Failure to achieve sufficient project management, acquire and retain technical staff, receive building permits, maintain sufficient water and energy delivery to mining sites, and sustain an adequate labor force could jeopardize expansion of Afghanistan's rail system. Professional project management and recruitment of the staff needed for construction and for railway and mining operations must be achieved for these mutually reliant sectors. Land use agreements, potential land grant arrangements, and building permits must be both properly negotiated and legally binding to enable railway construction to proceed. Customs arrangements with neighboring countries must also be expedited to ensure railway construction materials and equipment as well as rolling stock and control systems equipment can be imported in a timely manner.

6. Political (External to Afghanistan). Afghanistan's relations with neighboring countries and their respective railways will have a major impact on the success of the Afghanistan railway. Relations with Iran and Pakistan are crucial to efficient transport of iron ore to port for onward seafight to South and East Asian markets. Negotiations with those countries and their railway programs are a high priority and are essential to revenue generation. Continued negotiations with Tajikistan, Uzbekistan, and Turkmenistan are encouraged to determine procedures for freight originating, terminating, and transiting between the countries.

7. Legal and Regulatory. Afghanistan will need a viable legal and regulatory framework for both the railway and mining sectors permitting and enforcing property rights and the contractual agreements. The ARA will also need sufficient resources and capabilities to develop appropriate economic and safety regulations for the railway. Establishment and enforcement of safety regulations should enable a safe environment for railway personnel and communities near the railway and encourage a more efficient railway, resulting in fewer accidents.

Overall, the preferred national railway design presents medium risk based on key ANRP stakeholder input and is consistent with other large-scale capital investment projects in Afghanistan.

Recommendations to GIRoA:

- Develop and implement a comprehensive railway risk management process to identify and manage risk throughout development and operation of the railway.
- Assign the ARA chief executive director as the risk management functional lead and provide sufficient resources to the ARA for execution of risk management responsibilities.
- Require formal approval of project risk mitigation/avoidance plans prior to project funding approval.

Implementation Strategy

The ANRP provides a framework connecting Afghanistan's outlying cities, industrial sites, and commercial

interests with neighboring countries and new markets. The implementation strategy describes a macro-level plan for the expansion of Afghanistan's existing rail line. The expanded railway will help Afghanistan resume its historically important place in international trade and figure prominently in the region's future stability and progress. The overarching objectives of this implementation strategy are to 1) develop a combined rail-maritime logistics network capable of transporting Afghanistan iron ore, copper, and other minerals in a cost-efficient manner to yield competitively priced exports in the global market; 2) develop a multimodal network to promote development of industries and traffic identified in the Commercial Market Feasibility Analysis; and 3) develop the commercial, financial, and government structures needed to promote the preceding objectives.

Appealing to Regional Investors

Private investment backed by firm commitments from the GIRoA is a critical imperative for successful development and operation of the railway. International donors have already taken the initiative in Afghanistan's transportation revival, but much more assistance is needed. The Asian Development Bank (ADB) is currently the lead donor for advancing rail in Afghanistan. For example, ADB covered 97 percent of the \$175 million cost of the Hairatan–Mazar-e-Sharif rail line. ADB has also funded a \$2.86 million feasibility study to expand the existing rail line from Mazar-e-Sharif through Sheberghan and Andkhoy to Aqina. The Indian government has offered \$1 billion to help build a line from the Haji Gak iron mining area of interest near Kabul. Ownership would likely be mixed, with GIRoA retaining the land and rail lines and private entities largely controlling locomotives and rolling stock. As he contemplated myriad rail projects in 2012, Afghanistan Deputy Public Works Minister Noor Gul Mangal emphasized that further railway development could be instrumental in ending Afghanistan's economic and geographical isolation:

"We would be able to import and export to Russia, Turkey, and even European countries." That's a good deal for Afghanistan—and the world at large.

Conclusion

Joint DOD and interagency planning, analysis, and collaboration, complemented by academic and private industry expertise, enabled development and delivery of comprehensive recommendations to Afghanistan that can facilitate sustainable revenue generation and regional connectivity. While many railway proposals have been provided to GIRoA, the uniqueness of the ANRP is twofold: the ANRP provides objective recommendations principally focused on best value for the Afghan people, and the ANRP is underpinned by a business case (the Commercial Market Feasibility Analysis) reflecting revenue potential by sector over a 25-year period.

Afghanistan and its neighbors face numerous tough challenges to realize the potential economic growth that could potentially result from development of a national railway system with regional connectivity. Interministerial competition, lack of cooperation and transparency, and rampant corruption must genuinely be fixed before the key decisions in the ANRP can be enacted. GIRoA must develop a reinvestment strategy for the revenue generated by a national rail system that supports continued railway expansion and funding for other national priorities. And the people of Afghanistan must tangibly benefit from a national rail system to ensure long-term security and economic success.

Time will tell how much of the ANRP comes to fruition, but the collective efforts of the ANRP stakeholders have significant potential to improve conditions for the people of Afghanistan. JFQ

Mine-resistant, ambush protected vehicle recovers pallet of supplies dropped from C-130 Hercules aircraft in Shay Joy District, Afghanistan (U.S. Navy/Jon Rasmussen)



The USCENTCOM Train

The Deployment and Distribution Operations Center Turns 10

By Mark A. Brown

On December 12, 2003, just months after the U.S. invasion of Iraq and on the cusp of transition to Operation *Iraqi Freedom II*, General John Abizaid, USA, accepted on behalf of U.S. Central Command (USCENTCOM) an invitation that would birth the first Deployment and Distribution Operations Center (DDOC). In an October 24, 2003, memorandum, General John Handy, USAF, commander of U.S. Transportation Command (USTRANSCOM), and General Paul Kern, commander of Army Materiel Command, had offered a “joint intermodal distribution team”

led by a flag officer who “would have visibility and synchronization authority over all theater-level lift platforms.”¹ With General Abizaid’s go-ahead, a team of 42 USTRANSCOM distribution experts began arriving at Camp Arifjan in Kuwait to establish initial operational capability and validate the emerging DDOC concept during the major muscle movements of the *Iraqi Freedom II* transition.

Secretary of Defense Donald Rumsfeld decided in September 2003 to transfer oversight of the entire Department of Defense (DOD) distribution process to USTRANSCOM.² With the title of DOD Distribution Process Owner added to his list of responsibilities, General Handy decided process changes would be appropriate for oversight of movements, especially

those supporting the operation and the active USCENTCOM area of responsibility. Furthermore, a Government Accountability Office (GAO) report released in December 2003 revealed inefficiencies in the logistics support structure; these inefficiencies created a \$1.2 billion discrepancy between the amount of materiel shipped to theater and the amount received by the end user and a “backlog of hundreds of pallets and containers of materiel at various distribution points due to transportation constraints and inadequate asset visibility.”³ So on December 12, 2003, General Abizaid accepted the offer for a USTRANSCOM team of transportation experts to establish themselves at Camp Arifjan to eliminate “gaps and seams between the Strategic and Theater movement end distribution systems.”⁴

Colonel Mark A. Brown, USAF, is Chief of Current Operations for the U.S. Central Command Deployment and Distribution Operations Center.

But why a new organization? The theater Joint Movement Center (JMC) had been formally defined in joint doctrine and was performing functions similar to those of the emerging DDOC. The GAO report, USTRANSCOM's new role, and perceptions of theater airlift being inefficiently tasked led Generals Handy and Abizaid to conclude the theater JMC needed to be replaced. The JMC did not have a joint manning document with a specified list of transportation skill sets required; forming a JMC was more of a pick-up game. USTRANSCOM wanted to send its transportation experts into theater to work the issues, and that is exactly what that first-generation DDOC was chartered to do. The USCENTCOM DDOC (CDDOC) became fully mission capable on January 20, 2004, and during the brief transition, USCENTCOM/J4 assigned the theater-level JMC as a subordinate organization under the CDDOC director.⁵ The theater-level JMC merged into CDDOC on March 22, 2004.

The original concept, titled Joint Intermodal Distribution Operations Center, envisioned the new center under the tactical control of a "theater commander, nested into existing Theater Support Command."⁶ However, when actually deployed in early 2004, CDDOC was assigned not to a theater commander or any component but to USCENTCOM headquarters under the J4. That command relationship endures to the present. It was important then and now for CDDOC to make decisions on allocation, mode determination, and validation of movements from an area of operations-wide, combatant command perspective. Although CDDOC physically resides as a next-door neighbor to U.S. Army Central headquarters at Camp Arifjan, it is a tenant organization assigned to Headquarters USCENTCOM/J4. An enduring operating principle at CDDOC has been its charge to act independently from the service or functional components. From the onset, CDDOC has acted based on USCENTCOM priorities and direction.

At the 10-year mark, CDDOC has matured and evolved from the initial sketches of late 2003. CDDOC has

served USCENTCOM and the Defense Transportation System (DTS) from the Operation *Iraqi Freedom* II transition, through the troop surges in both Iraq and Afghanistan, through the withdrawal from Iraq, and now into a full-thrust redeployment and retrograde as Operation *Enduring Freedom* winds down. Manning has varied in step with movement tempo, from the initial cadre of 42 to a high of 85 while both operations were running full throttle. CDDOC has proved its worth over 10 years of refinement and proliferation across all the geographic combatant commands, refining and evolving to match the requirements of the current operational environment, and must do so again in the face of a redeployment and retrograde of unprecedented proportions. The present 2014 structure consists of 45 teammates largely from USTRANSCOM and its components, as well as the Defense Logistics Agency (DLA), headed by a one-star flag officer. The scope of their task at hand is daunting.

Current Mission

After 13 years of U.S. military operations in Afghanistan, U.S. and allied bases have proliferated, and some have matured into well-established and fully equipped hubs of activity, people, and materiel. Before the Presidentially directed deadline of December 31, 2014, CDDOC will oversee the redeployment of the bulk of the 47,000 troops currently in Afghanistan. The actual number of troops to remain in place is contingent on the Afghan government signing a bilateral support agreement authorizing a relatively small and enduring U.S. military presence. Since January 2012, CDDOC has guided the redeploy movement of 87,000 military, civilian, and contractor personnel from Afghanistan, roughly the population of Des Moines, Iowa, the Ohio State University, or a packed Rose Bowl stadium. There is also the equipment: tactical vehicles of every variety as well as road graders, cranes, and fuel tanker trucks; containers of spare parts; and a miscellany of unit gear. This mountain of equipment must be transferred to the Afghan govern-

ment, transferred or sold to another allied nation, or destroyed by DLA Disposition Services. The remainder enters the DTS to be retrograded back to home bases in the United States or military installations overseas.

This vast redeployment and retrograde task nests in a tangle of diplomatic, geographic, and fiscal constraints, each contributing to the complexity and requiring the careful attention of CDDOC and its several strategic partners. For example, in the diplomatic realm, some neighboring countries in the Middle East are sensitive to overt support to this U.S. operation. In some cases, governments find that American equipment publicly and visibly transiting their corridors is politically untenable. The DTS adopts mitigating measures. Similarly, some partner nations want to be careful not to provoke retaliation by the Taliban if they openly grant the United States access to their transportation nodes and corridors.

Simple geography presents significant constraints that compound the diplomatic factors. Afghanistan is, of course, a land-locked country with some major land routes traversing rugged terrain. Access to seaports starts with lengthy ground or air legs to position cargo for onward movement by sea. High altitudes in the north are susceptible to severe winter weather.

On the home front, the U.S. electorate generally supports the withdrawal from Afghanistan but demands efficiency in the face of extraordinary fiscal constraints. That is why General Paul Selva, commander of Air Mobility Command (AMC), announced at the September 2013 Air Force Association symposium that "we've documented now this past year \$400 million of essentially cost avoidance" from choosing sealift over airlift for transatlantic legs back to the United States.⁷ When airlift out of Afghanistan increased in mid-2013 after Afghanistan threatened to levy ground transit fees, the *New York Times* highlighted the impact on the overall retrograde price tag: "Air shipments are a far more expensive solution than simply paying the fines demanded by the Afghan government. If continued, the

air shipments could result in the withdrawal of forces reaching or exceeding \$7 billion, the upper end of [the DOD] estimated cost.”⁸ CDDOC is charged to execute the redeploy/retrograde mission within reasonable costs. There is generally no great urgency to the retrograde of equipment back to its home station, and airlift, a scarce and costly mode of transportation, must remain a carefully allocated resource even if capacity consistently exceeds requirements. That is a principle long codified in joint doctrine⁹ and one of the business rules that CDDOC has dealt with throughout its 10-year history. In 2003, in fact, inefficiencies in airlift allocation were one factor leading to establishment of the first DDOC.

What Lies Ahead

Although CDDOC has operated through the surges in Iraq and Afghanistan and the withdrawal from Iraq, the exact conditions and scope of the present Afghanistan withdrawal are unprecedented. A withdrawal is fundamentally different from a rotation; nothing can remain behind. The United States is well entrenched in several large operating bases after 12 years of battling the Taliban, and everything and everyone must be moved by one of several processes. Redeployment returns military members, DOD civilians, and their unit equipment to their home stations. Retrograde moves theater-procured equipment (equipment that was not unit deployed) to its final destination. A substantial remainder of U.S. equipment will be neither redeployed nor retrograded. Through the Foreign Military Sales or Foreign Excess Personal Property programs, the United States transfers ownership of its unneeded property to other nations.

Items not transferred, retrograded, or redeployed are destroyed by DLA Disposition Services. DLA's process ensures that items identified as excess are destroyed to ensure nothing of any tactical value to adversaries is left behind. Brigadier General Francisco Espallat, USA, CDDOC director from August 2013 to January 2014, called DLA

disposal capabilities “nothing short of amazing in terms of capacity, scale and scope. During the months of July, August and September of 2013, almost 140 million pounds of materiel was turned into scrap . . . a simply remarkable feat.” Where feasible, DLA sells the scrap locally, which generates revenue while putting potentially useful (but nonlethal) materials into Afghan hands.

The threat scenario also contributes to define the nature of the CDDOC task at hand since U.S. forces gradually become less militarily capable and therefore more vulnerable as the withdrawal progresses. This dynamic is by no means unique to *Enduring Freedom*; withdrawing forces faced this set of risks leaving Iraq as well. The power vacuum inevitably created by U.S. and North Atlantic Treaty Organization (NATO) withdrawal from Afghanistan means there is uncertainty about future allocations of political power. Will the Taliban exploit the exit, gain influence in Afghan politics, and exact retribution on Afghans who collaborated with U.S. and NATO forces? With December 31, 2014, clearly defined as the end of the operation and NATO operations, CDDOC's primary customer is faced with a dilemma: U.S. warfighters in Afghanistan may continue to face a viable, even resurgent, threat from the adversary while CDDOC and its partners on the U.S. Forces-Afghanistan (USFOR-A) staff are asking them to turn in their tactical vehicles for redeployment. Warfighting commands must make complex decisions during this withdrawal about the sequence, rate, and timing of base closures; reduction in “boots on the ground”; and turn-in of tactical equipment. These same commanders must logically synchronize their equipment redeployment and retrograde with the corresponding personnel redeployments. These actions must, in turn, be adjusted to accommodate the changing operational environment.

Within this complex set of decisions lies a classic scenario in which those who lead logistics must be careful not to constrain operational forces and unwittingly create vulnerabilities. There is an inherent tension, accentuated during a

withdrawal, between the priorities of the warfighter and those of the logistician. The warfighter demands equipment and supplies in abundance to bolster fighting power against known threats and to hedge against unknown ones. The logistician, also executing USFOR-A orders like the warfighter, demands a steady, scheduled flow of personnel and equipment to be made available for transportation out of theater. This natural tension requires constant communication between the warfighter who wants to keep his soldiers and equipment, and the logistician who wants to transport them home.

The CDDOC staff is one major point of intersection for these competing interests. More specifically, much of this deconfliction and crucial communication happens in a compact set of offices in the New Kabul Complex in Afghanistan. There, liaison officers (LNOs) to USFOR-A from CDDOC and USTRANSCOM interface directly with the USFOR-A commander and staff—the warfighters. Successfully mapping out details of this massive withdrawal hinges on striking a proper balance between warfighter and logistician priorities, and the LNOs serve both parties as brokers, negotiators, and channels of direct “hot mic” communication. They communicate warfighter direction and priorities to CDDOC and its partners, and CDDOC adapts and shapes its processes in response.

Innovations

Within the last year, CDDOC has created processes—“re-tooled the plant”—to optimize the theater transportation system while remaining responsive to warfighter requirements and priorities. First, CDDOC has regularly deployed a small forward team of transportation experts into Afghanistan known as the Advisory Team for Expeditionary Air Mobility (A-Team). A-Team plans its engagements based on upcoming base closures and provides deployed warfighters with on-scene guidance and assistance in planning their outbound movements. Though fighting units at all echelons have capable embedded logisticians, these units are not necessarily prepared to

execute a comprehensive base closure required during a withdrawal. The A-Team contributes expertise for planning and executing the complete transition from a fully manned and equipped forward operating base (FOB) engaging the enemy to bare terrain revealing little evidence of past warfighter presence. A-Team members educate, initiate, and collaborate with remote warfighters to assist the theater's transportation system make that transition happen.

Second, CDDOC has adjusted its movement processes in response to a persistent and effective threat to U.S. and NATO personnel: improvised explosive devices (IEDs). Truck convoys manned by U.S. and NATO personnel have proved highly vulnerable to IED attacks, with adversary tactics constantly evolving. As the IED threat persisted and proved consistently lethal, the urgency to get soldiers off the road increased. CDDOC and its partners substantially adjusted the ratio of air and ground movements to lessen soldiers' exposure to the IED threat during convoy operations. Since planning for air movements requires greater precision (such as in load planning, pallet building, and identifying hazardous material), the A-Team's engagements at closing FOBs, while educating users on airlift processes, complemented the overall effort to increase air movement and get soldiers off the road. Lieutenant Colonel Breck Woodard, USAF, who has led CDDOC's new Retrograde Division since August 2013, quantified the results of those first engagements: "In the first 60 days of this initiative, the [US]CENTCOM DDOC enabled the closing of three major FOBs, increased airlift velocity 400 percent, supported the building and shipment of over 14,771 air pallets, put over 7,386 twenty-foot equivalent units of cargo in the air, and most importantly, eliminated 224 ground convoys which kept over 5,600 Soldiers out of harm's way on the most dangerous roads in the world."

A third CDDOC innovation, affecting a variable in the airlift velocity equation, is the One-Touch concept. When planning FOB closures, CDDOC looks for airlift-capable sites where intratheater airlift

can deliver FOB cargo directly to one of the theater's seaports instead of aggregating air cargo at an Afghanistan hub such as Bagram. Where aircraft performance factors permit, CDDOC plans C-130s or C-17s to fly full planeloads directly to a seaport where USTRANSCOM ships provide cost-effective onward movement to the United States. Overall velocity is increased, and handling decreased, when intermediate stops are eliminated. As redeployment tempo increases, One-Touch mitigates cargo bottlenecks at the major hubs by overflying those hubs and delivering directly to the multimodal ports.

A fourth initiative, Cascading FOBs, turns those airlift-capable FOBs into aggregation points. Smaller FOBs without fixed-wing airlift capability feed their cargo into a nearby airlift-capable FOB. Finally, CDDOC has assisted the J3 staff at USCENTCOM with developing expanded options for further accelerating movements in response to the warfighter's needs.

As the redeployment and retrograde operation began in the summer of 2013, then-Brigadier General Lee Levy, the CDDOC director from January to August 2013, commented that the experience of overseeing this massive redeployment and retrograde was like "getting a doctorate in strategic transportation."¹⁰ Earlier logistics leaders such as General Handy and General Kern had foreseen in 2003 the need for an independent team of transportation experts to guide USCENTCOM's movement processes. Their original Joint Intermodal Distribution Operations Center concept has matured into a network as DDOCs proliferated across all the geographic combatant commands (and one subunified command: United States Forces Korea). It has also evolved. CDDOC, out of operational necessity, has modified its manning, organization, and processes to fit the given conditions: periods of steady-state sustainment between surges and withdrawals. The DDOC is defined and codified in joint doctrine, having proved its worth as a forward-deployed USCENTCOM/J4 team formed from USTRANSCOM and DLA movement experts.

In the current season of retrograde and redeployment, CDDOC has modified movement processes to accommodate the warfighters of Operation *Enduring Freedom* and address the inherent and chronic tension between warfighter and logistician priorities. Lessons will be learned and processes will be refined as the remaining withdrawal concludes at the end of the year. But what does a post-2014 CDDOC look like? CDDOC will likely downsize significantly in 2015 and transition to smaller-scale, steady-state operations. Its structure, processes, and experts, though, will stand by in reserve for USCENTCOM's next contingency. JFQ

Notes

¹ General John P. Abizaid, USA, Commander, U.S. Central Command, official correspondence, December 12, 2003.

² Department of Defense, "U.S. Transportation Command Appointed as Defense Distribution Process Owner," press release 701-03, September 25, 2003.

³ Government Accountability Office (GAO), *Defense Logistics: Preliminary Observations on the Effectiveness of Logistics Activities during Operation Iraqi Freedom*, GAO-04-305R (Washington, DC: GAO, 2003).

⁴ Abizaid.

⁵ Glenn G. Joerger, Deputy Director of Operations, Headquarters U.S. Transportation Command, telephone interview by author, February 12, 2004.

⁶ General John W. Handy, USAF, Commander, U.S. Transportation Command, official correspondence, October 24, 2003.

⁷ Brendan McGarry, "Air Force Shortens Cargo Routes from Afghanistan," *Military.com*, September 24, 2013, available at <www.military.com/daily-news/2013/09/24/air-force-shortens-cargo-routes-from-afghanistan.html>.

⁸ Matthew Rosenberg, "Rifts Over Fees and Taliban Sour Afghanistan Exit," *The New York Times*, July 18, 2013, available at <www.nytimes.com/2013/07/19/world/asia/rifts-over-fees-and-taliban-sour-afghanistan-exit.html?pagewanted=2&_r=0>.

⁹ The new edition of Joint Publication 3-17, *Air Mobility Operations* (Washington, DC: The Joint Staff, September 30, 2013), maintains this principle. See I-13-I-14.

¹⁰ Video interview with Brigadier General Lee Levy II, USAF, U.S. Central Command Deployment and Distribution Operations Center director, March 20, 2013, available at <www.dvidshub.net/video/285910/brig-gen-lee-levy-ii#.U9Ea5lbqxSZ>.

The NDU Foundation Congratulates the Winners of the 2014 Essay Competitions

The NDU Foundation is proud to support the annual Secretary of Defense, Chairman of the Joint Chiefs of Staff, and *Joint Force Quarterly* essay competitions. NDU Press hosted the final round of judging on May 15–16, 2014, during which 23 faculty judges from 15 participating professional military education institutions selected the best entries in each category. The First Place winners in each of the three categories are published in the following pages.

Secretary of Defense National Security Essay Competition



In 2014, the 8th annual competition was intended to stimulate new approaches to coordinated civilian and military action from a broad spectrum of civilian and military students. Essays were to address U.S. Government structure, policies, capabilities, resources, and/or practices and to provide creative, feasible ideas on how best to orchestrate the core competencies of our national security institution. The NDU Foundation awarded the first place winner a generous gift certificate from Amazon.com.

First Place

Commander David S. Forman, USN
National War College
“Deterrence with China: Avoiding Nuclear Miscalculation”

Second Place

Mark Libby, U.S. Foreign Service
National War College
“Hedging, Cooperation, and Prestige: British and French Nuclear Deterrence (How We Can Stop Worrying & Learn to Live with These Bombs)”

Third Place

**Marie L. Sanders, Office of the
Director of National Intelligence**
National War College
“Avoiding Thucydides’ Trap: China’s Interests in Latin America and Opportunities for the United States”



Chairman of the Joint Chiefs of Staff Strategic Essay Competition

This annual competition, in its 33rd year in 2014, challenges students at the Nation’s joint professional military education institutions to write research papers or articles about significant aspects of national security strategy to stimulate strategic thinking, promote well-written research, and contribute to a broader security debate among professionals. The first place winners in each category received a generous Amazon.com gift courtesy of the NDU Foundation.

Strategic Research Paper

First Place

Lieutenant Colonel Clorinda Trujillo, USAF
Air War College
“The Limits of Cyberspace Deterrence”

Second Place

Lieutenant Colonel Nicole S. Jones, USA
U.S. Army War College
“Adapting International Law for Cyberspace”

Third Place

Major Matthew L. Tuzel, USAF
School of Advanced Warfighting
“Tactics, Technology, and the End of America’s Precision Advantage”

Strategy Article

First Place

Lieutenant Colonel Bradford John Davis, USA
U.S. Army War College
“Opportunities in Understanding China’s Approach to the Senkaku/Diaoyu Islands”

Second Place

Lieutenant Douglas W. Gates, USN
Naval War College (Junior)
“U.S.-Japan-Korea Trilateral Security Cooperation: The Negative Secondary Effects of the Pacific Pivot”

Third Place

Colonel Timothy D. Brown, USA
U.S. Army War College
“RAF Enhanced: A New Concept for Whole-of-Government Solutions”

Joint Force Quarterly Kiley Awards

Each year, judges select the most influential articles from the previous year's four issues of *JFQ*. Three outstanding articles were singled out for the Kiley Awards, named in honor of Dr. Frederick Kiley, former director, NDU Press.

Best Forum Article

Lindsay L. Rodman, "Fostering Constructive Dialogue on Military Sexual Assault"

Best Recall Article

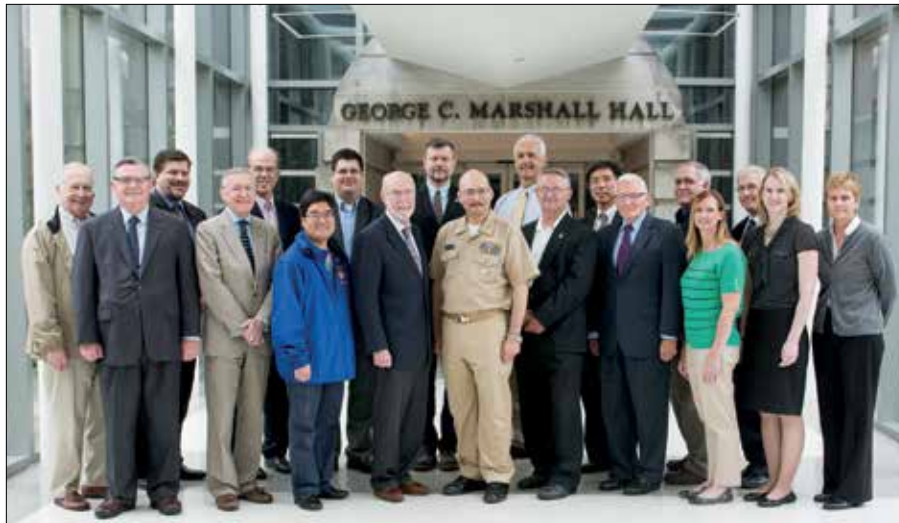
Richard L. DiNardo, "The German Military Mission to Romania, 1940–1941"

Best Features Article

Marc Koehler, "The Effects of 9/11 on China's Strategic Environment: Illusive Gains and Tangible Setbacks"

Distinguished Judges

Twenty-three senior faculty members from the 15 participating PME institutions took time out of their busy schedules to serve as judges. Their personal dedication and professional excellence ensured a strong and credible competition.



Left to right: Dr. James A. Mowbray, Air War College; Dr. Joseph J. Collins, National War College; Dr. Nichola E. Sarantakes, Naval War College; Dr. Douglas Hime, Naval War College; Dr. Stephen Burgess, Air War College; Dr. Eric Shibuya, Marine Corps Command and Staff College; Dr. Ryan Wadle, Air Command and Staff College; Dr. Larry D. Miller, U.S. Army War College; Dr. James Kiras, School of Advanced Air and Space Studies; CDR Youssef Aboul-Enein, USN, Eisenhower School; CAPT Bill Marlowe, USN (Ret.), Joint Forces Staff College; COL Dale D. Fair, USA, Joint Forces Staff College; Dr. Jim Chen, Information Resources Management College; Dr. Benjamin (Frank) Cooling, Eisenhower School; Dr. Richard J. Norton, Naval War College; Lt Col Michelle Ewy, Air Command and Staff College; Dr. Mark Clodfelter, National War College; Ms. Joanna E. Seich, NDU Press; Dr. Donna Connolly, Naval War College

Not shown: Dr. William T. Eliason, Editor in Chief, *Joint Force Quarterly*; Dr. Geoffrey Gresh, College of International Security Affairs; Dr. Antulia (Tony) Echevarria, U.S. Army War College; Dr. Carl Horn, Information Resources Management College; Dr. James Lacey, Marine Corps War College; and Dr. Harold R. Winton, School of Advanced Air and Space Studies. Photo by Katie Lewis, NDU



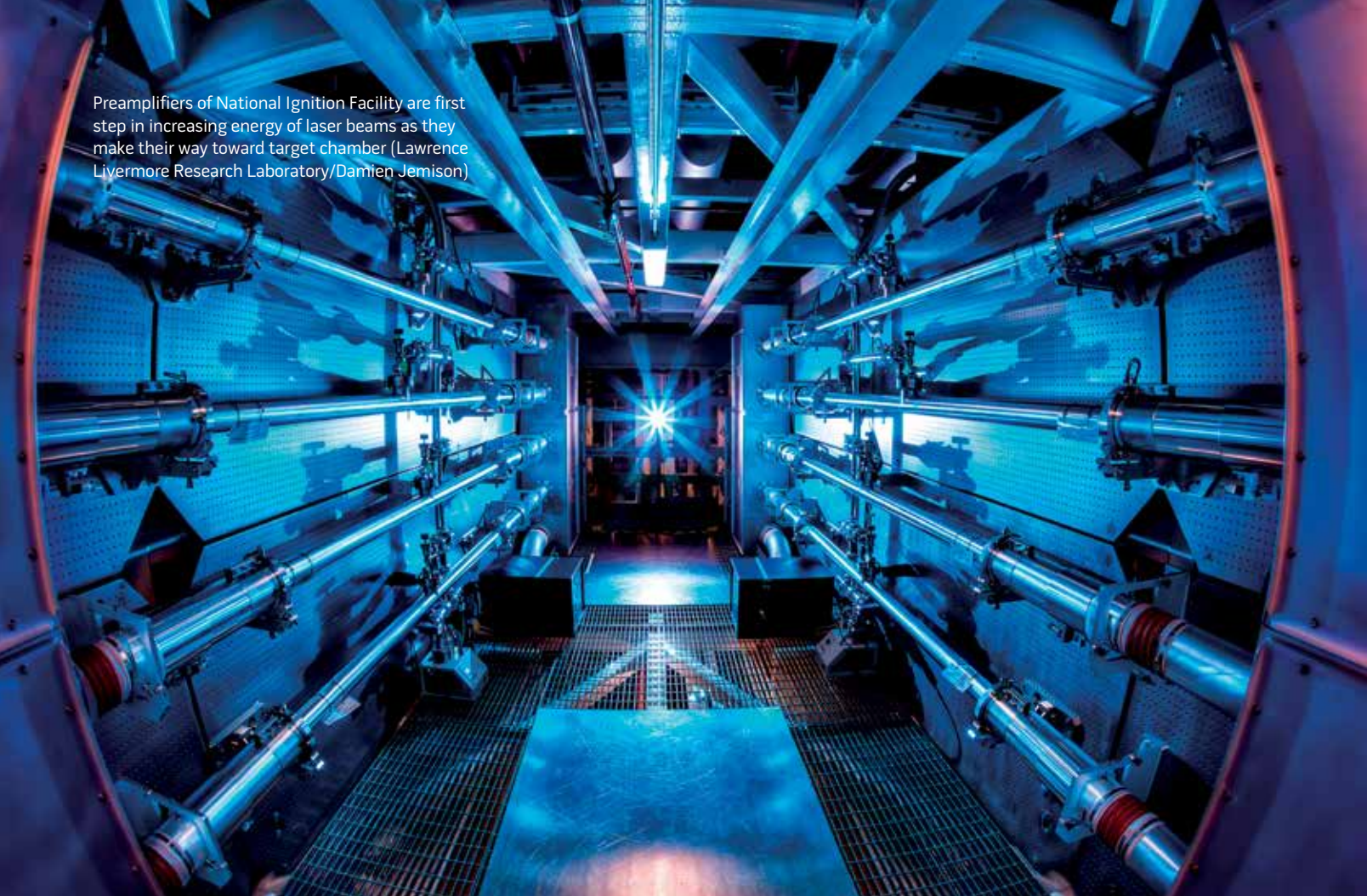
NDU Foundation

The NDU Foundation is a nonprofit 501(c)(3) organization established in 1982 to support and enhance the mission and goals of the National Defense University, America's preeminent institution for military, civilian, and diplomatic national security education, research, outreach, and strategic studies. The Foundation promotes excellence and innovation in education by nurturing high standards of scholarship, leadership, and professionalism. It brings together dedicated individuals, corporations, organizations, and groups that are committed to advancing America's national security and defense capabilities through the National Defense University. The Foundation provides NDU with privately funded resources for:

- Education, Research, Library, and Teaching Activities
- Academic Chairs, Faculty Fellowships, and Student Awards
- Endowments, Honoraria, Seminars, and Conferences
- Multicultural, International, and Interagency Programs
- National Security and Homeland Defense Outreach

Keep informed about NDU Foundation activities by visiting online at: www.nduf.org.

Pre-amplifiers of National Ignition Facility are first step in increasing energy of laser beams as they make their way toward target chamber (Lawrence Livermore Research Laboratory/Damien Jemison)



Deterrence with China

Avoiding Nuclear Miscalculation

By David S. Forman

The record reveals that defense planners have not been particularly successful in predicting the future. The U.S. has suffered a significant strategic surprise once a decade since 1940: Pearl Harbor, the North Korean invasion of South Korea, the Soviet H-bomb test, the Soviet reaction to the Arab-Israeli War of 1973, the fall of the Shah of Iran, the collapse of the Soviet Union and, most recently, 9/11.

—MACKUBIN THOMAS OWENS

Commander David S. Forman, USN, wrote this essay while a student at the National War College. It won the 2014 Secretary of Defense National Security Essay Competition.

As China rises and the United States seeks to maintain its global dominance, the world is faced with a new historical phenomenon: a dramatic shift in power between

two nuclear-capable nations. As the relative power of each nation nears parity, tension is inevitable and the character of the evolving Sino-U.S. relationship poses a risk of nuclear miscalculation.

Nuclear use between China and the United States would be a catastrophe, but China is an independent actor, and the United States can only influence, but not control, the crossing of the nuclear threshold. If U.S. policymakers neglect this risk, miscalculation is more likely.

This article analyzes nuclear deterrence principles with China across the spectrum of peacetime, conventional crisis or conflict, and nuclear war. If the United States finds itself in a crisis or conflict with China, it would be important to know how the United States achieved deterrence in peacetime as well as how deterrence might be regained if a crisis deteriorates to the point of involving nuclear weapons. The article then makes recommendations on how to enhance nuclear deterrence. By assessing the full spectrum of potential conflict in this manner, the United States can lower the risk of miscalculation.

Nuclear weapons have helped prevent conflict between world powers on anything close to the scale of another world war,¹ but nuclear deterrence toward China is different. Pivotal factors that allowed deterrence to be effective in the past do not project to the future of the Sino-U.S. relationship for two main reasons: the relative growth of China within the relationship, and the fluid maritime relationship between the United States and China, which affects how a conflict might begin and therefore how nuclear deterrence could be implemented.

Though 20th-century China developed in a world largely influenced by the United States, China is now in a position to influence the world toward its own interests.² China's growth from a considerably closed society in 1972 to a global near-peer to the United States today is a fundamental difference from the Soviet-U.S. relationship. The history of the nuclear age has yet to see a significantly weaker nuclear power eclipse a dominant nuclear power.

The second factor that distinguishes the Sino-U.S. relationship is its maritime nature, and military tensions at sea differ greatly from tensions on land. Naval assets are continually in motion, and

there is no equivalent to trench warfare or prolonged stalemates in the air or on the sea. Also, as evidenced by North Korea's suspected sinking of the South Korean corvette *Cheonan* in 2010,³ the sea sometimes offers a sense of plausible deniability that leads to aggression that would not occur on land.

China's nuclear arsenal is estimated to be small in comparison to that of the United States, but it is growing.⁴ Without official reports from China, U.S. estimates are susceptible to large errors, but analysts assess that China holds between 175 and 250 nuclear warheads.⁵ China has demonstrated land and air launch capabilities, and reliable submarine launch capability is expected in 2014 or 2015.⁶ Some of China's missiles are already capable of reaching portions of the United States, and fielding capable ballistic missile submarines (SSBNs) will only improve their capability.

If conflict begins, China and the United States do not currently have the tools to ensure it does not become nuclear.⁷ When policymakers consider the art of nuclear deterrence, many still default to Cold War principles.⁸ Blindly assuming that two great powers, each with expectations of influence and respect, can avoid conflict is unwise and increases risks of miscalculation. Based on the character of the Sino-U.S. relationship, nuclear deterrence cannot be evaluated in a vacuum, but rather along a continuum of peacetime, conventional crisis or conflict, and nuclear war.

Deterrence during Peacetime

A nation's primary goal for peacetime deterrence should be to achieve its political objectives *without* fighting a nuclear war.⁹ Three basic elements help codify peacetime deterrence. First is a nation's nuclear *declaratory policy*, which lays the foundations of a nation's intentions and is a powerful political tool. Second is the demonstrated performance of delivery systems and warheads, referred to as *deterrent reliability*. Third is a measure of each nation's ability to achieve military objectives using only its conventional capability (without resorting to nuclear weapons),

or *nonnuclear stability*. When each nation can manage these three elements in the correct way, the cost-benefit calculations of each side should favor deterrence of a nuclear conflict.

Declaratory Policy. From Beijing's perspective, current U.S. nuclear declaratory policy suggests that if Washington determined an "extreme circumstance" existed, it might resort to using its nuclear weapons to strike first. Because China is *not* a nonnuclear country under the terms of the Non-Proliferation Treaty, the negative security assurance of the 2010 Nuclear Posture Review does not apply to China.¹⁰ Though U.S. political leaders assess a first strike as next to impossible, not all Chinese leaders hold the same view.¹¹

Deterrent Reliability. A credible nuclear deterrent is the product of capability and intent.¹² Intent derives from declaratory policy as mentioned above, and capability is sustained through demonstrated reliability of delivery systems and warheads. The United States expends considerable effort to ensure the reliability of each leg of its nuclear weapon delivery triad, which consists of intercontinental ballistic missiles (ICBMs), submarine-launched ballistic missiles (SLBMs), and B-2 and B-52 bombers. The U.S. Air Force and U.S. Navy fully test the continuity of launch signals and together launch five unarmed missiles each year. The launch record is stellar, and confidence in these delivery systems is extremely high.¹³ Confidence in the warheads is a different story.

The United States last detonated an actual warhead in 1992. Time is incrementally eroding warhead reliability and, in turn, U.S. nuclear credibility. The Stockpile Stewardship Program (SSP) was created in the mid-1990s to ensure existing warheads were properly maintained, and from a scientific perspective, this program is a success; however, as noted by Dr. Kathleen Bailey from the National Institute for Public Policy, "SSP is not intended as, nor is it, a substitute for nuclear testing. There is no way that SSP can ever provide the high level of confidence in reliability of the stockpile that can be achieved by nuclear testing."¹⁴

Despite rigorous nonnuclear testing of the stockpile,¹⁵ quarterly testing reports from the National Nuclear Security Administration eventually may be insufficient to convince future adversaries, China included, that U.S. warheads are reliable.¹⁶ Detailed computer simulations provide American scientists with confidence of continued reliability, but the United States is not trying to deter American scientists.¹⁷ After 21 years, the question is rapidly becoming: do *other countries* consider U.S. warheads credible?

Nonnuclear Stability. When nuclear-capable nations are greatly outmatched by an adversary's *nonnuclear* capabilities, leaders of the less capable nation are forced to rely more heavily on their nuclear arsenals for security. Retired Russian General Makhmut Gareyev, president of the Academy of Military Sciences in Moscow, stated in 2004, "Basically [our nuclear arsenal] is the only factor which can still ensure our country's safety. We have nothing else to repel strategic military threats anymore."¹⁸ In response to a perceived threat, if a nation's leaders are forced to choose between relinquishing their own political power and authorizing a nuclear strike, then under some circumstances, a nuclear strike becomes a rational decision.

Five Policy Recommendations

First, the United States should maintain its current nuclear declaratory policy and not adopt an explicit "no first use" policy; certain forms of strategic ambiguity discourage military adventurism and can enhance nuclear stability. As a deterrence specialist stated, the overall concept of deterrence "takes place in the head of an adversary who lives in another country, has different values, is under different pressures, and has different goals."¹⁹ Being too explicit in declaratory policy removes political options and reduces the strength of deterrence.

Second, to maintain the reliability of its nuclear arsenal, the United States should seek international agreement among current nuclear powers to test nuclear warheads on a cyclic schedule.

Each nation would be permitted to conduct infrequent underground tests that could be observed by select nuclear and nonnuclear countries. Though the Comprehensive Test Ban Treaty (CTBT) procedure for peaceful tests was meant to account for geological construction projects, the precedent could be expanded because testing with international consensus would not be provocative.²⁰ Periodic international testing dates would serve as natural vehicles to discuss nuclear policies, and extended deterrence credibility could be strengthened. With no testing *ever*, the success of the CTBT could undermine nuclear deterrence and threaten the very security it was designed to protect.

Third, the United States must continue the uphill battle of maintaining the demonstrated reliability of its nuclear delivery triad. More specifically, the Air Force has yet to determine plans for replacing its long-range bombers²¹ and has been plagued by injurious reports that could undermine confidence in the reliability of the ICBM launch teams.²² The Navy is under pressure to justify the cost of its plans to replace its SSBN fleet. After a recent 2-year delay in the planned SSBN replacement program, any further delays would cause shortages in the 2030s of SSBNs for combatant commander requirements.²³ The challenges of designing, testing, certifying, and deploying a new submarine, combined with the challenges of maintaining the oldest *Ohio*-class submarines, already incur additional risk for the leg of the triad that could carry up to 70 percent of U.S. nuclear warheads.²⁴

Additionally, if the United States were to lose its current ICBM capability, either deliberately or due to perpetual neglect, the lack of a land-based deterrent would allow China to focus solely on SSBNs to prevent U.S. retaliatory attack capability.²⁵ The likelihood of being able to simultaneously disarm U.S. ICBMs and SLBMs is so remote that China would be wasteful to invest in trying; however, if the United States reverts to a dyad of delivery systems in SLBMs and aircraft (aircraft cannot be readied quickly), then investing in technology to mitigate

SLBMs becomes reasonable. This may still sound like a wasteful investment, but private enterprise is inadvertently allowing potential adversaries to close the gap on U.S. undersea dominance. Google is mapping and imaging the ocean floor in high resolution,²⁶ and research initiatives are proliferating underwater hydrophones that stream to the Internet.²⁷

Fourth, although too much information about an adversary can tempt the use of force,²⁸ the United States must seek a basic understanding of the essential elements of Chinese nuclear doctrine to lower the risk of miscalculation. The United States can incentivize information-sharing by offering China economic benefits. China's recent economic growth is not on auto pilot, and the success of President Xi Jinping's domestic agenda is far from certain. As one example, exchanging U.S. support for Chinese membership in the developing Trans-Pacific Partnership for basic Chinese nuclear doctrinal information would be a win-win for regional strategic security.²⁹

Fifth, the United States must consider how the development of a conventional prompt global strike (CPGS) capability—the ability to conduct a conventional strike anywhere in the world within 1 hour—would affect the nonnuclear balance with China. As part of a broader desire to reduce the role of nuclear weapons in U.S. foreign policy, the Obama administration has continued to support the Department of Defense's pursuit of a global strike capability that was mentioned in the 2006 Quadrennial Defense Review.³⁰ The capability of CPGS may prove advantageous in some scenarios,³¹ but those advantages do not come without a cost to nuclear deterrence stability with China—a cost that could outweigh the benefits.

Deterrence during Conventional Crisis or Conflict

Despite overt attempts by the United States to support the peaceful rise of China's military through cooperation in events such as Rim of the Pacific 2014 and humanitarian assistance/disaster response exercises, the United States does not have the only vote



Target assembly for National Ignition Facility's first integrated ignition experiment is mounted in cryogenic target positioning system, while two triangle-shaped arms form shroud around cold target to protect it before shot (Lawrence Livermore Research Laboratory)

when it comes to choosing peace or conflict. There is evidence that the Sino-U.S. relationship will be predominantly adversarial. Henry Kissinger recently noted, "Enough material exists in China's quasi-official press and research institutes to lend some support to the theory that relations are heading for confrontation rather than cooperation."³²

China has rapidly modernized its naval forces over the last decade,³³ and David Gompert's research at RAND provides evidence of why the Sino-U.S. relationship is especially challenging. He analyzed three historical cases of what happened when developing sea powers challenged existing sea powers: Germany and the United Kingdom in 1914, Japan and the United States in 1941, and the long but steady ascent of the U.S. Navy over the Royal Navy. The first two cases ended in war, and the third "led to a

gradual and largely amicable transfer of first regional and then global predominance from one navy to the other."³⁴ But importantly, Gompert quickly notes, "the United States is not about to defer to China in East Asia as Britain deferred to America in the Western Hemisphere."³⁵ If the Sino-U.S. relationship develops similarly to Gompert's first two cases studies, then history's lessons do not bode well for peace in the Pacific.

Assessing the Actual Threat. The United States misjudged the precursors of conflict in the past, and the same could happen again. Dennis Ross, chief peace negotiator for George H.W. Bush and Bill Clinton, recounts how the United States misjudged Iraq's 1990 invasion of Kuwait: "Few in the neighborhood or in the administration foresaw the possibility of Iraq actually seizing all of Kuwait. Their assessments were guided by the wrongheaded assumptions about

Saddam Hussein."³⁶ China analysts must consider the consequences of similarly wrongheaded assumptions. For example, few analysts predicted China's decision to declare its November 2013 Air Defense Identification Zone, yet its unilateral action sent shockwaves of concern through the region.³⁷

How Limited Can War Be? Several of America's previous limited wars were fought against vastly weaker and non-nuclear powers. Yet China is not vastly weaker than the United States, and the United States would be unwise to assume crisis or conflict with China would remain limited. Carl von Clausewitz theorized that war is a "paradoxical trinity—composed of primordial violence, hatred, and enmity,"³⁸ and conclusions extrapolated from previous wars cannot completely inform American policymakers in their thinking about the possibility of conflict with China.



Blue crew of *Ohio*-class ballistic missile submarine USS *Nevada* prepares to moor as submarine returns home to Naval Base Kitsap-Bangor following strategic deterrent patrol (U.S. Navy/Ahron Arendes)

Many current discussions of the likelihood of conventional confrontation leading to nuclear conflict are not logically consistent. Writers often simplify their analyses and presume the use of nuclear weapons is so unlikely it can simply be ignored. As an example, defense policy advisor Michael Pillsbury specifically depicts 16 Chinese fears, 6 of which specifically apply to conventional crisis or conflict scenarios: fear of an island blockade, fear of aircraft carrier strikes, fear of major airstrikes, fear of attacks on strategic missile forces, fear of jamming or precision strikes, and fear of attacks on anti-satellite capabilities.³⁹ Yet despite China's proximate fears, some analysts propose strategies that directly stimulate those fears while ignoring the nuclear threat.⁴⁰

In the *Journal of Strategic Studies*, Sean Mirski of Harvard Law School explores how the United States might implement a blockade strategy against China but also admits, "The United States will probably never have to consider implementing a blockade in the context of an unlimited war because such

a conflict . . . could only arise subsequent to a total breakdown in nuclear deterrence."⁴¹ Additionally, T.X. Hammes of the National Defense University promotes a distant blockade of China that "establishes a set of concentric rings that denies China the use of the sea inside the first island chain, defends the sea and air space of the first island chain, and dominates the air and maritime space outside the island chain."⁴²

All these concepts fail to adequately consider that China is a nuclear capable nation with several hundred warships. Even though not all of those warships are extremely able or their crews proficient, analysts should not assume China would allow the United States to starve China's economy with a blockade. A blockade would threaten China's regime and easily cause it to resort to force, and perhaps nuclear force. Precisely because some analysts do not understand China's psychology and assess scenarios devoid of nuclear risk, promoting these strategies may increase the likelihood of nuclear miscalculation.

Finally, the precedent of U.S. actions will determine the future validity of extended nuclear deterrence, and if U.S. commitment is rapidly eclipsed by desires to de-escalate, other nations may find renewed desire to both increase their own conventional weapon capabilities and seek their own nuclear arsenal. Nations such as Japan and South Korea may decide America's extended deterrent guarantees are unreliable and pursue nuclear weapons as security against nuclear attack.⁴³ The United States must anticipate how difficult it might be to pursue a limited conflict due to the political pressures to defend other nations in the region and prevent nuclear proliferation.

The Crisis Before the Storm. A Sino-U.S. confrontation would have global consequences that could cause physical and economic hardship for millions.⁴⁴ Political and military leaders would find themselves in crisis mode, and understanding this mindset is critical to sustaining nuclear deterrence during a Sino-U.S. crisis or conflict. William Ury and Richard Smoke, from Harvard and

Brown universities, respectively, analyze nuclear crises and note, “Times of crisis call for a special kind of negotiation. There is no time for drawn-out discussion or the usual diplomatic dance, and typically the negotiators are under considerable stress.”⁴⁵

In conventional engagements with modern powers such as China and the United States, large quantities of airplanes, ships, submarines, and cyber and space assets can rapidly come into play. As Ury and Smoke make clear, “Decision makers may fail to appreciate the value of time in a crisis or potential crisis, thereby unintentionally allowing the crisis to grow worse.”⁴⁶ If conflict begins, events may transpire at a pace that challenges the current national security decisionmaking apparatus. If this occurs, the risk of miscalculation will increase.

Natural uncertainties inherent in any conflict would be exacerbated because the U.S. method of political and military communication is so different from China’s. For example, when a Chinese F-8 aircraft collided with a U.S. Navy EP-3 aircraft in April of 2001, the United States struggled to get China to take the collision seriously and questioned if Beijing even knew the collision occurred. The Special Assistant to the U.S. Ambassador to China recounted: “While we in the Embassy were trying without success to reach officials at the Ministry of Foreign Affairs and Ministry of National Defense, the U.S. Pacific Command made the incident public in a brief, neutrally worded press release posted on its Web Site.”⁴⁷ If a collision between Chinese and U.S. aircraft was posted on a Web site before any official diplomatic or military communication was established, a similar uncertainty should be expected in the future.

Three Policy Recommendations

First, America’s political leaders and policymakers must aim to better understand the structure of China’s nuclear forces and its military decisionmaking process.⁴⁸ The United States must ensure a well-intentioned plan or military action does not *inadvertently* appear as a preemptive strike on China’s

nuclear forces.⁴⁹ Years ago, when China needed to develop its command and control organization for its nuclear forces, China’s Second Artillery Corps, also known as Strategic Rocket Forces, were deemed highly capable and given the task. As a result, nuclear and non-nuclear forces are physically collocated and share the same command and control structure. John Lewis and Xue Litai, writing in the *Bulletin of the Atomic Scientists*, describe a plausible scenario: China launches a conventional missile in a crisis or conflict, and the United States counterstrikes against Chinese collocated conventional and nuclear systems and “force[s] the much smaller surviving and highly vulnerable Chinese nuclear missile units to fire their remaining missiles.”⁵⁰ Resolving incongruous Sino-U.S. perceptions about the employment of the Second Artillery Corps is possibly the single most influential aspect of avoiding nuclear miscalculation.

Second, a reliable second-strike capability is a predominant factor for dissuading first strikes, and therefore the United States should take care to avoid explicitly targeting—and the appearance of targeting—China’s developing SSBN capability. The U.S.-China Economic and Security Review Commission recently stated, “The JL-2 [Julang-2], when mated with the [People’s Liberation Army] Navy’s JIN-class nuclear ballistic missile submarine (SSBN), will give China its first credible sea-based nuclear deterrent.”⁵¹ If China can achieve reliable second-strike capability through deployment of its SSBNs, it may be ready to divide its conventional and nuclear forces to achieve a greater margin from nuclear miscalculation.

Third, the potential for conventional crisis or conflict with nuclear-capable powers requires matching military means to political ends in a fundamentally different way. The United States must consider *not* approaching a Sino-U.S. engagement with expectations to establish large areas of military dominance. Dominance requires flawlessly attacking Chinese antiaircraft missile sites and command and control nodes that also serve

China’s nuclear forces. Flawless military plans are fiction, and based on what the United States knows of China’s Second Artillery Corps, the dangers of trying and failing could result in tactical victory but ultimate strategic defeat.⁵² To prevent a potential Sino-U.S. conventional conflict from becoming nuclear, the United States should aim to keep the engagement zone away from mainland China. American political and military leaders must be prepared for heavy losses of personnel and military ships and aircraft, and while unnecessary loss is abhorrent, aiming for a blinding victory risks nuclear retaliation that could lead to more catastrophic loss.

Deterrence during Nuclear War

In the unlikely but not impossible case that nuclear deterrence fails, if the United States has not prepared methods or plans to de-escalate in advance, the results could be far more calamitous than necessary. By developing and potentially announcing broad methodologies for how the United States would reluctantly fight a nuclear war, it is perhaps possible to reach China’s breaking point sooner, allow China to communicate when the breaking point is reached, and conclude hostilities earlier than if the conduct of a nuclear war were never discussed at all. For purposes of this analysis, assume China employed a nuclear weapon by some means and that the United States or its allies faced continued nuclear threats from China.

Four Policy Recommendations

First, how does the United States avoid using more nuclear weapons than necessary to achieve its military and political objectives? One way is to promote interval attacks that allow for conflict resolution between each attack. China is not yet capable of executing mutually assured destruction doctrine like Russia, and based on the reliability of military or political communications between China and the United States, the United States could choose to launch successive attacks within a matter of hours or a matter of days. If China



Test launch of LGM-25C Titan II ICBM from underground silo at Vandenberg Air Force Base during mid-1970s (U.S. Air Force)

attempted attacks at a rapid pace, and if a failure of U.S. theater or national missile defense allowed China's attacks to be successful, the pace of U.S. launch could be adjusted accordingly.

Second, Washington could consider how to rapidly shift to deterrence by denial. How would the United States take away China's nuclear capability altogether? China has been historically assessed to have a "minimum retaliatory strike deterrent" designed to dissuade

other nations, but most specifically the United States, from blackmailing or using nuclear weapons against China.⁵³ If China uses nuclear weapons to attack the United States or a U.S. ally, America's political leaders might feel compelled to use all of the Nation's capabilities to eliminate China's ability to launch any further nuclear attacks.

An important aspect of deterrence by denial is ballistic missile defense. According to the 2010 Ballistic Missile

Defense Review, "China is one of the countries most vocal about U.S. ballistic missile defenses and their strategic implications, and its leaders have expressed concern that such defenses might negate China's strategic deterrent."⁵⁴ What was potentially destabilizing in peacetime—better U.S. missile defenses may cause China to develop more missiles—can rapidly become essential to ending a nuclear conflict. As both China's launch capability and U.S. missile defense capability evolve over the years, U.S. ability to negate China's deterrent in peacetime may fluctuate. While ballistic missile defenses alone may be overwhelmed by China's arsenal, conventional attacks on China's launchers *combined* with missile defense may be adequate to protect the United States from a nuclear weapon. Protecting the United States from attack will enable de-escalation much sooner than if a nuclear weapon lands on U.S. soil.

Third, the United States should assess how nuclear war could be ended by nonnuclear and nonmilitary means. To assume nuclear weapons can only be answered with nuclear weapons is a false premise. Depending on the circumstances of the engagement, the United States does not necessarily need to respond in kind. If the United States can achieve its political and military objectives without using its own nuclear weapons, then it should do so.

Various political methods exist to convince China to end the conflict. As one example, despite the current cold relations between Washington and Moscow, some in Russia support a concept of "the Great Strategic Triangle" between the United States, Russia, and China.⁵⁵ Russia might gain elevated international influence following a Sino-U.S. nuclear conflict, and while Moscow should not be expected to directly support Washington's interests, Russia may still have interest in ending the conflict quickly. Russia might be in a position to use its own political and military ties with China and the United States to enable Sino-U.S. communications from its third-party perspective. Depending on the character of the war, such interlocutors may be needed to avoid further

unnecessary escalation or sustained nuclear attacks.

Fourth, while conceptualizing the end of a nuclear war with China, a secondary issue to consider is the uncertainty of the assumption that the United States could communicate with China's political leadership. Even in peacetime, the United States doubts the robustness of China's nuclear command and control structure. The burden and chaos of nuclear war may cause the United States to further question China's political control of its nuclear arsenal. If China's command and control fails during nuclear conflict, it might become impossible to deter China, and the U.S. President will be left with little choice but to use military force to disarm China of its nuclear arsenal.

Conclusion

Nuclear deterrence and nuclear war are two fundamentally different acts, yet they must be considered together to support proper analysis and policy. As the Sino-U.S. relationship moves forward, nuclear deterrence should not be relegated to the sidelines. China developed nuclear weapons to prevent U.S. coercion, but now a clear power struggle in the Asia-Pacific creates the potential that military conflict could begin and subsequently grow out of control. If the United States takes proactive measures in peacetime and has prepared for unwanted but possible transitions to conventional and nuclear conflict, then some risk could be mitigated. Unfortunately, the limited bandwidth of policymakers has not yet allowed meaningful consideration of nonpeaceful contingencies for China. The United States clearly does not want war; nuclear war with China would be an unfathomable calamity. However, even though the United States can influence the probability of a conflict, in the end, Washington does not have the final word. Therefore, prudence requires the United States to prepare for the worst in a way that does not make nuclear war a self-fulfilling prophecy. Preparations must not lead to the very endstate the United States is trying to avoid.

The road ahead is long, and the issues presented here could be pertinent for decades. Solutions that seem impossible now may become more plausible over time, and the United States should continue to evaluate reasonable methods to lower the risk of nuclear conflict. War is possible but not inevitable, and as Vice President Joe Biden recently quoted his father, "The only conflict worse than one that is intended, is one that is unintended."⁵⁶ JFQ

Notes

¹ Clark A. Murdock, *The Department of Defense and the Nuclear Mission in the 21st Century* (Washington, DC: Center for Strategic and International Studies, 2008), 13.

² Many international organizations, such as the World Trade Organization, International Monetary Fund, and United Nations are heavily influenced by American views on economics, human rights, and government. Between President Richard Nixon's famous trip in 1972 to Beijing and 2011, China's gross domestic product grew from 19th globally (\$1.28 billion) to 3rd (\$4.2 trillion). See United Nations, "GDP and its breakdown for all years—sorted alphabetically, All countries for all years—sorted alphabetically," National Accounts Main Aggregates Database, available at <<http://unstats.un.org/unsd/snaama/dnlist.asp>>.

³ Victor Cha, "The Sinking of the *Cheonan*," Center for Strategic and International Studies, April 22, 2010, available at <<http://csis.org/publication/sinking-cheonan>>.

⁴ Hans M. Kristensen and Robert S. Norris, "Chinese nuclear forces, 2013," *Bulletin of the Atomic Scientists* 69, no. 6 (November 1, 2013), available at <<http://thebulletin.org/2013/november/chinese-nuclear-forces-2013>>.

⁵ Robert S. Norris and Hans M. Kristensen, "Chinese nuclear forces, 2010," *Bulletin of the Atomic Scientists* 66, no. 134 (2010), 139.

⁶ Office of the Secretary of Defense, *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2013* (Washington, DC: Department of Defense, 2013), 31.

⁷ Avery Goldstein, "First Things First," *International Security* 37, no. 4 (Spring 2013), 53.

⁸ Paul Bracken, *The Second Nuclear Age, Strategy, Danger and the New Power Politics* (New York: Times Books, 2012), 257.

⁹ T.V. Paul, *The Tradition of Non-Use of Nuclear Weapons* (Stanford: Stanford University Press, 2009), 13. Renowned economist Thomas Schelling made popular the concept of a "tradition of non-use of nuclear weapons" within the theory of nuclear deterrence.

¹⁰ *Nuclear Posture Review Report* (Washington, DC: Department of Defense, April 2010), viii. In this report, the United States created a negative security assurance for several countries. The United States declared it "would only consider the use of nuclear weapons in extreme circumstances to defend the vital interests of the United States or its allies and partners" (viii–xi) and that it "will not use or threaten to use nuclear weapons against non-nuclear weapon states that are party to the NPT [Non-Proliferation Treaty] and in compliance with their nuclear non-proliferation obligations" (viii).

¹¹ Bill Gertz, "Guess Who's Coming to Dinner, Chinese general who threatened nuclear strike on U.S. visits Washington this week," *The Washington Free Beacon*, March 4, 2013.

¹² Terry Diebel, *Foreign Affairs Strategy: Logic for American Statecraft* (New York: Cambridge University Press, 2007), 143.

¹³ Lockheed Martin, "Lockheed Martin-Built Trident II D5 Missile Achieves a Total of 148 Successful Test Flights Since 1989," September 24, 2013, available at <www.lockheedmartin.com/us/news/press-releases/2013/september/924-ss-FBM.html>. To verify reliability, the Air Force annually removes nine launch cables from randomly selected intercontinental ballistic missiles (ICBMs) and reconnects them to test equipment to verify correct launch signals are sent to the missiles. The launch signal is also tested from E-6 aircraft to verify connectivity with the Airborne National Command Post, a vital element of the contingency control system governing nuclear launch. Additionally, once a year the Air Force removes the warhead from a Minuteman III ICBM and actually launches the missile. The Navy also removes the warheads from four submarine-launched ballistic missiles every year and conducts four launches to fully test the reliability of the launch signal system and missile launch capability.

¹⁴ Kathleen C. Bailey, *The Comprehensive Test Ban Treaty: An Update on the Debate* (Fairfax, VA: National Institute for Public Policy, 2001), 8.

¹⁵ Cole J. Harvey, "Nuclear Stockpile Modernization: Issues and Background," Nuclear Threat Initiative, February 15, 2010, available at <www.nti.org/analysis/articles/nuclear-stockpile-modernization/>.

¹⁶ Quarterly testing reports are available at <<http://nnsa.energy.gov/ourmission/managingthestockpile/sspquarterly>>.

¹⁷ Nevada National Security Site, *Stockpile Stewardship Program* (Las Vegas: National Nuclear Security Administration, 2013), available at <www.nv.doe.gov/library/factsheets/DOENV_1017.pdf>.

¹⁸ David Holley, "Seeking respect and protection, Russia bolsters nuclear arsenal," *Seattle Times*, December 13, 2004, available at <http://seattletimes.com/html/nation-world/2002117512_russarms13.html>.

¹⁹ William F. Hoefft, Jr., “Deterrence: Now More Than Ever,” U.S. Naval Institute *Proceedings* 139, no. 6 (June 2013), 26–31, available at <www.usni.org/magazines/proceedings/2013-06/deterrence—now-more-ever>.

²⁰ Comprehensive Nuclear Test Ban Treaty (CTBT), 77, available at <www.ctbto.org/fileadmin/content/treaty/treaty_text.pdf>. Although the CTBT of 1996 prohibits “any nuclear weapon test explosion or any other nuclear explosion,” the treaty also provides a procedure to seek approval of testing for peaceful purposes. Specifically, Article VIII states: “On the basis of a request by any State Party, the Review Conference shall consider the possibility of permitting the conduct of underground nuclear explosions for peaceful purposes.”

²¹ Nuclear Threat Initiative, “Air Force Chief: Bomber Cost to Be Tightly Capped,” Global Security Newswire, November 15, 2013, available at <www.nti.org/gsn/article/air-force-chief-bomber-cost-be-tightly-capped/>.

²² Robert Burns, “AP Exclusive: Commander Cites ‘Rot’ in Nuke Force,” *The Big Story*, May 8, 2013, available at <<http://bigstory.ap.org/article/ap-exclusive-air-force-sidelines-17-icbm-officers>>.

²³ Rear Admiral Richard P. Breckenridge, testimony before the House Armed Services Committee, September 12, 2013, available at <<http://docs.house.gov/meetings/AS/AS28/20130912/101281/HHRG-113-AS28-Wstate-JohnsonD-20130912.pdf>>.

²⁴ Amy F. Wolf, *The New START Treaty: Central Limits and Key Provisions*, R41219 (Washington, DC: Congressional Research Service, April 8, 2014), 20, available at <www.fas.org/sgp/crs/nuke/R41219.pdf>.

²⁵ Bomber aircraft are not usually loaded for nuclear strikes and can take a long time to prepare for nuclear missions.

²⁶ “A clearer view of the seafloor in Google Earth,” *Google.com*, February 2, 2012, available at <<http://google-latlong.blogspot.com/2012/02/clearer-view-of-seafloor-in-google.html>>.

²⁷ Rhitu Chatterjee and Rob Hugh-Jones, “Sounds of the sea: Listening online to the ocean floor,” *BBC News Magazine*, January 16, 2012, available at <www.bbc.co.uk/news/world-16555916>.

²⁸ Goldstein, 75.

²⁹ Ryan Burkhart, “The U.S., China, and the Trans Pacific Partnership,” *Diplomatic Courier*, November 1, 2013, available at <www.diplomaticcourier.com/news/regions/asia/1868-the-u-s-china-and-the-trans-pacific-partnership>.

³⁰ *Quadrennial Defense Review Report* (Washington, DC: Department of Defense, February 6, 2006), 6, available at <www.defense.gov/qdr/report/report20060203.pdf>.

³¹ M. Elaine Bunn and Vincent A. Manzo, *Conventional Prompt Global Strike: Strategic*

Asset or Unusable Liability? Strategic Forum, No. 263 (Washington, DC: NDU Press, 2011), 5. Bunn and Manzo note four plausible scenarios where conventional prompt global strike would clearly enhance U.S. security objectives: “when terrorist leaders are located, WMD transfers are suspected, missile launches are imminent, and ‘high-value’ targets (for example, a national leader or command and control nodes) are identified in larger military campaigns.”

³² Henry Kissinger, “The Future of U.S.-Chinese Relations: Conflict Is a Choice, Not a Necessity,” *Foreign Affairs* 91, no. 2 (March/April 2012), 44–45, available at <www.foreignaffairs.com/articles/137245/henry-kissinger/the-future-of-us-chinese-relations>.

³³ Ronald O’Rourke, *China Naval Modernization: Implication for U.S. Navy Capabilities—Background and Issues for Congress*, RL33153 (Washington, DC: Congressional Research Service, October 17, 2012), 40, available at <<https://opencrs.com/document/RL33153/>>.

³⁴ David C. Gompert, *Sea Power and American Interests in the Western Pacific* (Santa Monica, CA: RAND, 2013), iii.

³⁵ *Ibid.*, xiii.

³⁶ Dennis Ross, *Statecraft and How to Restore America’s Standing in the World* (New York: Farrar, Straus and Giroux, 2008), 75.

³⁷ Daniel Byman, “The Foreign Policy Essay: Oriana Skylar Mastro on ‘China’s ADIZ—A Successful Test of U.S. Resolve?’” *Lawfareblog.com*, December 15, 2013, available at <www.lawfareblog.com/2013/12/the-foreign-policy-essay-orian-sky-lar-mastro-on-chinas-adiz-a-successful-test-of-u-s-resolve/>.

³⁸ Carl von Clausewitz, *On War*, ed. Michael Howard and Peter Paret (Princeton: Princeton University Press, 1976), 89.

³⁹ Michael Pillsbury, “The Sixteen Fears: China’s Strategic Psychology,” *Survival: Global Politics and Strategy* 54, no. 5 (October–November 2012), 149–182, available at <www.tandfonline.com/doi/abs/10.1080/00396338.2012.728351#preview>.

⁴⁰ See, for instance, Jan van Tol et al., “Air-Sea Battle: A Point-of-Departure Operational Concept,” Center for Strategic and Budgetary Assessments, May 18, 2010. The U.S. Navy recently invested in next-generation jamming capability for the EA-18B aircraft, and the Department of Defense refocused its attention on antisatellite weapons in the summer of 2013.

⁴¹ Sean Mirski, “Stranglehold: The Context, Conduct and Consequences of an American Naval Blockade of China,” *Journal of Strategic Studies* 36, no. 3 (June 2013), 390.

⁴² T.X. Hammes, *Offshore Control: A Proposed Strategy for an Unlikely Conflict*, Strategic Forum, No. 278 (Washington, DC: NDU Press, June 2012), 4.

⁴³ Steve Herman, “Rising Voices in S. Korea, Japan Advocate Nuclear Weapons,” *Voice of America*, February 15, 2013, available at <www.voanews.com/content/

rising-voices-in-south-korea-japan-advocate-nuclear-weapons/1604309.html>; and M.J. Chung, “Keynote: M.J. Chung, Member, National Assembly of the Republic of Korea,” panel, Carnegie International Nuclear Policy Conference, Washington, DC, April 9, 2013, available at <<http://carnegieendowment.org/2013/04/09/keynote-m.j.-chung-member-national-assembly-of-republic-of-korea/fv9t>>.

⁴⁴ Douglas P. Guarino, “Study: Two Billion Could Starve in Event of ‘Limited’ Nuclear War,” Global Security Newswire, December 10, 2013, available at <www.nti.org/gsn/article/study-two-billion-could-starve-event-limited-nuclear-war/>.

⁴⁵ William L. Ury and Richard Smoke, “Anatomy of a Crisis,” in *Negotiation Theory and Practice*, ed. J. William Breslin and Jeffrey Z. Rubin, 47 (Cambridge: The Program on Negotiation at Harvard Law School, 1991).

⁴⁶ *Ibid.*, 49.

⁴⁷ John Keefe, “A Tale of ‘Two Very Sorries’ Redux,” *Far Eastern Economic Review*, March 21, 2002, available at <www.freerepublic.com/focus/f-news/646427/posts>.

⁴⁸ Samantha Hoffman and Peter Mattis, “Inside China’s New Security Council,” *The National Interest*, November 21, 2013, available at <<http://nationalinterest.org/commentary/inside-chinas-new-security-council-9439>>.

⁴⁹ Larry M. Wortzel, *China’s Nuclear Forces: Operations, Training, Doctrine, Command, Control and Campaign Planning* (Carlisle, PA: Strategic Studies Institute, May 2007), iii.

⁵⁰ John W. Lewis and Xue Litai, “Making China’s nuclear war plan,” *The Bulletin of the Atomic Scientists* 68, no. 5 (2012), 61, available at <http://iis-db.stanford.edu/pubs/23840/Making_China’s_nuclear_war_plan.pdf>.

⁵¹ U.S.-China Economic and Security Review Commission, *2013 Report to Congress* (Washington, DC: Government Printing Office, 2013), 214.

⁵² Goldstein, 88.

⁵³ Linton Brooks, “The Sino-American Nuclear Balance: Its Future and Implications,” in *China’s Arrival: A Strategic Framework for a Global Relationship*, ed. Abraham Denmark and Nirav Patel, 64 (Washington, DC: Center for a New American Security, 2009).

⁵⁴ Department of Defense, *Ballistic Missile Defense Review Report, February 2010* (Washington, DC: Department of Defense, 2010), 34.

⁵⁵ Alexi Arbatov and Vladimir Dvorkin, *The Great Strategic Triangle* (Moscow: Carnegie Moscow Center, April 2013).

⁵⁶ Joe Biden, “Remarks to the Press by Vice President Joe Biden and Prime Minister Shinzo Abe of Japan,” December 2, 2013, available at <www.whitehouse.gov/the-press-office/2013/12/03/remarks-press-vice-president-joe-biden-and-prime-minister-shinzo-abe-jap>.

Forward deployed *Ticonderoga*-class guided-missile cruiser
USS *Cowpens* launches Harpoon missile from aft missile
deck as part of live-fire exercise in Valiant Shield 2012
(U.S. Navy/Paul Kelly)



The Limits of Cyberspace Deterrence

By Clorinda Trujillo

For to win one hundred victories in one hundred battles is not the acme of skill. To subdue the enemy without fighting is the acme of skill.¹

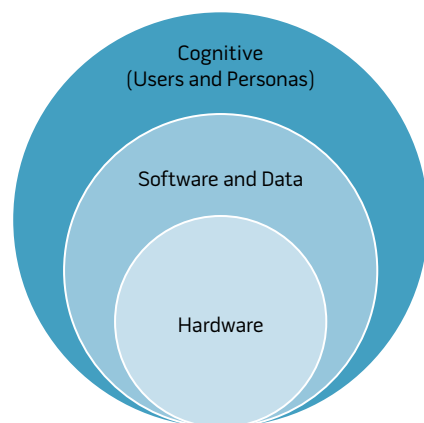
—SUN TZU

Lieutenant Colonel Clorinda Trujillo, USAF, wrote this essay while attending the Air War College, Air University. It won the Strategic Research Paper category of the 2014 Chairman of the Joint Chiefs of Staff Strategic Essay Competition.

As a concept, deterrence has been part of the military vernacular since antiquity. In his *History of the Peloponnesian War*, Thucydides quotes Hermocrates as stating, “Nobody is driven into war by ignorance, and no one who thinks that he will gain anything from it is

deterred by fear.”² In the 2,400 years since then, the domains for the conduct of military affairs have expanded from the original land and maritime domains to air, space, and now cyberspace. As warfighting expanded its scope, strategic theory did as well. Today, U.S. doctrine declares that the fundamental

Figure 1. Cyberspace Components



purpose of the military is to deter or wage war in support of national policy.³ Therefore, military strategists and planners have a responsibility to assess how adversaries may be deterred in any warfighting domain. Through the joint planning process, planners, working through the interagency process, consider deterrent options for every instrument of national power—diplomatic, informational, military, and economic—across all phases of military operations.⁴ However, most of the thought and analysis in deterrence has revolved around the use of conventional and nuclear weapons.

In May 2009, President Barack Obama acknowledged the United States considers its digital infrastructure a strategic national asset and declared that protecting it would be a national security priority.⁵ Besides working to ensure information and communication networks are secure, this protection would also take the form of deterring, preventing, detecting, and defending against cyber attacks. As a result, American national and military policy has incorporated cyberspace deterrence as a necessary objective and has identified a need to use cyber capabilities to deter adversaries in or through cyberspace. But is this an achievable objective and, if so, to what extent?

By providing an understanding of the cyberspace domain and deterrence theory, as well as reviewing existing policy, this article shows that although deterrence is a viable component of strategic thought for conventional and

nuclear military operations, deterrence in cyberspace is limited due to restrictions imposed by a lack of attribution, signaling, and credibility. As a result, the U.S. Government should strengthen its cyberspace defenses, pursue partnerships, and advance policy and legislative solutions, while undertaking further research to overcome the limits inherent in cyberspace deterrence today.

Understanding Cyberspace

Cyberspace is a domain created through the interaction of three different components: the hardware, the virtual, and the cognitive (see figure 1). The physical reality of cyberspace is comprised of the interdependent network of information technology infrastructures.⁶ This includes all the hardware of telecommunication and computer systems, from the routers, fiber optic and transatlantic cables, cell phone towers, and satellites, to the computers, smartphones, and, ultimately, any device that contains embedded processors such as electric power grids and the F-22 Raptor. Some of these systems might be connected to local networks or the Internet some or all of the time. Others might never be physically connected but can receive data input through connected devices or external media. Cyberspace also has a virtual component that encompasses the software, firmware, and data—the information—resident on the hardware. This includes the operating systems, applications, and data stored on the hard drive or memory of a computing system.

This hardware and software are extremely complex, fast, and cheap. In the past 40 years, the number of transistors on a microprocessor has increased from 2,300 to over 2.5 billion. Storage devices are 200,000 times the size of the first computer hard drive. Aircraft flown by the U.S. Air Force have evolved from the F-4 Phantom, with 8 percent of its functions performed by software, to the F-22 Raptor, which is 80 percent dependent on computer technology.⁷ Cyberspace has become a global, pervasive environment with everyone from users to corporations to governments becoming more dependent on connectivity and access—and this

access is extremely fast. One computer can connect to another on the other side of the world in milliseconds. Furthermore, the cost of entry into cyberspace has become negligible. Originally, only research institutions and governments could afford it, but now anyone can purchase a smartphone or a laptop computer and have access to the environment, the billions of users, and the millions of terabytes of information resident in it.

The human, or cognitive, aspect is the final element of cyberspace. Whereas other domains are solely part of the physical environment, cyberspace, as the only man-made domain, is shaped and used by humans. Cognitive personas interact with the virtual environment and each other. In cyberspace, this human persona can be reflective, multiplicative, or anonymous. To access certain networks, for example, researchers have developed identity management tools to ensure the identity is an accurate reflection of the person. However, the same user can have a different persona, or many cyber personas, in other systems—for example, multiple email accounts. This leads to an element of anonymity whereby one cannot always positively identify the user of a system. It is difficult to prove that a person using an account is the person he or she claims to be. Cognitive users of the cyberspace environment can be nation-state or nonstate actors (such as users, hackers, criminals, or terrorists).

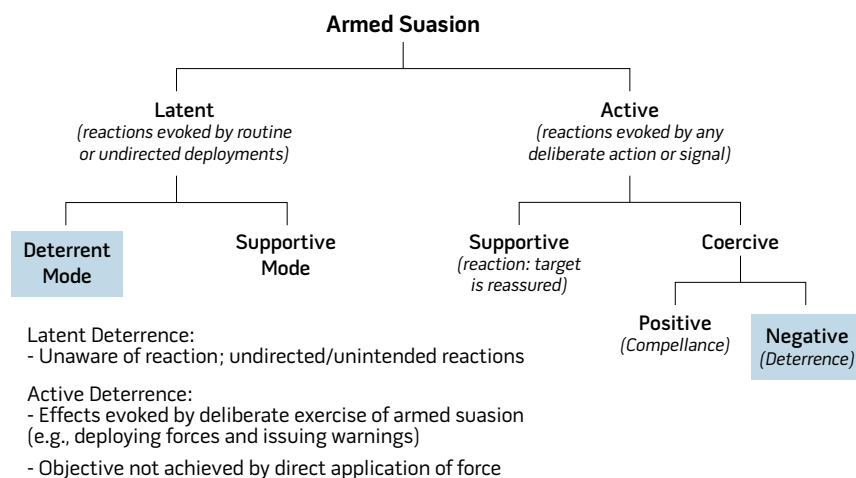
When the architecture of cyberspace was originally developed, its creators envisioned neither the proliferation nor the advanced technologies that would evolve. If he had a chance to do it again, Vint Cerf, one of the “fathers” of the Internet, has stated, “I would have put a much stronger focus on authenticity or authentication—where did this email come from, what device I am talking to.”⁸ The limitations of cyberspace make it difficult to protect and defend it. Although the physical elements may reside within sovereign territorial boundaries, the virtual spaces do not. Pakistan has cyber assets in the United States; India has some of its assets in Norway.⁹ This limits the idea of a possible “Monroe Doctrine”¹⁰ in cyberspace, especially when private

and foreign entities own so much of the infrastructure, data, and virtual components. In many ways, the capabilities and uses inherent in cyberspace are limitless, restricted only by existing hardware and software restraints. To address successfully whether the concept of cyberspace deterrence is feasible, however, requires a framework for deterrence theory itself.

Understanding Deterrence

Deterrence, according to joint doctrine, is the prevention of action by either the existence of a credible threat of unacceptable counteraction or the belief that the cost of action outweighs the perceived benefits.¹¹ In other words, deterrence is successful when an actor is convinced that restraint from taking an action is an acceptable outcome.¹² It is a state of mind in the adversary.¹³ Although the U.S. military can take actions with intent to deter, it is the adversary who determines whether the actions are successful. Deterrent options can be either latent (passive) or active. Latent deterrence is a defensive measure also referred to as deterrence by denial. Active deterrence is achieved through the threat of retaliation—or rather, deterrence by punishment.¹⁴ Edward Luttwak in *The Political Uses of Sea Power* proposed a typology for the political application of naval power that addressed the breadth of military purpose from deterring to waging war. This typology is applicable to the cyberspace domain and succinctly depicts both of these deterrent options (see figure 2).¹⁵ The first of these options is latent deterrence where there is no directed effort by an actor to deter another. In cyberspace, if a hacker wanted to break into a wireless network but the administrator had changed the default password, the hacker might be initially deterred. However, the administrator was not actively deterring the hacker. Instead, he or she had taken basic cybersecurity actions to protect, or defend, the network. As a result, the security and resiliency of computer systems provide a possible deterrent to actors in cyberspace. The second deterrent option is active deterrence. In this

Figure 2. Edward Luttwak's Armed Suasion Typology



case, the deliberate exercise of military influence evokes deterrent effects. For example, if the United States issued warnings or threats to an adversary, this would be an active deterrence act.

Successful active deterrence, however, requires attribution, signaling, and credibility.¹⁶ A target for deterrence must be identifiable (or *attributable*). For example, in the nuclear arena, the United States has matured its capability in forensics to determine the origin of nuclear material regardless of the source.¹⁷ It can attribute the material to a particular nation or actor, which thus becomes the target to which deterrent actions are tailored. *Signaling* is the effort to communicate the message to the intended audience. *Credibility* requires maintaining a level of believability that proposed actions might be used. If the United States claims that a response would be full spectrum, the target needs to believe it. This also requires a demonstration of capability. To deter a target actively, one has to have the means to threaten the target into inaction. In a nuclear scenario, all nations are aware of the American ability to attribute a nuclear attack to its source, U.S. retaliatory policy, and its demonstrated nuclear abilities. The United States has the clear capability and credibility to follow through with this threat and has provided signaling to any who would challenge it. However, nuclear deterrence strategy does not translate well to other domains. To address some

of these concerns in today's asymmetric environments, Washington revised its deterrent options to a tailored deterrence concept focused on specific state or non-state actors.¹⁸ Nevertheless, cyberspace policy and doctrine have not evolved as smoothly.

Cyberspace and Deterrence in Policy and Doctrine

In 2009, Lieutenant General Robert Schmidle, Jr., USMC, then the first deputy commander for U.S. Cyber Command, summarized the state of strategic thinking for the newest warfighting domain: "There is a real dearth of doctrine and policy in the world of cyberspace."¹⁹ At that time, cyberspace strategic thought was limited in scope and, in some cases, classified. More than 10 years earlier, President Bill Clinton had identified the importance of and vulnerability present in American systems when he issued an executive order in 1996 on critical infrastructure protection.²⁰ In the ensuing decade, however, terms such as *computers*, *cyberspace*, or *networks* barely received mention in American national strategic policy. For example, the 2005 National Defense Strategy touched on cyber assurance support. In addition, the 2006 Quadrennial Defense Review declared the Department of Defense (DOD) would "maintain a deterrent posture to persuade potential aggressors that objectives including cyberspace would be denied and could result in

Table 1. Deterrence and Cyberspace in Policy

Policy	Summary
2010 National Security Strategy	Prevent/deter state and nonstate actors: <ul style="list-style-type: none"> • identify and interdict threats • deny hostile actors' ability to operate within borders • protect critical infrastructure and key resources • secure cyberspace (invest in people/technology and strengthen partnerships). Recognizes some threats cannot be deterred.
2011 National Military Strategy	Military role is to deter and defeat aggression. Enhance deterrence by having capability to fight through degraded environment and improving ability to attribute and defeat attacks on systems and infrastructure. Military must provide broad range of options to ensure access and use of cyberspace and hold malicious actors accountable. Need for resilient cyberspace architecture employing detection, deterrence, denial, and multilayered defense.
2011 International Strategy for Cyberspace	Dissuade and deter with overlapping policies that combine network resilience with vigilance and credible response options. The United States will respond to hostile acts in cyberspace as to any other threat to the country through the use of any available means.
2011 DOD Strategy for Operating in Cyberspace	Support 2011 International Strategy for Cyberspace. Deter/mitigate insider threats through workforce accountability and internal monitoring. Enables collective self-defense and deterrence through development of international shared situational awareness and warning capabilities.

Table 2. Deterrence and Cyberspace in Joint Doctrine

Joint Publication	Deterrence and Cyberspace Summary
3-0, <i>Joint Operations</i>	Role of deterrence in general: "Deterring adversaries is a [U.S.] goal." Role of deterrence in joint operational planning process Cyberspace only mentioned in inclusion of U.S. Cyber Command and its mission.
3-12, <i>Cyberspace Operations</i>	Does not mention deterrence specifically or directly. Cyberspace defensive actions include protect, detect, characterize, counter, and mitigate to secure, operate, and defend network. Cyberspace attack actions are deny, degrade, disrupt, destroy, and manipulate to create direct denial. Cyberspace capabilities are integrated at all levels and in all military operations. Cyberspace operations are conducted across the range of military operations.
3-13, <i>Information Operations</i>	Effective employment of information-related capabilities (including cyberspace operations) during shape and deter phases of an operation or campaign can have significant impact. Cyberspace capabilities deny or manipulate decisionmaking.
3-14, <i>Space Operations</i>	Space deterrence is accomplished by: <ul style="list-style-type: none"> • promoting/demonstrating responsible behavior in space • pursuing partnerships that encourage restraint • contributing to quick attribution for attacks • protecting space capabilities and infrastructure • implementing appropriate responses should deterrence fail.
3-27, <i>Homeland Defense</i>	Offensive capabilities with defensive may deter adversary from threatening or attacking the homeland. Environment presents unique challenges for joint force commander (JFC) in selection and engagement of targets in cyberspace. Because specific attribution and geographic location are often difficult to determine, JFC must abide by rules of engagement.
5-0, <i>Joint Operation Planning</i>	Includes examples of deterrent options for each instrument of national power. Informational flexible deterrent options include protecting friendly communications systems and intelligence assets through computer network defense, operations security, and information assurance.
Deterrence Operations Joint Operating Concept	Published in 2006, but not a standard joint publication. It was scheduled for an update in 2008. Identified that network defense capabilities could play important role in deterrence operations.

overwhelming response,"²¹ but did not build upon this, and neither did military doctrine. Although President George W. Bush did not address cyberspace in the 2002 National Security Strategy (NSS), he did mention deterrence. First, there is a preeminent focus on weapons of mass destruction and the importance to deter their use whenever possible. The 2002 NSS highlights the military's role in deterring these threats against U.S.

interests and theorizes that traditional concepts of deterrence will not work against terrorists.²² Furthermore, the 2002 NSS identified a requirement to detect and deter international industrial espionage but did not present this task as a military role. Instead, this is covered under the task of enforcing trade agreements and laws against unfair practices.

Since President Obama's statement in 2009 emphasizing the importance of

cyberspace to national security, policy and doctrine for the cyberspace domain and cyberspace deterrence have advanced significantly. Although not consistent with each other, the 2010 NSS, the 2011 National Military Strategy, and other policy documents have begun to address cyberspace and define objectives for cyberspace deterrence (see table 1). Joint doctrine also varies in its maturity and consistency in referring to deterrence

or the cyberspace domain (see table 2). For example, Joint Publication (JP) 3-14, *Space Operations*, includes ways through which space deterrence is accomplished. Although some of these would be applicable to the cyberspace domain, JP 3-12, *Cyberspace Operations*, does not address deterrence at all. Moreover, cyberspace doctrine for the military Services is not consistent with joint doctrine. It is continuing to mature through military exercises and the evolution of the U.S. Cyber Command force development construct. For instance, the relevant doctrine for the Air Force was last updated in 2011—2 years before the publication of the joint doctrine—and does not address deterrence in a useful capacity.²³

Based on this existing policy and doctrine and additional scholarly efforts, proposed cyberspace deterrent options include:

- develop policy and legal procedures
- develop other credible response options
- pursue partnerships
- secure cyberspace
- enhance resiliency
- strengthen defense
- conduct cyberspace deception.

Each of these deserves a brief explanation. Developing policy serves as a signaling component of deterrence and provides credibility when supported by demonstrated action. Closely integrated with policy is enhancing legal procedures to apprehend and prosecute criminals and nonstate actors. Other credible response options include demonstrating capabilities to identify and interdict threats, to conduct offensive actions in cyberspace, and to implement appropriate responses should deterrence fail. The notion of pursuing partnerships drives an environment where multiple states and nonstate actors can work together for the improvement of all those involved. This can be accomplished through strengthening international norms for cyberspace, but can also further a framework for constructive deterrence.²⁴ In this situation, adversaries are co-opted into a relationship, preventing them from taking the action one is working to deter. Securing cyberspace

involves investing in digital literacy, developing secure technologies, and mitigating the insider threat. Enhancing resilience is a latent deterrent that helps one “fight through” in a degraded environment. Aligned with this is strengthening defense by protecting infrastructure, denying adversaries the ability to operate within one’s borders, improving the ability to defeat attacks, sharing situational awareness, and improving attribution. Some authors suggest deception serves as a deterrent because cyberspace operations have the ability to manipulate decisionmaking. However, deception is not a deterrent; it is an intentional act designed to gain an advantage and inherently serves a different purpose than deterrence.²⁵

Barriers to Cyberspace Deterrence

Cyberspace characteristically provides limitations to many of the proposed cyberspace deterrent options. The first of these is the attribution challenge compounded by the speed of the domain. In 2012, then-Secretary of Defense Leon Panetta stated, “Potential aggressors should be aware that the U.S. has the capacity to locate them and to hold them accountable for their actions.”²⁶ Nothing could be further from the truth. In 2007, Estonia was the target of “large and sustained distributed denial-of-service attacks flooding networks or websites . . . many of which came from Russia,”²⁷ but who was responsible? Although the attacks appeared to come from network addresses within Russia, it was never confirmed whether this was a state-sponsored or nonstate effort. Some authors argue that an obvious deterrent to attacks, espionage, or criminal activity in cyberspace is to identify publicly the countries where these efforts originated, thereby leading others to regard that nation as a risky place to do business.²⁸ Nations could also pursue sanctions against those harboring these actors.²⁹ Unfortunately, many countries, including the United States, do not have the resources or the legal standing to validate the identity of the attackers

or to take actions against them. The difficulty of attribution is also a significant challenge to a cyberspace response. Any rapid counterstrike is likely to hit the wrong target, but hesitation could lead to increased vulnerability and exploitation.

A second limitation to cyberspace deterrence is that the first-strike advantage cannot be deterred. Sun Tzu wrote, “Know the enemy and know yourself,”³⁰ but in cyberspace, many vulnerabilities are unknown. In 2007, both American and British government agencies detected a series of attacks codenamed “Titan Rain.”³¹ These attacks, reportedly one of the largest scale infiltrations known at the time, had allegedly been going on undetected since 2002.³² This is only one example, but it demonstrates how the complexities of the domain make it impossible to be aware of all vulnerabilities or to monitor all systems. Existing cyberspace capabilities, defenses, and forces (both law enforcement and military) also fail to deter opponents. In 2012, Symantec, a cybersecurity company, identified a 58 percent increase in mobile malware and over 74,000 new malicious Web domains.³³ Moreover, there is a healthy market for zero-day exploits with prices ranging from \$5,000 to \$250,000.³⁴ In a related study on the cost of cybercrime, the Ponemon Institute found a 42 percent increase in successful cyber attacks on companies in 2012—a number that continues to move upward, although this trend could be attributed to businesses being more forthcoming on criminal activity.³⁵ Both Symantec and McAfee have provided estimates on the annual cost of worldwide cybercrime ranging from \$110 billion to \$1 trillion,³⁶ though determining accurate costs is difficult as many companies do not want to report incidents due to possible business repercussions, and others may not be aware of criminal activity. Accordingly, it is difficult to show where deterrent actions deny either state or nonstate actors benefits.

Third, there is a risk of asymmetric vulnerability to attack in cyberspace—that is, the threat that the use of a capability could backfire. As one actor develops



Workers prepare for launch of third Advanced Extremely High Frequency satellite, a joint-Service system that provides survivable, near worldwide, secure, protected, and jam-resistant communications for high-priority national military operations (Courtesy Lockheed Martin)

offensive and defensive capabilities, other actors will strive to improve their offensive and defensive skills as well. This continuous endeavor could push a model that leads to a cyber “arms race.”³⁷ In 1998, the Central Intelligence Agency (CIA) director announced the United States was developing computer programs to attack the infrastructure

of other countries.³⁸ By then, the U.S. Government Accountability Office estimated over 120 state and nonstate actors had or were developing information warfare systems.³⁹ Information on exploiting vulnerabilities and attacking networks is readily available on the Internet,⁴⁰ and with American dependency on cyberspace being greater than most, the United

States is taking a risk by developing advanced cyberspace capabilities.

Credibility is also a significant issue in cyberspace. Credibility is dependent on proof, but attacks that work today may not work tomorrow. Even though the United States has “pre-eminent offensive cyberspace capabilities, it obtains little or no deterrent effect”⁴¹ from them for two reasons. First, claiming to put a specific target at risk from a cyber attack will likely result in that asset receiving additional protection or being moved offline and placed out of risk.⁴² Second, secrecy may be working against American interests. General James Cartwright, USMC, stated, “You can’t have something that’s secret be a deterrent. Because if you don’t know it’s there, it doesn’t scare you.”⁴³ Once introduced, cyberspace weapons become public property, which quickly renders the capability useless.⁴⁴ Stuxnet, the malware that destroyed centrifuges in Iranian nuclear facilities, is a perfect example. After its identification, responses resulted in two separate reactions: companies patched vulnerabilities in their software exploited by Stuxnet, and variants of the malware began to appear. Unlike kinetic weapons, cyber weapons, once released, can be analyzed, understood, and modified by other actors, thereby eliminating the deterrent element of the cyberspace capability.

Credibility is also dependent on action. However, the United States has a poor track record of responding to cyberspace incidents due to delayed detection, inability of attribution, and limited, if any, action⁴⁵ as the boundaries of proportionality are still evolving. In 2009, then-Major General William Lord, commander of the Air Force Cyber Command (Provisional), noted, “It’s easier for us to get approval to do a kinetic strike with a 2,000-pound bomb than it is for us to do a non-kinetic cyber activity.”⁴⁶ Even though President Obama, through the International Strategy for Cyberspace, has stated the United States reserves the right to respond to hostile acts in cyberspace with any instrument of national power, and the Pentagon has declared that a computer attack from a foreign nation could be considered an

act of war, both have left unclear what the response would be.⁴⁷ The U.S. Government, its citizens, and private organizations are on the receiving end of millions of cyber intrusions per day, but the United States has established a precedent of limited action to and tolerance of these incidents. The 2007 Estonia incident also depicts one aspect of this credibility challenge. As a result of the alleged Russian cyber attacks, Estonia declared its security threatened and sought support from the North Atlantic Treaty Organization.⁴⁸ However, many Alliance members, including the United States, did not share this perspective. There had been no physical violence, casualties, or territorial invasion, and Russia did not claim responsibility for the incidents. Tolerance to crime, espionage, and other cyberspace acts has established a high threshold preventing the use of force in domains other than cyberspace to date.

Lastly, cyberspace actors have a different risk tolerance than those acting in a physical domain due to their perceived anonymity, invulnerability, and global flexibility. Neither policy nor legal recourse is sufficient to deter state or nonstate actors from their objectives. For example, no one has officially claimed responsibility for the development and deployment of Stuxnet. Additionally, last year, the Federal Bureau of Investigation published a Cyber Most Wanted list.⁴⁹ Although there are Federal arrest warrants on these people, it is likely none of them are in the country or committed their crimes while in it. In many cases, the actors' goals are to defy authority or gain prestige.⁵⁰ Existing guidance is neither credible nor enforceable and antiquated legal procedures have not kept up with technological advances to meet this challenge. Then-commander of U.S. Cyber Command, General Keith Alexander, USA, stated in 2012, "Last year we saw new prominence for cyber activist groups, like Anonymous and Lulz Security that were encouraging hackers to work in unison to harass selected organizations and individuals."⁵¹ Besides being insufficient to deter state and nonstate actors, U.S. or international cyberspace policy challenges American interests. Washington

wants to maintain freedom of action in cyberspace, which includes the ability to conduct espionage and exploitation for diplomatic and military reasons. Pursuing partnerships, especially in the international commons, challenges this desire. In December 2012, the International Telecommunications Union revised governing agreements with a negotiated global telecommunications treaty. On the day before the scheduled signing, the United States rejected it for two reasons: the interrelationship between telecommunications and the Internet,⁵² and an expansion of the United Nations' role in Internet governance.⁵³ Even though the agreement would not have been legally binding, the United States believed the former reason could have led to restrictions on free speech and the latter would drive a government-led model for Internet oversight. Instead, the United States prefers the multi-stakeholder model in place today that allows for government, commercial entities, academia, and others to deliberate and establish Internet standards. If Washington is serious about international partnerships in cyberspace, it needs to find a way to overcome its realist angst in this domain. The impetus to maintain cyberspace freedom of action limits the option to hold a nation accountable for cyber activities within its borders.

These barriers to deterrence delineate problems with attribution, signaling, and credibility—all characteristics of active deterrence. Moreover, the technology and architecture of the cyberspace domain—the complexity, vulnerability, and attribution problems—limit the success of credible response options for deterrence as well. However, even though the cyberspace domain is not 100 percent defensible, latent deterrence options through cyber defense do provide a viable option for use in cyberspace.

Recommendations

Successful cyberspace deterrence needs to be a whole-of-government effort to defend the military, the public and private sectors, and international partners and allies. Based on the assessment presented, feasible options

for cyberspace deterrence comprise strengthening defense to include securing cyberspace and increasing resiliency, pursuing partnerships, and advancing policy and legislative solutions. Today, these options are restricted to the realm of latent deterrents. Further research, however, may yield opportunities that eliminate the attribution, signaling, and credibility restrictions of the cyberspace domain.

To support defensive actions, private and public organizations need to identify critical assets and build up resiliency of those systems including ensuring non-homogeneity in systems technology. For example, rather than standardizing software and hardware across a network, organizations should install different operating systems for key backup systems. Unfortunately, recent efforts are headed the other way. DOD is developing a single integrated network with an expectation that it will be more cost effective and can be more easily defended. Instead, this centralizes vulnerabilities and makes it easier for adversaries to exploit. For instance, the Air Force's unclassified network desktop and server solution is built around the Microsoft Windows operating system, but this operating system has thousands of known (and unknown) vulnerabilities. The unclassified network routers are a standardized Cisco product, yet Cisco has identified and published 560 security advisories for its systems.⁵⁴ As a result of identifying a new vulnerability in either the Microsoft or Cisco systems, a cyber actor can exploit or attack all areas of the network dependent on those products. On the other hand, this actor would be unable to affect the F-22's Integrated Management Information System directly as it runs on a different operating system.

In addition, the military needs to defend priority systems and expand the forces available to conduct mission assurance. Mission assurance is the ability to ensure a mission is successfully accomplished even when under attack or in a reduced operating environment. Although all military systems depend on cyberspace, not all systems have equal priority. Further efforts should be made

to exercise with degraded cyberspace capabilities to identify critical priorities and determine the necessary forces and resources for defense. However, this is not just a military issue. The critical infrastructure of the United States is also at risk. In coordination with DOD and the Department of Homeland Security, the National Guard conducts mission assurance assessments for critical defense industrial base and prioritized critical infrastructure and key resource assets.⁵⁵ Increased growth in this program would expand the available defenses and resiliency for the Nation and increase its latent deterrent capabilities.

To further strengthen defenses, the U.S. Government should incentivize the public and private sectors to take steps that will compel them to assure others they have not been maliciously compromised. Unlike the pursuit of regulatory solutions, incentives would drive an increase in cybersecurity. For example, U.S. Transportation Command has modified contracting language to require companies to provide information assurance data and report compromises.⁵⁶ In return, the command shares information with contractors to enhance their cybersecurity. This effort could be enhanced by linking contracting bonuses or profit opportunities to specific cybersecurity postures. The U.S. Government, on the other hand, could establish guidelines to provide tax breaks or subsidies for compliance with certain standards.

In the pursuit of partnerships, Washington should engage internationally to establish cyberspace norms. Lack of norms has led to a substantial gray area exploited by state and nonstate actors alike. In 2011, China, Russia, and others submitted an International Code of Conduct for Information Security to the United Nations as a possible starting point for the development of these norms.⁵⁷ The United Kingdom has also hosted two international conferences on the subject.⁵⁸ However, different nations have different priorities and interests in the pursuit of the normalization of cyberspace. The United States seeks to ensure freedom of access while enhancing the security of networks. Other countries,

such as Russia and China, focus on the risk of freedom of access to their political stability. One recommendation would engage the United States with those countries, whether they are allies, partners, or friends, who have similar interests to address these issues from a common platform. Although a broad agreement may not be possible at this time, steps are needed toward improving overall security in the cyberspace environment.

Another area to improve is advancing policy and legal options. Legislation lags behind the speed of innovation in cyberspace. The development of warfare and corresponding law for other domains has been refined over decades, as in the case of air and space, or centuries. In cyberspace, technological progress has been exponential, but corresponding domestic and international law is decades behind schedule. This status quo hinders the pursuit and prosecution of criminal actors due to the global nature of cyberspace. The U.S. Government needs to assign greater resources to address this problem today. Policy can also support deterrence goals, but it needs to be clearly stated, credible, and consistent.

Lastly, the U.S. Government and DOD should advocate for greater research and development to increase attribution and systems security and to support an evolution of the cyberspace domain toward a more secure and robust environment. For example, improvement in identity management has shown significant results in deterring attacks. Implementation of the DOD Common Access Card reduced intrusions into military networks by over 50 percent.⁵⁹ Ultimately, cyberspace attacks are possible only because networks and systems have flaws.⁶⁰ If the United States can eliminate those flaws, additional cyberspace deterrent options may become available.

Conclusion

In 1982, an American satellite detected a large blast in Siberia that turned out to be an explosion of a Soviet gas pipeline.⁶¹ This explosion, which was the result of a deliberate action by the CIA to tamper with the software in the computer control system, represented the

first cyber attack of its kind in history. This attack demonstrated the use of a weapon that ignored physical defenses and deterrent threats and showed “the U.S. was willing to use malware against a hostile, nuclear-armed superpower without concern of attribution or threat of retaliation.”⁶² If the United States is not deterred, how can it ensure others would be?

Deterrence through cyberspace *by means of* cyberspace is limited due to its inherent character and purpose. The anonymity, global reach, scattered nature, and interconnectedness of the domain reduce the effectiveness of deterrence and can render it useless.⁶³ In this environment, developing deterrents or a deterrent strategy against state or nonstate actors does have some utility. Even though the man-made nature of the domain hinders the attribution, signaling, and credibility required for active deterrence, all cyber actors do want to accomplish something, and defensive deterrence is more effective in cyberspace than attempting to impose costs.⁶⁴ Defensive deterrence, however, is a whole-of-government, whole-of-nation effort. The U.S. military is focused on defending its own networks, but there is a lack of effort to defend the national infrastructure. Through understanding the limits of cyberspace deterrence, strategists, policymakers, and planners can advance policy and doctrine that will rise to the challenges presented in this warfighting domain. Nevertheless, additional research may one day overcome these limits to cyberspace deterrence. JFQ

Notes

¹ Sun Tzu, *The Art of War*, trans. Samuel B. Griffith (New York: Oxford University Press, 1963), 77.

² Thucydides, *History of the Peloponnesian War*, trans. Benjamin Jowett, available at <www.perseus.tufts.edu/hopper/text?doc=Perseus%3Atext%3A1999.04.0105%3Abook%3D4%3Achapter%3D59>.

³ Joint Publication (JP) 3-0, *Joint Operations* (Washington, DC: The Joint Staff, August 11, 2011), I-1.

⁴ JP 5-0, *Joint Operation Planning* (Washington, DC: The Joint Staff, August 11, 2011), E-1.



F-15 Eagle departs during mission employment phase exercise at Nellis Air Force Base that incorporates Air Force capabilities in diverse scenarios including aircraft with space and cyberspace assets (U.S. Air Force/Brett Clashman)

⁵ The White House, “Remarks by the President on Securing Our Nation’s Cyber Infrastructure,” May 29, 2009, available at <www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure>.

⁶ JP 1-02, *Department of Defense Dictionary of Military and Associated Terms* (Washington, DC: The Joint Staff, April 2001), 64.

⁷ Kadir Alpaslan Demir, “Challenges of Weapon Systems Software Development,” *Journal of Naval Science and Engineering* 5, no. 3 (2009), 106.

⁸ Joseph Menn, “Founding father wants secure ‘Internet 2,’” *Financial Times*, October 11, 2011, available at <www.ft.com/intl/cms/s/2/9b28f1ec-0009-11e0-aeca-00144feab49a.html#axzz2nm8mMPNV>.

⁹ “Where There is Smoke, There is Fire: South Asian Cyber Espionage Heats Up,” *ThreatConnect.com*, August 2, 2013, available at <www.threatconnect.com/news/where-there-is-smoke-there-is-fire-south-asian-cyber-espionage-heats-up/>; Norman Shark, “Operation Hangover: Unveiling an Indian Cyberattack Infrastructure,” *NormanShark.com*, May 2013.

¹⁰ Bob Brewin, “NSA Director Calls for a Cyberspace Monroe Doctrine,” *Nextgov.com*, May 6, 2009, available at <www.nextgov.com/cybersecurity/2009/05/nsa-director-calls-for-a-cyberspace-monroe-doctrine/43773/>.

¹¹ JP 3-0, GL-9.

¹² Department of Defense (DOD), *Deterrence Operations Joint Operating Concept*, Ver. 2.0, December 2006, 3.

¹³ John B. Sheldon, *Space Power and Deterrence: Are We Serious?* Policy Outlook (Washington, DC: The George C. Marshall Institute, November 2008), 1.

¹⁴ Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica, CA: RAND, 2009), 7.

¹⁵ Edward N. Luttwak, *The Political Uses of Sea Power* (Baltimore: The Johns Hopkins University Press, 1974), 4.

¹⁶ Peter Marquez, “Space Deterrence: The Prêt-à-Porter Suit for the Naked Emperor,” in *Returning to Fundamentals: Deterrence and U.S. National Security in the 21st Century*, 10 (Washington, DC: The George C. Marshall Institute, August 2011).

¹⁷ Defense Threat Reduction Agency and U.S. Strategic Command Center for Combat-

ing WMD and Standing Joint Force Headquarters—Elimination, “Nuclear Forensics and Attribution,” available at <www.dtra.mil/Missions/NuclearDetectionForensics/Forensics.aspx>.

¹⁸ *Quadrennial Defense Review Report* (Washington, DC: DOD, February 6, 2006), 4.

¹⁹ Sandra Erwin, “Cyber Command Wrestling with Unresolved Technology Policy Issues,” *National Defense*, March 2, 2011, available at <www.nationaldefensemagazine.org/blog/lists/posts/post.aspx?ID=341>.

²⁰ President William J. Clinton, Executive Order 13010, “Critical Infrastructure Protection,” *Federal Register* 61, no. 138 (July 17, 1996), available at <www.gpo.gov/fdsys/pkg/FR-1996-07-17/pdf/96-18351.pdf>.

²¹ *Quadrennial Defense Review Report*, 25.

²² *The National Security Strategy of the United States of America* (Washington, DC: The White House, September 2002), 15.

²³ Air Force Doctrine Document 3-12, *Cyberspace Operations* (Washington, DC: Headquarters Department of the Air Force, July 15, 2010, incorporating change 1, November 30, 2011), mentions *deterrence* only in a description of the purpose of the “offensive” principle

of joint operations: “Disrupt, degrade, deny, deter, seize, retain, and exploit initiative.” However, the example *cyberspace operation* is a distributed denial of service attack on Estonia in 2007, which is not an example of deterrence.

²⁴ Michael E. Vlahos, “Shadows of Globalization: A Guide to Productive Deterrence,” in *Unrestricted Warfare Symposium 2006*, 191–193 (Baltimore: The Johns Hopkins University, 2006).

²⁵ Joseph W. Caddell, *Deception 101—Primer on Deception* (Carlisle, PA: Strategic Studies Institute, 2004), available at <www.strategicstudiesinstitute.army.mil/pubs/display.cfm?pubID=589>.

²⁶ Leon E. Panetta, “Remarks by Secretary Panetta on Cybersecurity to the Business Executives for National Security, New York City,” October 11, 2012, available at <www.defense.gov/transcripts/transcript.aspx?transcriptid=5136>.

²⁷ Jason Healey and Leendert van Bochoven, “NATO’s Cyber Capabilities: Yesterday, Today, and Tomorrow,” Atlantic Council Issue Brief, February 2012, available at <www.atlanticcouncil.org/publications/issue-briefs/natos-cyber-capabilities-yesterday-today-and-tomorrow>.

²⁸ David E. Sanger, *Confront and Conceal* (New York: Broadway Paperbacks, 2012), 268.

²⁹ Franklin D. Kramer and Melanie J. Teplinsky, “Cybersecurity and Tailored Deterrence,” Atlantic Council Issue Brief, December 2013, available at <www.atlanticcouncil.org/images/publications/Cybersecurity_and_Tailored_Deterrence.pdf>.

³⁰ Sun Tzu, 84.

³¹ Richard Norton-Taylor, “Titan Rain—how Chinese hackers targeted Whitehall,” *The Guardian.com*, September 4, 2007, available at <www.theguardian.com/technology/2007/sep/04/news.internet>.

³² Paul Cornish et al., *On Cyber Warfare—A Chatham House Report* (London: Royal Institute of International Affairs, 2010), 8.

³³ Symantec Corporation, *Internet Security Threat Report 2013—Volume 18*, April 2013, 10, available at <www.symantec.com/content/en/us/enterprise/other_resources/b-istr-main_report_v18_2012_21291018.en-us.pdf>.

³⁴ Andy Greenberg, “Shopping for Zero-Days: A Price List for Hackers’ Secret Software Exploits,” *Forbes.com*, March 23, 2012, available at <www.forbes.com/sites/andygreenberg/2012/03/23/shopping-for-zero-days-an-price-list-for-hackers-secret-software-exploits/>.

³⁵ Ponemon Institute Research Report, “2012 Cost of Cyber Crime Study: United States,” Ponemon Institute, October 2012, 1, available at <www.ponemon.org/local/upload/file/2012_US_Cost_of_Cyber_Crime_Study_FINAL6%20.pdf>.

³⁶ Paul Hyman, “Cybercrime: It’s Serious, But Exactly How Serious?” *Communications of the ACM* 56, no. 3 (March 2013),

18, available at <http://cacm.acm.org/magazines/2013/3/161196-cybercrime-its-serious-but-exactly-how-serious/fulltext>.

³⁷ Yang Jian, “Deterrence Has No Place in Cyberspace,” *China-U.S. Focus.com*, February 28, 2013, available at <http://chinausfocus.com/peace-security/deterrence-has-no-place-in-cyberspace/>.

³⁸ John Christensen, “Bracing for Guerrilla Warfare in Cyberspace,” *CNN.com*, April 6, 1999, available at <http://cyber.law.harvard.edu/eon/ci/elabs/security/cyberterror.htm>.

³⁹ Ibid.

⁴⁰ Kathryn L. Gauthier, *China as Peer Competitor? Trends in Nuclear Weapons, Space, and Information Warfare*, Maxwell Paper No. 18 (Montgomery, AL: Air War College, July 1999), 27.

⁴¹ John Markoff, David E. Sanger, and Thom Shanker, “In Digital Combat, U.S. Finds No Easy Deterrent,” *The New York Times*, January 26, 2010, available at <www.nytimes.com/2010/01/26/world/26cyber.html?_r=0>. Dr. Lewis also reiterated his point on November 15, 2012; see “Jim Lewis of CSIS speaks at Stimson on Cyber Deterrence,” November 15, 2012, available at <www.stimson.org/about/news/jim-lewis-of-csis-speaks-at-stimson-on-cyber-deterrence/>.

⁴² Libicki, 52–53.

⁴³ Andrea Shalal-Esa, “Ex-U.S. general urges frank talk on cyber weapons,” Reuters, November 6, 2011, available at <www.reuters.com/article/2011/11/06/us-cyber-cartwright-idUSTRE7A514C20111106>.

⁴⁴ Sarah Weiner, “Searching for Cyber-Deterrence,” Center for Strategic and International Studies, November 26, 2012, available at <http://csis.org/blog/searching-cyber-deterrence/>.

⁴⁵ Kevin Chilton and Greg Weaver, “Waging Deterrence in the Twenty-First Century,” *Strategic Studies Quarterly* (Spring 2009), 39.

⁴⁶ Quoted in Kevin R. Becker, “Strategic Deterrence in Cyberspace: Practical Application,” graduate research project, Air Force Institute of Technology, June 2009, 82.

⁴⁷ Siobhan Gorman and Julian E. Barnes, “Cyber Combat: Act of War—Pentagon Sets Stage for U.S. to Respond to Computer Sabotage with Military Force,” *The Wall Street Journal*, May 31, 2011, available at <http://online.wsj.com/news/articles/SB10001424052702304563104576355623135782718>.

⁴⁸ Peter W. Singer and Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know* (Oxford, UK: Oxford University Press, January 2014; uncorrected advance reading copy), 102.

⁴⁹ Federal Bureau of Investigation, “Cyber’s Most Wanted,” available at <www.fbi.gov/wanted/cyber>.

⁵⁰ Patrick M. Morgan, “Applicability of Traditional Deterrence Concepts and Theory to the Cyber Realm,” in *Proceedings of a Workshop on Detering Cyber Attacks: Informing Strate-*

gies and Developing Options for U.S. Policy, 58 (Washington, DC: The National Academies Press, 2010).

⁵¹ General Keith B. Alexander, commander, U.S. Cyber Command, “Statement Before the House Committee on Armed Services, Subcommittee on Emerging Threats and Capabilities,” March 20, 2012.

⁵² Eric Pfanner, “U.S. Rejects Telecommunications Treaty,” *The New York Times*, December 13, 2012, available at <www.nytimes.com/2012/12/14/technology/14iht-treaty14.html?_r=0>.

⁵³ James R. Clapper, “Statement for the Record: Worldwide Threat Assessment of the U.S. Intelligence Community,” House Permanent Select Committee on Intelligence, April 11, 2013, 2–3.

⁵⁴ Cisco, “Cisco Security Advisories, Responses, and Notices,” available at <http://tools.cisco.com/security/center/publication-Listing.x>.

⁵⁵ National Guard, “Critical Infrastructure Protection Mission Assurance Assessments,” fact sheet, available at <www.nationalguard.mil/media/factsheets/2013/CIP-MAA%20-%20March-2013.pdf>.

⁵⁶ Rita Boland, “Command’s Cybersecurity Crosses Domains, Directorates,” *Signal.com*, June 1, 2013, available at <www.afcea.org/content/?q=node/11124>.

⁵⁷ Yang.

⁵⁸ Timothy Farnsworth, “Is There A Place for Nuclear Deterrence in Cyberspace?” *Arms Control Now: The Blog of the Arms Control Association*, May 30, 2013, available at <http://armscontrolnow.org/2013/05/30/is-there-a-place-for-nuclear-deterrence-in-cyberspace/>.

⁵⁹ Commission on Cybersecurity for the 44th Presidency, “Securing Cyberspace for the 44th Presidency,” Center for Strategic and International Studies, December 2008, 62.

⁶⁰ Libicki, xiii.

⁶¹ “Cyberwar: War in the fifth domain—Are the mouse and keyboard the new weapons of conflict?” *The Economist*, July 2010, available at <www.economist.com/node/16478792?story_id=16478792&src=rss>.

⁶² Richard B. Andres, “The Emerging Structure of Strategic Cyber Offense, Cyber Defense, and Cyber Deterrence,” in *Cyberspace and National Security*, ed. Derek S. Reveron, 89 (Washington, DC: Georgetown University Press, 2012).

⁶³ Tang Lan and Zhang Xin, “The View from China: Can Cyber Deterrence Work?” in *Global Cyber Deterrence: Views from China, the U.S., Russia, India, and Norway*, ed. Andrew Nagorski, 1 (New York: EastWest Institute, 2010).

⁶⁴ M. Elaine Bunn, *Can Deterrence Be Tailored?* INSS Strategic Forum No. 225 (Washington, DC: NDU Press, January 2007), 3.

Ground Self-Defense Force soldiers stand in formation with fixed bayonets during opening ceremony Orient Shield XI, a 2-week exercise in Kami-Furano, Japan, which partners Japanese military with U.S. forces (U.S. Army)



Opportunities in Understanding China's Approach to the Senkaku/Diaoyu Islands

By Bradford John Davis

In 2010, two Japanese coast guard vessels and a Chinese fishing boat collided in the disputed waters near the Senkaku/Diaoyu Islands, sparking increasingly confrontational behavior by both China and Japan.¹ The pattern

of escalation continued in 2012 when Japan nationalized several of the disputed islands by purchasing them from the private owner. China promptly responded by sending warships to the area in a show of force.² Although

escalation to the point of war is unlikely, these incidents underscore the destabilizing regional effects of the disputed islands and associated maritime boundaries. China's territorial claims are rooted in historical context, nationalism, national security, and economic interests.³ By understanding China's perspectives, motives, and approaches to resolving this dispute, the United States can anticipate the current pattern

Lieutenant Colonel Bradford John Davis, USA, wrote this essay while a student at the U.S. Army War College. It won the Strategy Article category of the 2014 Chairman of the Joint Chiefs of Staff Strategic Essay Competition.



Yasukuni Shrine

of escalation, forecast future Chinese behavior, and identify opportunities for conflict management and eventual de-escalation to improve strategic stability in the region.

Named the Senkaku Islands by Japan and the Diaoyu Islands by China, the group of eight small uninhabited islands in the southern end of the Ryukyu Island chain comprise a mere 7 square kilometers of land.⁴ In the context of increasingly contested sovereignty in the East China Sea, these seemingly unimportant islands have a far greater strategic significance than size and location would otherwise warrant. The Sino-Japanese friction over maritime resources has created a dangerous military competition in which both countries are applying a zero-sum-gain approach based on sovereignty.⁵ As the current pattern of escalation continues, the risk of destabilizing the region also increases.

Regional instability in the East China Sea carries several significant risks to U.S. strategic interests. First, increased militarization of the dispute generates pressure for both China and Japan to invest in weapons technologies and additional platforms. Second, as more ships and aircraft operate in the area while China and Japan endeavor to demonstrate administrative control of the maritime boundaries, the likelihood of an incident sparking rapid escalation increases. This carries significant alliance implications for the United States vis-à-vis the 1960 Treaty of Mutual Cooperation and Security with Japan.⁶ Third, American corporations have economic interests in keeping the sea lines open to international shipping and ensuring access for future energy exploration. Finally, the United States needs to maintain healthy diplomatic relations with China to encourage Chinese acceptance of international norms and promote

global economic stability.⁷ Because these are vital interests to the United States, it is important to understand China's approach to the dispute when developing a regional strategy.

China's historical claim to the uninhabited islands dates back to the Ming Dynasty, when the Ryukyu Kingdom served as a vassal state from the 14th to 17th centuries and tribute payments continued until 1875. During this period, Chinese fishermen used these islands as shelter and navigational aids. As Chinese power waned during the Qing Dynasty and Japanese power grew as a result of the Meiji Restoration, Japan formally annexed the islands as part of the Okinawa Prefecture in 1895. The Cairo and Potsdam Declarations led China to believe the Allied Powers would expel Japan from the Ryukyu Islands at the conclusion of World War II. Instead, the United States retained administrative control and

eventually returned the Ryukyu Islands, including the Senkaku/Diaoyu Islands, to Japanese administration in 1972.⁸ The Chinese connect the current territorial disputes to a greater historical context of past treatment by the great powers.⁹

The “Century of Humiliation” is a powerful narrative in Chinese modern culture invoking nationalism and strong emotions against the great powers. China’s agitation and protests over Japanese textbooks that China feels underemphasize war atrocities and official ceremonies at the Yasukuni Shrine, where individuals convicted of war crimes by the International Military Tribunal of the Far East are enshrined, reinforce and exemplify these deep-seated historical grievances.¹⁰

Nationalism builds a strong narrative in China’s domestic views toward the dispute.¹¹ As Japan’s relative economic power declines and China experiences a surge in patriotism with its newfound economic strength, the narrative of the disputed islands increasingly has become one of national pride and just restoration of what rightfully belongs to China.¹² Elite power struggles within the Chinese Communist Party, a slowing of the economy, or Japanese actions undermining the legitimacy of the current rulers could increase the sense of nationalism among the Chinese population or even cause China’s political leaders to promote anti-Japanese sentiment to deflect attention from domestic political rancor.¹³ This sense of nationalism reduces China’s political flexibility in de-escalating or resolving the dispute and may promote inflammatory rhetoric aimed at placating China’s domestic audience at the risk of sending undesirable signals to the international audience.¹⁴

National security is also a significant factor in China’s approach to the dispute. The U.S. alliance system along the First Island Chain stretching from Japan to Taiwan to the Philippines,¹⁵ and arguably as far as Australia with proposed American basing initiatives, serves as a de facto line of containment using an offshore control strategy. While this strategy seems defensive in nature from the U.S. perspective, it directly threatens

China’s economic survival by giving the United States the ability to readily interdict China’s shipping.¹⁶ Strategically, China would want to prevent total containment¹⁷ within the First Island Chain and ensure access to its self-proclaimed exclusive economic zone. In these terms, China’s desire to exert sovereignty over the Senkaku/Diaoyu Islands can be viewed as a natural defensive strategy to protect shipping lanes supporting China’s energy and economic interests. Additionally, China has established a pattern of using military force as a means of signaling in its offshore territorial disputes.¹⁸ This pattern of aggressive military signaling increases the potential for incident and conflict.

In understanding the historic context, the strong narrative of nationalism, and the military framing of the dispute, the United States can work toward several opportunities for de-escalation. Foremost, it is essential that the United States maintain a strong alliance with Japan to persuade it from developing a more aggressive national defense force or a nuclear deterrent. Additionally, the United States should continue a policy of strategic ambiguity over the disputed territory and encourage China and Japan to leave the disputed islands unoccupied and not pursue unilateral resource exploration and development.¹⁹ China and Japan have already initiated negotiations for energy development in areas of the East China Sea, but confrontation over the disputed islands disrupted the negotiations.²⁰

The United States could also improve regional stability by promoting joint Sino-Japanese security patrols and development of the economic resources as a means to de-escalate tensions. Joint patrolling builds trust, and joint development can work to decouple use of the resources from the issue of sovereignty.²¹ China established precedence for joint development vis-à-vis a 2004 agreement for energy exploration in the South China Sea with the Philippines. Although the joint exploration project failed to produce results and was eventually discontinued, it demonstrated the potential of joint development initiatives as opportunities for de-escalation.²² Additionally, a narrative

constructed from joint cooperation can work to assuage a small portion of the anti-Japanese sentiment in China.

The United States can also help China and Japan establish bilateral institutions to serve as a mechanism to resolve disputes. For example, a joint Sino-Japanese commission active from 2006 to 2010 reviewed the historic claims to the islands, enabling a shared understanding of the dispute.²³ Additionally, bilateral institutions can develop policy and establish frameworks to peacefully resolve disputes, thus eliminating the need for risky military signaling. Although China is unlikely to engage in multilateral institution-building at this time because its relative power is greatly reduced in a multilateral environment, opportunities to increase regional security cooperation through multilateral institutions such as the Association of Southeast Asian Nations Regional Forum may arise as bilateral institutions mature.²⁴

Final resolution of the dispute will take time, patience, and commitment by all parties to develop and adhere to a resolution process. In developing this process, the first step is reframing the problem from unilateral enforcement of perceived sovereignty into cooperative enforcement of international norms in accordance with the United Nations Convention on the Law of the Seas (UNCLOS). Strict adherence to international norms would not only reduce the risk of the current dispute escalating into a conflict, but also decrease uncertainty for corporations wanting to participate in joint ventures developing offshore resources.²⁵ In reframing the dispute, China and Japan can change their approach from the current win-lose dilemma into a win-win solution acceptable to both countries.

By understanding China’s perspectives, motives, and approaches to resolving the Senkaku/Diaoyu Islands dispute, the United States can help “create a context in which [China and Japan] can choose to construct a mutually acceptable framework of common practice in the East China Sea.”²⁶ It is in U.S. strategic interests to promote regional stability, maintain strong Asia-Pacific



Aerial Photo of Kita-Kojima (left) and Minami-Kojima of Senkaku Islands, Ishigaki City, Okinawa, Japan (Courtesy National Land Image Information)

alliances, safeguard international shipping lanes, and ensure access to energy resources. The United States is in a unique position to de-escalate the dispute by encouraging China and Japan to institute joint patrols, joint resource development, bilateral institutions, and adherence to UNCLOS norms. If managed carefully, the United States could assist in de-escalating the Sino-Japanese dispute while simultaneously building a stronger diplomatic relationship based on strategic cooperation between Washington and Beijing.²⁷ JFQ

Notes

¹ Tim Giannuzzi, "Three Boats Making Waves in East China Sea," *The Calgary Herald*, September 16, 2010.

² Mure Dickie, "Beijing Attacks Deal to Buy Disputed Senkaku Islands," *Financial Times*, September 11, 2012; "China Sends Warships after Japan Announces Purchase of

Disputed Senkaku Islands," *Asian News International*, September 11, 2012.

³ Shihoko Goto, "Introduction," in *Clash of National Identities: China, Japan, and the East China Sea Territorial Dispute*, ed. Tatsushi Arai, Shihoko Goto, and Zheng Wang, 5 (Washington, DC: Wilson Center, 2013), available at <www.wilsoncenter.org/sites/default/files/asia_china_seas_web.pdf>.

⁴ Marianne Lavelle and Jeff Smith, "Why are China and Japan Sparring over Eight Tiny, Uninhabited Islands?" *National Geographic News (Online)*, October 26, 2012, available at <<http://news.nationalgeographic.com/news/energy/2012/10/121026-east-china-sea-dispute/>>.

⁵ Paul J. Smith, "The Senkaku/Diaoyu Island Controversy," *Naval War College Review* 66, no. 2 (Spring 2013), 27–44.

⁶ Ronald O'Rourke, *Maritime Territorial and Exclusive Economic Zone (EEZ) Disputes Involving China: Issues for Congress*, R42784 (Washington, DC: Congressional Research Service, December 10, 2012), 27–30.

⁷ Ibid., ii.

⁸ Daqing Yang, "History: From Dispute to Dialogue," in *Clash of National Identities*, 22–24.

⁹ Zheng Wang, "Perception Gaps, Identity Clashes," in *Clash of National Identities*, 14.

¹⁰ James J. Przystup, *Japan-China Relations 2005–2010: Managing Between a Rock and a Hard Place, An Interpretative Essay*, INSS Strategic Perspectives, No. 12 (Washington, DC: NDU Press, October 2012), 4.

¹¹ Thomas J. Bickford, Heidi A. Holtz, and Frederick Vellucci, Jr., *Uncertain Waters: Thinking About China's Emergence as a Maritime Power* (Washington, DC: Center for Naval Analyses, September 2011), 56.

¹² Goto, 6.

¹³ M. Taylor Fravel, "The Dangerous Math of Chinese Island Disputes: If History Is Any Guide, There's a Real Risk Beijing Will Use Force Against Japan Over the Senkakus," *Wall Street Journal (Online)*, October 28, 2012.

¹⁴ Jessica Chen Weiss, "Powerful Patriots: Nationalism, Diplomacy, and the Strategic Logic of Anti-foreign Protest" (Ph.D. diss., University of California at San Diego, 2008), 13.

¹⁵ Bickford, Holtz, and Vellucci, 15.

¹⁶ T.X. Hammes, *Offshore Control: A Proposed Strategy for an Unlikely Conflict*, Strategic Forum, No. 278 (Washington, DC: NDU Press, June 2012), 5.

¹⁷ Bickford, Holtz, and Vellucci, 74–75.

¹⁸ Fravel.

¹⁹ Shinju Fujihira, "Can Japanese Democracy Cope with China's Rise?" in *Clash of National Identities*, 44.

²⁰ Przystup, 18–19.

²¹ Tatsushi Arai, "Transforming the Territorial Dispute in the East China Sea: A Systems Approach," in *Clash of National Identities*, 93.

²² Phillip C. Saunders, "China's Role in Asia," in *International Relations of Asia*, ed. David Shambaugh and Michael Yahuda, 2nd ed. (Lanham, MD: Rowman and Littlefield, 2014), 10.

²³ Yang, 26.

²⁴ Akihiko Kimijima, "From Power Politics to Common Security: The Asia Pacific's Roadmap to Peace," in *Clash of National Identities*, 62–64.

²⁵ O'Rourke, 52.

²⁶ Akio Takahara, "Putting the Senkaku Dispute into Pandora's Box: Toward a '2013 Consensus,'" in *Clash of National Identities*, 77.

²⁷ Phillip C. Saunders, *The Rebalance to Asia: U.S.-China Relations and Regional Security*, Strategic Forum, No. 281 (Washington, DC: NDU Press, August 2013), 10.



Cyber Security as a Field of Military Education and Study

By Eneken Tikk-Ringas, Mika Kerttunen, and Christopher Spirito

Information and communication technologies are acknowledged as enablers and the core arsenal of military capabilities, functions, and operations.¹ An increasing number of nations pursue improved fluency and agility of armed forces personnel in information and communication technology, its contemporary uses, and relevant defense and security implications. Underdeveloped terminology and

concepts, combined with recognized functional needs and national ambitions to control the relatively new battlespace and domain, create ambiguity and even anxiety among the current generation of planners and leaders. Particularly challenging is the balance between technical in-depth knowledge requirements and strategic understanding of the cyber domain desirable for joint planners, field commanders, and senior decisionmakers.

Several conceptual and practical questions must be resolved by military education institutions through cyber security and defense as a field of study and education. Based on empirical observations on joint and senior-level education, this article addresses the problems of conceptual confusion and contextual diversity in military cyber education.² It offers views on curriculum development and tentative ways to address the problems and develop both content and methods of education with emphasis on officer career courses at military academies and defense and war colleges.

Dr. Eneken Tikk-Ringas is a Senior Fellow for Cyber Security at the International Institute for Strategic Studies—Middle East. Dr. Mika Kerttunen is the Director of the Department of Leadership at the Baltic Defence College. Christopher Spirito is the International Cyber Lead at The MITRE Corporation.

Key Problems

Students and decisionmakers find it difficult to understand the term *cyber*. Cyber security and defense referring to and dealing with tangible concepts such as computers, networks, and information assurance are understandable; however, alternatively *cyber* is used to cover anything based on Internet protocol (IP) traffic, comprising the users as part of the definition, or being coterminous with electricity or electromagnetic spectrum.³

The essence of education easily remains blurred as key concepts are either undefined or incommensurably defined by different epistemic communities or administrative entities. One only need ask: what is the relation of “cyber security” and “cyber defense”; how does a “cyber attack” relate to “cyber warfare”; or does “cyber war” actually mean anything, or is it an intentionally constructed flickering illusion?⁴ Indeed, it remains to be seen if *cyber* as a term survives or will be rejected over time, not least because of the conceptual confusion that remains even within Western countries as to what it means.

Terminological and conceptual confusion is aggravated by the lack of taxonomy and missing links between allied and national doctrines. One need also critically examine whether or which 2,000-, 200-, or 20-year-old theories of war and operational concepts translate into the age of information and precision. Clausewitzian concepts such as hatred, center of gravity, or the superiority of defense over offense might appear different, even outdated, in the cyber era and space. Contemporary armed forces need to possess situational awareness beyond their immediate tasks and duties. For example, the Schmitt test to determine if an incident meets the threshold of use of force or armed attack requires competence often not belonging to an officer’s area of expertise or available within and from the domain immediately under their command.⁵ The speed and stealth of cyber maneuvers and effects intensify the presented challenges.

These inconsistencies make it difficult to make officer cohorts understand cyber as a concept and address it in a constructive manner, yet they should not be seen

as diminishing the need to grasp the role of advanced technology in the current and future role of armed forces. Any contemporary operation or mission and up-to-date combat, combat support, and combat support service function is likely to involve cyber components or capabilities and therefore require a fundamental understanding of technology and a developed understanding of its use.

Right now, the level of awareness of cyber as an environment and as a tool typically is low among the audience, making it difficult to introduce more sophisticated and complex issues and to design far-reaching education and training strategies. However, it must be noted that the lack of general understanding is a generational issue, and the problem of current leadership not having proficiency in or even a basic understanding of the cyber domain should be to some extent resolved within the next decade.

National requirements sent to cyber warriors and cyber-savvy officers vary from country to country. Usually in smaller countries, officers are educated as generalists expected to cover broad fields of expertise during their service. They are often required to perform functions up to two levels above their rank. Similarly, national and cultural values and habits are reflected in command and control and leadership functions. One only needs to compare the Nordic interpretation of mission command emphasizing the independence of the subordinate to the U.S. Army interpretation focusing on the control aspect to realize the different educational preferences.⁶ The diverse background of joint or international officer courses and varying levels of prior knowledge of students further underline the educational and conceptual challenge of creating lectures and discussions to match the requirements and target audience’s justified expectations.

In leader education, the questions of autonomous decisionmaking and independent thinking and action are paramount. Since the cyber domain and cyber operations require agility, adaptability, and creative and critical thinking, students with a common military mentality and an expectation of clear concepts, templates,

and orders-based execution that previously served them well may find they are not thinking out of the box but operating out of their comfort zone.⁷

Observations on Curricula

Comprehensive cyber defense and cyber security curricula for military education are still works in progress. Many professional military educational institutions tend to offer either tactical/technical (information assurance and security) or strategic/conceptual (policy and doctrine) level training and education, whereas joint and operational studies remain in the background as difficult to compile and deliver.⁸

However, understanding available cyber capabilities and assets and their potential use as well as threats is essential for service and joint level staff officers and commanders. Officers, regardless of their rank or position, must be able to assess their operational environments from a cyber perspective and be aware of the basic platforms and cyber capabilities. Field commanders are required to actively pursue cyber options in their missions and within their area of operations. They need to understand how to deliver a cyber effect and know the potential political and legal consequences of the decisions and actions—for example, wiping out all local communications—and especially relating to third party infrastructure. Commanders must be able to estimate when it is safe to assume or accept a cyber risk. Without such a skill, officer students cannot qualify as commanders, planners, or decisionmakers. Furthermore, it is important to be able to implement footprint control—that is, to assess electronic exhaust and determine how much one leaves behind or gives away. Commanders need to ask about IP security, patching, or radio frequency identification attacks against their own systems as they need to be aware of casualties, consumption, or morale. Joint and senior level cyber curricula must discuss appropriate levels of decisionmaking. This discussion of responsibilities and cyber rules of engagement easily returns to a conceptual jargon-talk; thus, tangible field examples must be found or developed.

Elements and aspects of cyber security and defense form an important part of higher level education. “Cyber capabilities and their use in war and peacekeeping” and “planning the use of cyber capabilities” should constitute the core themes of any joint and senior level officer course. Recognizing mutual spectrum co-dependency in a conflict provides two parallel perspectives on cyber operations that officers must grasp: how to defend against attacks and how to exploit spectrum dependency to execute attacks.⁹

Currently, due to the lack of prior systematic cyber security and defense education, the joint and senior level audience is often required to work through weeks of learning and study material in a few days or even hours. However, it could be estimated that to combine the required cadet, service, joint, and strategic level studies, cyber security and defense themes would easily add up to 5 to 6 weeks of intensive studies.¹⁰ Any curricular planning should therefore focus on the full cycle of officer education rather than attempt to revisit the same items at all level of studies.

The Baltic Defence College’s model reference curriculum on cyber security and cyber defense forms a matrix between the four levels of officer education—cadet/junior officer, intermediate/service, joint operational, and senior—and four identified interdisciplinary core study areas—fundamentals, capabilities, operations, and additional aspects—that seek to logically proceed from general to specific and from academic to military. At the first level of studies—cadet/junior officer education—the emphasis is on basic technical and scientific foundations and basic cyber hygiene as well as the individual contribution to cyber security and defense. At the service/joint operational levels, the emphasis is on service-specific and joint capabilities and the planning for and use of those capabilities in operations. At the senior level, strategy and policy formulation, international relations, diplomacy, and campaign design will be more thoroughly addressed. The reference curriculum is hoped to provide developed understanding of training and education needs as well as a solid



Soldier connects with call manager during Cyber Endeavor, annual exercise designed for multinational operations in European theater (U.S. Army/Shawnon Lott)

foundation to develop a handbook on cyber defense.

Separating cyber as an area of studies should be seen as an interim solution on the way to treating the cyber domain and information and communication technologies as an essential and omnipresent aspect of all operations and functions. To create full cyber awareness, it is of utmost importance not to treat cyber themes as a separate area or discipline that one can enter and leave. As incoming students gradually become more competent and confident, more demanding and specific cyber security and cyber defense topics can be introduced into the curricula.

Educational Ways Forward

A simple solution to the above-described problem of basic computer and Internet illiteracy is to include competency tests and selected readings before lecture sessions. To create technical competency and make students comfortable with the domain, it would also be beneficial to have hands-on, engaging, and “fun-tech” courses before or between other classes. It is also preferable to decisively show what is gained from each element of study and how it is tied to particular requirements an officer actually needs to know, understand, and do.

To make cyber security and cyber defense more concrete and understandable, identifying relevant capabilities at small unit, larger brigade, air wing or corps size formations, and national levels is helpful. Investigating how these capabilities have been or can be used in the core functions of military operations such as command and control, intelligence, maneuver, interdiction, targeting and fire, logistics, and sustainment makes students comprehend cyber as an omnipresent and essential aspect.

Cyber defense and military cyber security need to be outlined in the context of the full spectrum of cyber security concerns reaching from basic cyber hygiene to civil-military cooperation and cyber diplomacy without overstressing the proportion of it. National strategies and service doctrines can be analyzed, compared, and critically scrutinized to understand different political and bureaucratic frameworks and factors and to appreciate different views and solutions to cyber operations and capabilities. Such an approach would integrate the notion of cyber to essential, concrete, and familiar concepts and practices; conceptual themes would become real and hopefully better appreciated and acknowledged.

We also advise distinguishing non-organic, reach-out cyber capabilities

such as advanced intelligence from integrated, organic capabilities. Naturally, the focus and levels of learning at officer courses differ from those at technical and specialist courses. Whereas the latter focus is on hands-on, in-depth technical and tactical skills, officer education particularly at joint and senior levels aims to develop understanding of concepts, knowledge of the use of cyber capabilities in military operations, and the ability to design and define strategies, policies, and future capabilities.

A culture and mindset of reporting and individual responsibility similar to organic or delegated resources need to be created within cyber operations. Questions such as “what constitutes cyber in war?” and “who is considered a cyber warrior with what responsibilities in a particular organization and organizational culture?” must be addressed when preparing the curriculum.

Investigation of known incidents and modi operandi enables one to combine conceptual issues to real capabilities and operations; this will increase motivation to learn. There is a demand for well-researched, theoretically anchored, and thoroughly documented cyber case studies. Loose references to “Estonia,” “Georgia,” or “Stuxnet” that only support individual prejudice or organizational bias are not hallmarks of high-quality education.¹¹ Alongside truthful, credible accounts of the attacks and operations, speculative *what if* and normative *what should* questions both test students’ competence and take discussions further. In this context, the demanding issue of civil-military roles, responsibilities, and interaction in the cyber domain can be addressed.¹²

There is a pressing need for comprehensive, well-referenced study materials to comprise the essentials of all levels of study and provide links to existing materials, concepts, and discourse. Such materials should link the concepts of cyber security and cyber defense to military theories and, more importantly, operationalize the theories, ideas, and concepts according to strategic, operational, and tactical levels and service and joint functions and operations.

It is plausible to conclude that officer cyber education must address and depart from the principal debates within cyber defense discourse. First is the education debate between a narrower focus of protecting and enabling one’s own networks and network-based service and a wider interpretation, recognizing cyber as an asset by using those networks and services also to deliberately cause, enforce, and project hostile cyber effect on the adversary’s systems and networks. Second, officer education needs to deal with the diverging views of the cyber element as an integral aspect or a separate function. As pointed out, demands of understanding and awareness of cyber concepts, capabilities, and threats do not fundamentally differ from the cognitive and educational requirements of mastering other operating environments, capabilities, and effects. Third, the interrelated roles and responsibilities between individuals, armed forces, and civilian society, including the private sector, must be examined and understood. Addressing these three debated and most practical areas would help to clear the terminological and conceptual fog of cyber as well as broaden and deepen understanding of cyberspace and the use of cyber capabilities. Finally, grasping cyber requires a broad set of educational methods. To be able to provide hands-on experience, thought-provoking readings and lectures, group discussions, debates, and exercises in which conceptual knowledge can be applied demands due consideration by military educational institutions of investments into the skills and competence of their directing staffs. Understanding the multifaceted nature of cyber security and defense and the broad requirements it sets for any military officer is the first step forward. JFQ

Notes

¹ See, for example, General Sir Nick Houghton observing that the British armed forces are critically deficient in the capabilities that enable the joint force, including intelligence, surveillance, and compatible communications. Richard Norton-Taylor, “Defence chief: UK armed forces have good equipment but not enough people,” *The Guardian*, December 18, 2013, available at <www.theguardian.com/politics/2013/dec/18/defence-chief-uk-armed-forces-equipment-nick-houghton>.

Our experience and observations are based on designing and implementing information assurance and cyber security and defense courses, modules, and workshops for joint and senior level officer and civil servant courses as well as for targeted national authorities and external customers in the Nordic-Baltic region, Gulf region, and the United States.

² The use of the term *cyber* derives from U.S. diplomatic culture and has been implemented into U.S. military doctrine as a domain control ambition involving nonstate actors as potential adversaries and targets. In contrast, North Atlantic Treaty Organization (NATO) doctrine restricts the use of *cyber* to protection of networks and strategic information assurance. See NATO, “Defending the Networks: The NATO Policy on Cyber Defense,” 2011, available at <www.nato.int/nato_static/assets/pdf/pdf_2011_09/20111004_110914-policy-cyberdefense.pdf>.

³ See, for example, Martin C. Libicki, “Don’t Buy the Cyberhype: How to Prevent Cyberwars from Becoming Real Ones,” *Foreign Affairs*, August 14, 2013, available at <www.foreignaffairs.com/articles/139819/martin-c-libicki/dont-buy-the-cyberhype>.

⁴ Michael N. Schmitt, “Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework,” *Columbia Journal of Transnational Law* 37 (1998/1999), 890–937.

⁵ On the concepts of mission command and command and control, see, for example, Field Manual 6-0, *Mission Command: Command and Control of Army Forces* (Washington, DC: Headquarters Department of the Army, 2003); and Marine Corps Doctrinal Publication 6, *Command and Control* (Washington, DC: Headquarters Department of the Navy, 1996).

⁶ On the cognitive and intellectual challenges at joint and senior level officer education, see, for example, Joan Johnson-Freese, *Educating America’s Military* (London: Routledge, 2013).

⁷ Observations based on study visits to several U.S. and all Nordic defense and war colleges.

⁸ James P. Farwell and Rafal Rohozinski, “The New Reality of Cyber War,” *Survival* 54, no. 4 (August–September 2012), 107–120.

⁹ An estimate based on the work on the Reference Curriculum on Cyber Security and Defense to be mentioned later.

¹⁰ On the demands of proper case study methodology, see Robert K. Yin, *Case Study Research: Design and Methods* (London: Sage, 2014).

¹¹ As examples of national cyber security strategies emphasizing interagency cooperation, see *The National Cyber Security Strategy* (The Hague: Ministry of Security and Justice, 2011); and *Finland’s Cyber Security Strategy* (Helsinki: Secretariat of the Security Committee, January 24, 2013).



Why Military Officers Should Study Political Economy

By Rebecca Patterson and Jodi Vittori

Colonel: Afghanistan may have one trillion dollars' worth of minerals! This is great for Afghanistan!

Staff Officer: Sir, we need to talk. . . .

Lieutenant Colonel Rebecca Patterson, USA, is an Assistant Professor in the College of International Security Affairs at the National Defense University (NDU). Lieutenant Colonel Jodi Vittori, USAF, Ph.D., is a Policy Adviser for Global Witness, a nongovernmental, not-for-profit organization that focuses on the nexus of natural resources, corruption, and conflict. She is also an Adjunct Professor at NDU.

The exchange above paraphrases a typical conversation between most military officers and those with a background in political economy and economic development. Conventional wisdom would suggest that mineral-rich states such as Afghanistan have great development potential; after all, government

revenue from the development of natural resources should pay for social services and poverty reduction, as well as salaries for government employees (including security forces). This could in turn improve security, quell various illicit power structures, and solve the variety of grievances that help stoke and perpetuate conflict.

Officers with an economics background, however, know differently; other issues are at play. First, there is the likelihood of the “resource curse,” the contention that states lacking in rule of law and stable institutions are more susceptible to various forms of nonstate violence and have low levels of economic and political development while their elites and institutions are more likely to engage in rentier behavior. Second, development generally is a multigenerational undertaking. The average state takes 40 years to graduate from low-income status to low-middle-income status—a timeline well beyond the interest of most external powers currently involved in Afghanistan, for example.

These insights and other political economy concepts are vital for military officers to comprehend if they are to understand the context of the wars they engage in. The concepts are equally critical to the development of postconflict military strategies targeting recovery. This article argues that today’s military officers could be at a disadvantage for the types of wars they are currently fighting and are likely to face in the future. There is much new research that pertains to the intersection of politics and economics and their role in conflict, especially in fragile states, but little of this has trickled down to most military officers. At the same time, military officers are far more involved in the economic and political development of failed and fragile states than in previous decades. They have been given new economic tools with which to “fight” counterinsurgency and promote stability but have received little information or education on how to use these tools. At best, the result has been poorly allocated money and missed political and economic opportunities. At worst, U.S. military officers have inadvertently helped delegitimize governments, increased the instability in already conflict-prone places, and helped put such states on the path to yet another cycle of violence.

It is not that military officers are indifferent to political and economic issues in warfare. Military officers have had a long history of involvement in economic issues, especially in what are now termed

“stabilization operations” in postconflict environments. The most illustrious example is perhaps General George Marshall, who, as Secretary of State, devised the European Recovery Program. The so-called Marshall Plan was largely credited with bolstering using economic aid friendly Western European governments in the face of mass protests and a rising tide of leftist groups. Likewise, General Douglas MacArthur adroitly addressed issues of political economy in recrafting Japanese institutions after World War II. Similarly, some of today’s generals display impressive acumen when it comes to economic and political effects of strategic policies. General Stanley McChrystal argued that corruption within the Afghan government was an important concern in his astute review of the conduct of the Afghan war in 2009. His successor, General David Petraeus, published specific rules governing the conduct of contracting in a counterinsurgency environment, recognizing how U.S. and North Atlantic Treaty Organization (NATO) contract spending could inadvertently delegitimize stability efforts in Afghanistan. These commanders understood that hard-power capabilities are beneficial but have their limits—an important realization when creating long-term stability plans for conflict zones.

President Barack Obama highlighted these issues in his 2013 counterterrorism strategy, stating that by “addressing underlying grievances and conflicts that feed extremism,” the United States could best “reduce the chances of large-scale attacks on the homeland and mitigate threats to Americans overseas,” accomplishing the goal of political stability and security more effectively than by employing additional troops.¹ Transitioning from a security focus to a development focus, in the words of General Petraeus, “reset the conditions for progress,”² namely promoting economic development and reducing corruption as two target areas for U.S. support. Most academic evidence supports the connection between terrorism, some criminal activity, and underdevelopment. According to the Organisation for Economic Co-operation and Development, terrorism “comes

from hatred born of exclusion, ignorance and prejudice, injustice and alienation, feelings of hopelessness and despair,”³ which are then “exploited” by terrorist leaders and organizations. Thus, while development does not address the immediate security threats posed by these groups, tackling issues such as poverty, education, health care, and other social services “deprive[s] terrorists of popular support, addressing the conditions terrorist leaders feed on”⁴ to maintain their credibility with the local population.

Nevertheless, most military officers display a lack of knowledge about political economy, economic and political development, and corruption. This is at the same time that officers are empowered with a host of monetary and contracting tools to ostensibly use as economic levers of power. For instance, findings based on various economic models and some limited studies argue that unemployment is an important cause of violence and conflict, as being unemployed lowers the opportunity costs of choosing to join a rebellion versus seeking gainful employment, especially in an area with a shortage of jobs.⁵ Likewise, Radha Iyengar, Jonathan Monten, and Matthew Hanson found that in postconflict Iraq, a 10 percent increase in labor-related spending generated a 15 to 20 percent decline in labor-intensive insurgent violence, suggesting that labor-intensive programs can reduce violence during insurgencies. As a result, commanders were given new tools with which to hopefully de-incentivize insurgents from taking up arms against coalition forces and host governments through various economic assistance programs.⁶

Commanders were also tasked to assist the host government in addressing grievances of the population with the belief that doing so would legitimize the government, thus gaining the public’s gratitude and support. According to Field Manual (FM) 3-24, *Counterinsurgency*:

The U.S. military has increasingly used development projects as a strategic weapon to fight ongoing counterinsurgency efforts in Afghanistan, Iraq, and other theaters. The approach is predicated on a hypothesis that

*such projects—which are commonly implemented by the domestic government and allied entities and deliver basic services and infrastructure—can improve economic outcomes, build support for the government, and ultimately reduce violence as sympathies for the insurgency wane.*⁷

As evidenced by its prominence in FM 3-24, the hypothesis now constitutes a major component of current U.S. counterinsurgency doctrine. Despite the ongoing application of the strategy, there is limited empirical evidence on the effectiveness of development projects in countering insurgencies.⁸ Informed by doctrine developed to address communist or anti-colonialist revolutions, the manual concludes that the effectiveness of counterinsurgencies is strongly influenced by the nature of interactions between the domestic government, foreign forces, and the civilian population. Specifically, foreign forces can bolster the authority of the government, which is seen as a legitimate actor that represents the well-being of the state's population, but it is the government's provision of basic security and public goods that primarily determines the population's support for the insurgency.⁹

The U.S. counterinsurgency plan, therefore, was to use “money as a weapons system.” In Iraq and Afghanistan, commanders were given special authorities to fund projects both to hire locals—especially military-aged males—and to address grievances through the provision of economic assistance. The idea was that economic assistance could be used as a type of weapon, legitimizing the host government, buying the support of the local populace, and delegitimizing the insurgent forces that could not outspend or outgovern the host government.

The foremost military spending tool was the Commander's Emergency Response Program (CERP), a military fund controlled by the Department of Defense (DOD) that allowed commanders discretion in using money toward reconstruction projects that could “immediately assist the indigenous population and that the local population or government can sustain.”¹⁰ The ideal

project for CERP funding would be quickly executable, employ and benefit the local populace, and be highly visible, including target development areas such as transportation, sanitation, education, irrigation/agriculture, telecommunications, civic works, and health care. The genesis of the program was the seizure by U.S. forces of approximately \$900 million from various locations during the invasion of Iraq. The funds were then used for various reconstruction projects, although DOD later contributed additional funds to sustain CERP over the years going forward.

Although CERP began as a program to build and repair the social and material infrastructure of Iraq, it grew into the Defense Department's flagship reconstruction program, receiving more than \$3.8 billion in U.S. appropriations by the end of 2010.¹¹ CERP made it possible for U.S. commanders to improve life by quickly repairing roads and bridges, rebuilding schools, improving health care, and removing trash. The program came to play an important and high-profile role in U.S. counterinsurgency efforts in both Iraq and Afghanistan. Much of this economic aid was disbursed by battlespace commanders, often with input from members of Provincial Reconstruction Teams (PRTs).

Provincial Reconstruction Teams were initially formulated by the Coalition Joint Civil-Military Task Force in 2002, intended for noncombat reconstruction efforts in Afghanistan, based on the work of earlier Civil Affairs teams. Their initial mission was to strengthen the capacity of the Afghan National Security Forces while also providing humanitarian assistance, undertaking reconstruction, and maintaining local governance.¹² The success of the teams in Afghanistan led to their expansion to Iraq, where the intent was to transition the lines of operation of governance and economics at the provincial level from the military to the PRTs, tasking these groups with developing the political and economic environment within each province.¹³

Over time, CERP has been widely criticized, specifically for its enormous bureaucratic process (the new standard

operating procedure is 165 pages) and over doubts about its effectiveness.¹⁴ But the provision of economic aid by the U.S. military in general has been controversial for a number of other reasons. First, development experts have been concerned that neutral aid agencies might be associated with the military forces that also distribute aid or be seen as a subset of military efforts. This could taint the neutrality of many aid agencies and put their missions and members' lives in danger. Second, military commanders rarely have had an economics background, thus having neither the understanding of best practices for disbursing aid nor much knowledge of the local environment. Third, there was an overall lack of coordination among the various international donors, especially in Afghanistan. The military and aid fields were rife with stories of poorly designed or coordinated projects; villages might be the recipients of multiple schools within a small area, for instance, but no teachers or other resources would be assigned to staff and maintain them.

Compounding this criticism and controversy was the U.S. counterinsurgency strategy of *clear-hold-build*, a strategy in which security forces retake a geographical area from insurgent control and win public loyalty while securing the territory from further insurgent attacks. As defined by the U.S. Army, this strategy encompasses information warfare, civil-military operations, and combat operations; the end goal is for local police to maintain the authority established by the armed forces.¹⁵ This strategy highlights the use of indigenous forces, who are especially knowledgeable about the local terrain and who will ultimately maintain security in contested areas. The efficacy of using indigenous forces, particularly in the challenging tasks of holding and building, quickly became apparent.

The dilemmas presented by using economic aid as a stabilization tool are many, and which strategy is the most effective remains an open question. Many argue that aid should only be provided in the more secure areas, both as a reward to that populace for its loyalty to the government and as a demonstration of

the benefits of working with the host government, as opposed to largely siding with insurgent or criminal elements. Aid was often distributed in more insecure areas, however. The premise for the first attempt, made in Marjah, Helmand Province, Afghanistan, in the winter and spring of 2010, was that the area would be cleared of Taliban and then a “government-in-a-box” would arrive. In theory, the surge of civilian governance achieved by immediate provision of services at the local level by said government would demonstrate to the local population both government legitimacy and effectiveness. Unfortunately, the security situation was never as stable as hoped; what little service provision did occur happened in a highly insecure environment. The Afghan government never deployed the so-called government-in-a-box, and there was always a lack of competent Afghan government workers willing to deploy to that area. The result was that aid agencies found the area too insecure to operate in, the Afghan government largely failed to provide services, and the U.S. military was left to provide much of the aid and oversight.

Afghanistan is especially unique because it is the only locale where DOD is authorized to disburse State Department funds. As a result, DOD controlled a substantial budget for “development.” One example is the Afghanistan Infrastructure Fund, a \$400 million fund (usually provided on an annual basis) approved by Congress for large-scale infrastructure development projects, including restoring power supplies and building large-scale roads.¹⁶ Another example is the Afghanistan Security Forces Fund, which uses funds to train Afghan police as part of the clear-hold-build campaign, charging these forces with maintaining security particularly around infrastructure projects.¹⁷ These funds were used not only for small-time projects like those of CERP but also for massive infrastructure projects like the 2010 Salang Tunnel restoration project.

In September 2009, as a part of Operation *Mountain Blade*, DOD contributed \$12.1 million in CERP funds to the U.S. Agency for International

Development (USAID) for construction of the Ring Road because it was deemed a “vital economic trade link” and a “key component to stability and unity in Afghanistan.”¹⁸ As a result, a trend that began in Iraq expanded exponentially in Afghanistan. Whereas economic development used to be the role of organizations such as USAID, various nongovernmental organizations (NGOs), and intergovernmental organizations such as development banks, the U.S. military had an increased role in deciding on projects and disbursements. In 2010, \$154 billion (with \$1.2 billion in CERP funding alone) in overall war funding was provided to DOD, compared to the \$9 billion given to the State Department and USAID.¹⁹ From 2001 to 2011, DOD spent \$757 billion in Iraq and \$416 billion in Afghanistan, while the State Department did not even match a quarter of that spending.²⁰

The U.S. military was engaged in everything from small local projects to major infrastructure projects. Given the poor security situation, military members also increasingly found themselves serving an advisory role to district and provincial governments and in a host of national-level ministries. Initiatives such as the Afghan Hands Program, which sought to use military members with some additional language, history, and counterinsurgency training who would then be “placed in strategic positions where they can make an immediate impact,”²¹ were tasked not only to PRTs but also to a variety of nonsecurity ministries such as the Ministry of Mines, Ministry of Finance, and Ministry of Power and Water. While one of their roles was to act as a vital liaison and information conduit between NATO forces and these ministries, their other role was to provide technical assistance to those ministries.

With the expansion of military tools such as money as a weapons system, CERP funds, and the increase in military personnel assigned to advisory positions to indigenous government institutions, the need for adeptness at political and economic concerns has ballooned. The result has also been a military whose success in terms of campaign outcomes

is greatly tied to economic and development issues from the tactical through the strategic levels. Military leaders were often major decisionmakers on multi-billion-dollar infrastructure projects, not only for the security issues that would come with them but also from a governance perspective. The more the military realized the connection between a sustainable economy and security, the more it felt it had to be involved in economic development.

Recent Research

Even as military leaders are increasingly involved in economic development, most are unaware of the cutting-edge research that challenges the way the military has approached the wars in Afghanistan and Iraq. Furthermore, such research provides important insights as well as potential tools. A great deal of research that addresses the intersection of economics and contemporary conflict has emerged in the last decade. What follows is a synopsis of such research.

For decades, the study of rebellion and insurgency largely focused on the role of grievance in fostering the conditions for rebellion. Notable scholars such as Ted Robert Gurr argued that perceptions of relative deprivation, ethnic or racial exclusion, and disparities in wealth were cited as primary reasons for rebellion.²² The underlying assumption that internal rebellions are grievance-based led to the creation of U.S. military doctrine that focused its members on bolstering host government capabilities, in particular to deliver services. Another significant assumption made in current U.S. counterinsurgency and stability doctrine has been that a host government in a stabilization, conflict, or postconflict environment has a desire to legitimize itself and merely lacks the tools, capacity, and resources to bring good governance to its people and sufficiently solve their grievances. Not only has this been the focus of counterinsurgency and stabilization doctrine, but it has also largely been the assumption implicit in much of the overall economic development discipline.

While we do not discount the importance of grievance in fostering rebellion, lessons from various military interventions as well as recent economic research point to additional causes of rebellion. One of these has been the role of opportunity in rebellion, sometimes described as “greed.” The greed theory of conflict asserts that actors who resort to violence (insurgents, for example) are motivated by personal economic gain and seek to appropriate material resources controlled by the government.²³ In this framework, powerbrokers fight not necessarily to alleviate grievances, but instead because doing so provides them with significant benefits, especially money and power. Hence, even if all grievances were alleviated by the government, rebels would still have an incentive to fight, as instability fosters their power, and indeed, a stable environment can be highly detrimental to their interests.

Subsidiary theories that focus on economics instead of political grievances include the “bargaining model” approach²⁴ and the “opportunity cost” theory of conflict.²⁵ The bargaining model builds upon the greed theory by assuming that material gain is the primary motivation for insurgent activity, but contends that violence occurs only when conflicting parties fail to negotiate a peaceful division of resources. Thus, information asymmetries, caused by power shifts among conflicting parties and/or by changes in the value of contested resources, can provoke conflict. The opportunity cost model places emphasis on the costs, rather than the benefits, of participating in conflict. This theory predicts that an increase in the income of the population raises the opportunity cost of participating in the conflict.

More recent scholarship has concentrated on the interests of governing elites, recognizing that some governing elites may have just as much interest in fostering instability as the rebels they are supposed to be fighting. Taking from Anne Krueger’s recognition of the role of rents for some governments and elites and the part institutions play in directing those rents, new scholarship has focused on the fact that some

governing elites may not necessarily have the interests of the country at heart.²⁶ Instead, as Paul Collier has noted, some countries are more akin to “survival of the fittest” rather than survival of the fittest, where the powerbrokers who can amass the largest war chests and patronage networks are best placed to run governments.²⁷ These powerbrokers focus on collecting rents for themselves and their followers. Governments are not neutral arbiters working toward the public good but instead are seeking as much benefit from the public trough as quickly as possible. Winning an election is not necessarily an opportunity to prove that one’s party and personalities are particularly adept at governing, but rather, to borrow from the title of Michela Wrong’s book, elections mean “it’s our turn to eat” for the winning coalition, with losers excluded or worse.²⁸

A few authors are particularly notable for the insights their work can provide to a wide variety of actors seeking to improve governance in the developing world and the security implications that the current regimes in the developing world exhibit. Perhaps the most noteworthy are Douglass North, John Wallis, and Barry Weingast, whose book *Violence and Social Orders* differentiates between two types of states: natural states and modern states.²⁹ Natural states limit violence by political manipulation of the economy to benefit privileged individuals, hindering economic and political development. Conversely, modern states create open access to economic and political organizations, which fosters competition and results in greater developed states both economically and politically. This book, building upon decades of work by each author in the fields of economics, democratization, and development, argues that politics and economics are iterative in governing regimes.³⁰ Unfortunately, these authors are writing exclusively for an academic audience. As such, their work is perhaps beyond the grasp of many well-educated military officers.

Fortunately, other authors do provide more accessible versions of their research. Perhaps the book most familiar to military audiences is Paul Collier’s *The Bottom*

Billion, in which he summarizes decades of his work on opportunity versus grievance in the instigation and perpetuation of conflict in an accessible manner with current, real world examples. Collier concludes that four traps keep countries poor and undeveloped: natural resources, geography, bad governance, and—most important to a military audience—conflict. The book includes recommendations for addressing these traps.

Anthropologist Robert Bates also provides an insightful examination of why some states fail while others succeed. His book *Prosperity and Violence* explores the relationship between political order and economic growth and finds that although political structures can be used for destructive ends, they are also important for ensuring the peace needed for prosperity.³¹ His follow-on book *When Things Fell Apart* examines political violence from its origins “at the top.” Instead of probing into the motivations of rebels, the book asks why governments adopt policies that impoverish their citizens by tracing political disorder to crises in public revenues.³²

In their article “Ethnicity, Insurgency, and Civil War,” David Laitin and James Fearon reject the common explanations—changes in the international environment, more ethnic or religious diversity, and more political grievances—for the increase in civil wars after the end of the Cold War.³³ Instead, they argue that the causes of civil war lie with insurgency theory—weak governments, rough terrain, large population, and access to weapons and support for the insurgency. They conclude that political opportunity is the greatest predictor of insurgencies.

Another recent book is Daron Acemoglu and James Robinson’s *Why Nations Fail*. While North, Wallis, and Weingast have argued that politics and economics are deeply intertwined in the success or failure of state institution building, Acemoglu and Robinson posit that political institutions are solely to blame and that economic success or failure is a dependent rather than an independent variable. *Why Nations Fail* argues that states are poor not because of geography or culture, but because a



U.S. Marines escort U.S. and British geologists through rugged terrain in Helmand Province to find rare minerals in attempt to boost Afghanistan's economy (U.S. Marine Corps/Christopher R. Rye)

small set of elites have organized society for their own benefit at the expense of the rest of society. Like Collier, Acemoglu and Robinson have taken years' worth of serious scholarly work and rewritten it in a manner accessible to most intelligent readers, with copious historical examples. While the book is certainly controversial, there is no doubt that at least some of the trends they describe ring very true

for officers who have worked in fragile, conflict-ridden states.

Many of the insights from these studies were compiled in the World Bank's *World Development Report 2011: Conflict, Security, and Development*. This report explicitly distills the lessons learned from the studies above, as well as copious statistical analyses and best practices from the development and conflict resolution

fields. It goes on to examine how conflict affects the politics and economics of societies, especially focusing on why most countries in significant periods of civil war or criminality today continue in cycles of violence, while those countries that have not seen conflict in decades are statistically highly unlikely to experience conflict. It concludes by offering insights into how international organizations, including military forces, can place such countries on the path of development and stronger institutions.

Many of these studies are found in the economic development, political economy, and sociology fields rather than in counterinsurgency or military history. Their focus on nation-building rather than warfighting has meant that few military scholars are familiar with these topic areas. Nevertheless, they provide significant insight into the issues military officers face today, not only as NATO transitions in Afghanistan in 2014, but also in ongoing or potential conflicts in Mali, Syria, Libya, Egypt, and even North Korea. They provide new understandings into what is fueling many ongoing conflicts and the unstable regimes that help perpetuate these situations. The studies also provide additional policy recommendations for mitigating the impact of destabilizing actors and situations. Without exposure to these fields of study, military officers are essentially creating strategy and fighting modern wars with one hand tied behind their backs.

Why Military Officers Should Study Political Economy

The military will inherently have an impact on security, governance, and economics.³⁴ Current doctrine even suggests that the military deliberately should plan to foster economic growth.³⁵ FM 3-0, *Operations*, dated February 2008, references "economics" more than 50 times including a discussion of critical factors to consider in planning.³⁶ Similarly, FM 3-24 contains guidance about the economic component of counterinsurgency as well as integrating civilian organizations into these operations. It does not, however, explain how military commanders at

the tactical, operational, or even strategic level should attempt to influence the economic development of a post-conflict society.

U.S. military officers have been given great discretion in disbursing military aid and/or planning complex reconstruction projects in Afghanistan and Iraq, but they have received little or no training. Just as with a traditional weapons system, troops well trained, resourced, and practiced on a weapon can use it to great advantage against an enemy. Conversely, troops poorly trained and resourced on a new weapons system cannot take advantage of its capabilities fully. Indeed, they may proverbially shoot themselves in the foot or be so inept that the weapon becomes a liability rather than an advantage. The concept of money as a weapons system is no different. Used well, money and the influence that comes with it have great potential. To fully realize its potential, one must understand the mechanics of the weapons system, its advantages, its disadvantages, the unwritten quirks, and the environment in which it will be operating. One must understand how money can be employed well, and conversely, how it can be employed poorly. One must understand the damage that can be done from poor employment, and how to recognize whether the money is being employed well. Risks for using money as a weapon must be understood, and risk mitigation strategies developed. Similarly, one must understand when not to use a weapon. Just because one is armed does not necessarily warrant using one's weapons. Otherwise, as witnessed in Iraq and Afghanistan, leaders at any level can find that their plans have gone horribly wrong. Worse, their prescriptions to fix problems may actually, inadvertently, make matters worse.

A number of additional tools are being developed for military leaders. For example, the United States Institute of Peace has developed handbooks for practitioners facing such environments. Many of these handbooks are co-authored by military leaders or those well versed in military issues. Other organizations such as RAND, the National Defense University, and the Command and

General Staff College Foundation have also published useful practitioner-focused handbooks.³⁷

The Asia Foundation published an excellent paper on how political settlements between elites work in conflict prone societies titled *Political Settlements: Implications for International Development Policy and Practice*.³⁸ The authors argue that actors in conflict situations create political settlements to limit the violence and disburse the rents to various powerbrokers. In such environments, there is a lack of trust, and as such, all major factions remained armed. Institutions in these countries are malleable and reflect the interests of powerbrokers rather than being independent actors or representing the national interest overall. As such, they argue that many development strategies have failed because they seek to decrease the power of the very powerbrokers that are critical to the initial political settlement. This particular paper is especially noteworthy because it provides practitioners advice on how to map the various networks that keep these actors in power, as well as strategies for marginalizing them and bringing reformist actors more to the fore.

Likewise, NGOs provide a number of resources, some of which are explicitly for security professionals. The NGO Global Witness, for instance, has long published studies on how resources affect conflict and provides practical policy recommendations. Transparency International has a London-based Defense Studies Program that trains select NATO officers before they deploy to Afghanistan. It also publishes handbooks on understanding and evaluating corruption inside defense ministries and defense industries. In October 2013, it published *Corruption and Peacekeeping: Strengthening Peacekeeping and the United Nations* for senior military leaders on how corruption affects peacekeeping operations.³⁹ A handbook is forthcoming for military officers in the field on how corruption affects stability operations and what security professionals can do to mitigate such a situation.

Fortunately, the American military has recognized that special skill sets are required in some stabilization operations

and has created a few organizations and programs to address the challenges inherent in complex operations. For instance, the Deputy Secretary of Defense established the Task Force for Business and Stability Operations in Iraq in 2006. Initially, the organization focused solely on Iraq, but over time, its mission expanded to include Afghanistan. With an eye on private sector development, the organization prioritized sustainable investment and development mining and oil in Afghanistan.

In tandem, initiatives such as Afghan First sought to bring in reputable local contractors for U.S. Government contracts in Afghanistan in the hopes of empowering new economic actors and stimulating the economy. Likewise, in 2010, Task Force Shafafiyat (the Dari and Pashto word for transparency) was created to counter rampant corruption that threatened the Afghan government and its economy as well as the legitimacy of the overall NATO mission there. In the wake of the massive Kabul Bank scandal, examining the interplay of economics and patronage networks became one of its lines of effort. Likewise, NATO established a two-star general officer position at the International Security Assistance Force, the Deputy Chief of Staff for Stability, whose responsibility was to focus on nonmilitary aspects of the campaign in Afghanistan. This included coordinating with international organizations and NGOs as well as ministries of the Afghan government such as the Ministries of Finance, Mining, Public Works, and Commerce and Industry.

Outside deployed regions, organizations such as the U.S. Army War College's Peacekeeping and Stability Operations Institute produce studies and doctrine dedicated to postconflict concerns that U.S. military personnel will likely face. Established in 1993, its focus includes peacekeeping and stability operations at both the strategic and the operational levels of war. This includes improving civil-military integration and collecting lessons learned. Likewise, the National Defense University's Center for Complex Operations works with a variety of NGOs, U.S. Government agencies,

and outside experts to bring the latest understanding and international best practices to military professionals.

A Syllabus for Further Study

While some elements of DOD have embraced the role of political economy and economic development, it is important that doctrine and education catch up with the operations that military professionals face. Some argue that the lessons learned from working in fragile and failed states will be unimportant in a post-Afghanistan U.S. military. Budget cuts and public weariness mean that the U.S. military will avoid nation-building in the future. The most recent change in national security prioritization, which orients the focus toward Asia, will likely emphasize conventional warfare, unlike the challenges faced in Afghanistan, Iraq, the Balkans, and Somalia. Nevertheless, critics seem to forget the dictum that “the enemy gets a vote.” One need only look at major ongoing conflicts to understand the role that political economy will likely play. The Arab Spring has led to sectarian strife in Syria, Egypt, and Libya. All were corrupt, relatively predatory governments, and all are increasingly operating on some form of war economy. One cannot operate in such environments or make viable military strategies without understanding the role elite powerbrokers play and how they can act as spoilers to any conflict resolution. Political economy concerns are equally important in traditional state-on-state conflict. For instance, North Korea has long been viewed through a traditional state conflict lens. However, current scholarship amplifies the role the various senior families play in maintaining the North Korean regime, as well as offering a better examination of what may occur when that regime eventually collapses. Hence, even traditional national security threats are not immune from the lessons from the recent conflicts in Afghanistan or Iraq.

Given the centrality of political economy concerns to contemporary conflict, we propose the following focus areas for military officers throughout their careers.

The first is a basic understanding of political economy, which goes beyond standard supply-and-demand curves taught in undergraduate programs. While these are important, equally important is to explicitly study the role of economics in conflict. Such an understanding should stretch beyond the more traditional study of the role of economics in fostering a military industrial complex. In many nations in which the United States has fought or will fight, there are few industrial complexes, and the official military may not be much more than a militia by another name. Hence, the political economy of conflict in developing countries should be studied as well.

Second, military officers should be schooled on the financing and resourcing of various illicit actors. These include not only insurgents, but also criminal organizations, warlords, and gangs. In particular, criminality continues to evolve. What was once considered a law enforcement problem increasingly looks like a military problem, in what some have termed a criminal insurgency. For example, in Central America and Mexico today, criminal organizations use methods and tactics akin to insurgencies, not necessarily for political gain, but to maintain their freedom of movement for material gain. Such criminal insurgencies now have violence levels and body counts that rival those of civil war or insurgency. Law enforcement agencies usually cannot cope with such crises without the assistance of military forces.⁴⁰ Our military leaders should be prepared for these contingencies.

Likewise, officers should be given a basic education in the current best practices in economic development, both on micro and macro levels. The goal is not to turn military officers into development experts—development should never become a core function of the U.S. military. Military officers should, however, be able to understand political economy issues related to development and apply those to strategy and tactics. They should also have the educational background necessary to be able to effectively coordinate with development bodies. They should understand the security ramifications of

various development strategies so that these security issues are recognized and planned for rather than responded to in a knee-jerk fashion.

In conjunction with education, doctrine must be modified to reflect the world in which our military leaders currently operate. For instance, FM 3-24 is a great handbook of the lessons learned from history for counterinsurgency operations. It is also a hallmark of cooperation between the military and academia, namely the Belfer Center at Harvard University. Its great weakness for today’s conflicts, however, is that it assumes, in a counterinsurgency, the host government wants to legitimize itself. While issues such as corruption are discussed, host governments are viewed as a situation where some corruption gets in the way of development and security. Lessons learned from a variety of developing country situations indicate that many elites, unfortunately, are not out to legitimize themselves beyond the minimum necessary and have their pocketbooks and power at heart rather than those of their nations. FM 3-24 remains silent on even the concept of such a government, and hence provides a military professional no insights on how to recognize such an environment or what to do about it. The same holds true for doctrine such as FM 3-07, *Stability Operations*, where much of the focus is on the interagency process and provides little insight into how to function in environments where the host government is predatory and highly corrupt. Such doctrine needs to be modified to ensure the lessons learned from over a decade of war are codified for the future.

Great military leaders such as George Marshall and Douglas MacArthur understood the importance of issues of political economy in their military careers. This reality is no different today. Military officers continue to be confronted with issues at the intersection of the political and the economic as they operate globally. As good stewards of American resources, further integration of these areas into military doctrine and education is required. JFQ

Notes

¹ "Remarks by the President at the National Defense University," Washington, DC, May 23, 2013, available at <www.whitehouse.gov/the-press-office/2013/05/23/remarks-president-national-defense-university>.

² David H. Petraeus, "Setting—and Capitalizing on—Conditions for Progress in Afghanistan," *Army* (October 2010), available at <www.ausa.org/publications/armymagazine/archive/2010/10/Documents/Petraeus_1010.pdf>.

³ Organisation for Economic Co-operation and Development (OECD), *A Development Co-operation Lens on Terrorism Prevention* (Paris: OECD, 2003).

⁴ Ibid.

⁵ The World Bank, *World Development Report 2011: Conflict, Security, and Development* (Washington, DC: World Bank, 2011), 79; Eli Berman et al., "Do Working Men Rebel? Insurgency and Unemployment in Afghanistan, Iraq, and the Philippines," *Journal of Conflict Resolution* 55, no. 4 (March 2011), 496–528.

⁶ Radha Iyengar, Jonathan Monten, and Matthew Hanson, "Building Peace: The Impact of Aid on the Labor Market for Insurgents," National Bureau of Economic Research Working Paper 17297, August 2011.

⁷ Field Manual (FM) 3-24, *Counterinsurgency* (Washington, DC: Headquarters Department of the Army, 2006).

⁸ Andrew Beath, Fotini Christia, and Ruben Enikolopov, "Winning Hearts and Minds through Development? Evidence from a Field Experiment in Afghanistan," Policy Research Working Paper 6129 (Washington, DC: The World Bank, July 2012); International Security Assistance Force (ISAF) Counterinsurgency Advisory and Assistance Team, *Less Boom for the Buck: Projects for COIN Effects and Transition* (Kabul: ISAF, 2011).

⁹ Stathis N. Kalyvas, "Ethnic Defection in Civil War," *Comparative Political Studies* 41, no. 8 (August 2008), 1043–1068.

¹⁰ Department of the Army, *Commander's Guide to Money as a Weapons System* (Fort Leavenworth, KS: Combined Arms Center, 2009).

¹¹ Rebecca Patterson and Jonathon Robinson, "The Commander as Investor: Changing CERP Practices," *PRISM* 2, no. 2 (March 2011), 115–126.

¹² William Durch, ed., *Twenty-First-Century Peace Operations* (Washington, DC: United States Institute of Peace, 2006).

¹³ Tim Ripley, *Operation Enduring Freedom: America's Afghan War 2001 to 2002* (Havertown, PA: Casemate, 2012).

¹⁴ Ibid.

¹⁵ *Counterinsurgency Operations* (Washington, DC: Department of the Army, 2004).

¹⁶ Office of the Secretary of Defense, *Justification for FY 2014 Overseas Contingency Operations Afghanistan Infrastructure Fund (AIF)*

(Washington, DC: Department of Defense, May 2013), available at <http://asafm.army.mil/Documents/OfficeDocuments/Budget/BudgetMaterials/FY14/OCO//aif.pdf>.

¹⁷ Ibid.

¹⁸ Ibid.

¹⁹ Amy Belasco, *The Cost of Iraq, Afghanistan, and Other Global War on Terror Operations Since 9/11*, RL 33110 (Washington, DC: Congressional Research Service, March 29, 2011), available at <www.fas.org/sgp/crs/natsec/RL33110.pdf>.

²⁰ Ibid.

²¹ Matthew Chlosta, "AFPAK Hands Begins Immersion in Afghanistan," ISAF Public Affairs Office, April 23, 2010, available at <www.isaf.nato.int/article/news/afpak-hands-begins-immersion-in-afghanistan.html>.

²² See, for instance, Ted Robert Gurr, *Why Men Rebel* (Princeton: Princeton University Press, 1970); and James M. Olson, C. Peter Herman, and Mark P. Zanna, eds., *Relative Deprivation and Social Comparison* (Hillsdale, NJ: Lawrence Erlbaum Associates, 1986).

²³ Paul Collier and Anke Hoeffler, "On Economic Causes of Civil War," *Oxford Economic Papers* 50, no. 4 (1998), 563–573; and "Greed and Grievance in Civil War," *Oxford Economic Papers* 56, no. 4 (2004), 563–595.

²⁴ James D. Fearon, "Rationalist Explanations for War," *International Organization* 49, no. 3 (1995), 379–414; Robert Powell, "Bargaining Theory and International Conflict," *Annual Review of Political Science* 5 (2002), 1–30; Robert Powell, "War as a Commitment Problem," *International Organization* 60, no. 1 (2006), 169–203.

²⁵ Hershel I. Grossman, "A General Equilibrium Model of Insurrections," *American Economic Review* 81, no. 4 (1991), 912–921; James D. Fearon and David D. Laitin, "Civil War Termination," Working Paper, Stanford University, 2008.

²⁶ Anne O. Krueger, "The Political Economy of the Rent-Seeking Society," *The American Economic Review* 64, no. 3 (June 1974), 291–303.

²⁷ Paul Collier, *The Bottom Billion* (Oxford: Oxford University Press, 2007).

²⁸ Michela Wrong, *It's Our Turn to Eat: The Story of a Kenyan Whistle-Blower* (New York: Harper, 2009).

²⁹ North, Wallis, and Weingast actually posit a third order—the foraging order, which are small groups characteristic of hunter-gathering societies. However, as this order is not relevant to most security-related strategy and planning, it is not discussed here. Douglass C. North, John Joseph Wallis, and Barry R. Weingast, *Violence and Social Orders: A Conceptual Framework for Interpreting Recorded Human History* (Cambridge: Cambridge University Press, 2009).

³⁰ Ibid.

³¹ Robert H. Bates, *Prosperity and Violence: The Political Economy of Development* (New York: Norton, 2001).

³² Robert H. Bates, *When Things Fell Apart: State Failure in Late-Century Africa* (New York: Cambridge University Press, 2008).

³³ James D. Fearon and David D. Laitin, "Ethnicity, Insurgency, and Civil War," *American Political Science Review* 97, no. 1 (February 2003), 75–90.

³⁴ Anne Ellen Henderson, "The Coalition Provisional Authority's Experience with Economic Reconstruction in Iraq: Lessons Learned," Washington, DC, United States Institute of Peace, April 2005, available at <www.usip.org/publications/the-coalition-provisional-authoritys-experience-economic-reconstruction-in-iraq-lessons>.

³⁵ FM 3-07, *Stability Operations* (Washington, DC: Headquarters Department of the Army, 2008).

³⁶ FM 3-0, *Operations* (Washington, DC: Headquarters Department of the Army, 2008).

³⁷ Arthur D. Simons Center for the Study of Interagency Cooperation, *Interagency Handbook for Transitions* (Fort Leavenworth, KS: Command and General Staff College Foundation Press, 2011); Kelvin Ong, *Managing Fighting Forces: DDR in Peace Processes* (Washington, DC: United States Institute of Peace, 2012); Colette Rasuch, ed., *Combating Serious Crimes in Postconflict Societies* (Washington, DC: United States Institute of Peace, 2009); Keith Crane et al., *Guidebook for Providing Economic Assistance at the Tactical Level During Stability Operations* (Santa Monica, CA: RAND, 2008).

³⁸ Thomas Parks and William Cole, *Political Settlements: Implications for International Development Policy and Practice*, Occasional Paper No. 2 (Washington, DC: The Asia Foundation, July 2010), available at <http://asiafoundation.org/resources/pdfs/PoliticalSettlements-FINAL.pdf>.

³⁹ Transparency International, *Corruption and Peacekeeping: Strengthening Peacekeeping and the United Nations* (London: Transparency International, October 2013).

⁴⁰ Hal Brands, "Crime, Irregular Warfare, and Institutional Failure in Latin America: Guatemala as a Case Study," *Studies in Conflict and Terrorism* 34, no. 3 (February 2011), 228–247.

Chairman of the Joint Chiefs of Staff
General Martin E. Dempsey addresses
students attending National Defense
University at Fort McNair, Washington, DC,
October 5, 2011 (DOD/D. Myles Cullen)



Low Cost, High Returns

Getting More from International Partnerships

By Russell S. Thacker and Paul W. Lambert

Unbeknownst to most Americans, over 8,000 international military personnel are trained or educated annually in the United States at the invitation of the U.S. Government, studying every aspect of the military profession. The most select officers with

future leadership potential are invited to participate in senior Professional Military Education (PME) courses alongside U.S. officers at schools such as National Defense University (NDU) and the Army, Naval, Air, and Marine Corps War Colleges. Many of these stu-

dents are funded by the United States through security assistance programs such as the International Military Education and Training (IMET) program, which has an annual cost of over \$100 million. This is a significant investment of time and treasure by the United States, and as we will show, the initial returns of these programs are high.

However, despite the significant investment, once courses end, the U.S. Government expends very little effort

Russell S. Thacker is Alumni and Outreach Manager for International Programs in the International Student Management Office (ISMO) at the National Defense University. Paul W. Lambert is an Assistant Professor in ISMO.

to maintain relationships with these international graduates and use them as potential strategic partners. The lack of attention is surprising, not only because we are divesting when our returns would be their highest but also given the way Departments of State and Defense leaders view these programs. Said Admiral Michael Mullen, former Chairman of the Joint Chiefs of Staff, “Security cooperation through PME is an investment in the future of both the selected students and the nations being engaged. Like all investments, an optimal return on our investment is sought.”¹ Unfortunately, we are not seeing an “optimal” return in the long run when benefits could be the greatest.

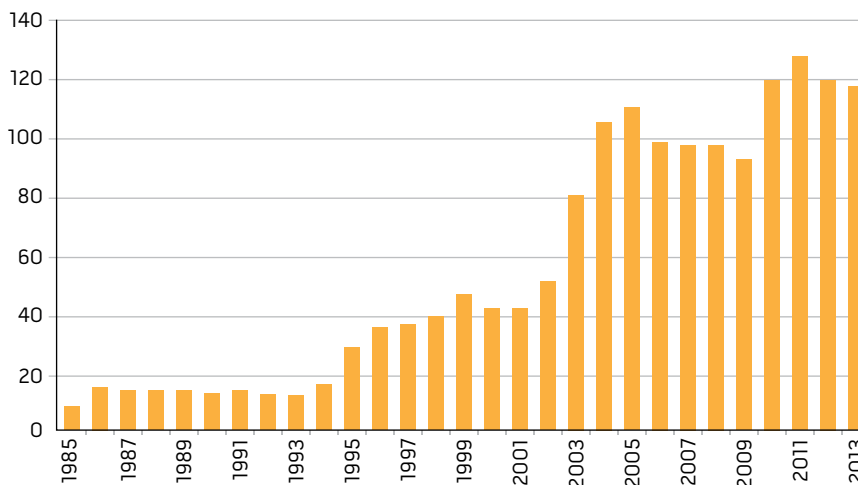
We argue that the United States can do better by maintaining long-term relationships with these graduates. While we think increased alumni outreach would be beneficial for all IMET and PME programs, the focus of this article is increased engagement with international graduates of Intermediate and Senior PME programs. Our analysis and recommendations for improvement are drawn primarily from our experience working with the international programs at National Defense University, a senior PME school.

Theory of Success for International Military Education

In the two decades since the fall of the Iron Curtain, participation of international military students in U.S. programs has exploded. At NDU, the number of students enrolled in our international programs grew from 12 per year in 1991 to 46 by the end of the decade. Following the September 11 attacks, a new wave of students focused on counterterrorism and homeland defense brought student totals to over 100 by 2010 (see figure 1). This rise is indicative of trends across U.S. PME and training schools. Currently, over 140 countries send students to study alongside the U.S. military each year at upwards of 180 U.S. military schools and facilities.²

What is the objective of these security assistance programs? As stated in the Foreign Assistance Act of 1961,

Figure 1. Growth of International Military Students at NDU*



*Includes students attending the College of International Security Affairs, Information Resources Management College, National War College, and Dwight D. Eisenhower School for National Security and Resource Strategy.

the intent of Congress in establishing the IMET program was to improve the ability of allied and friendly countries to achieve self-reliance in their security objectives, increase awareness of basic issues involving internationally recognized human rights and civil-military relations, and develop greater understanding and fraternity between participants and participating nations.³ Capacity-building, reinforcement of established norms and values, and a fostering of relationships all constitute ways in which the United States has retained influence with partner nations. Such military-to-military contact, which some call “defense diplomacy,” represents a powerful alternative to traditional instruments of power.⁴

Capacity-building. Much as technical training programs such as aircraft maintenance aim to raise the skill set of countries’ armed forces, the education offered to students at PME schools aims to bolster the leadership and strategic thinking capabilities of future leaders of partner nations. This education offers opportunities for greater interoperability, making countries more capable of working with the United States and within the international community by drawing from a shared curriculum and language. According to the State Department, one of the goals of the IMET program is to “enhance the ability of friends and allies

to participate in coalition, humanitarian, peacekeeping, counterterrorism, and counterinsurgency operations.”⁵

Recognition of Human Rights.

International PME programs also aim to instill recognition of established norms in human rights and civil-military relations through exposure of officers to U.S. values of equality, democracy, and civilian control of the armed forces. This experience comes through visiting institutions such as media outlets, universities, government agencies, and business locations around the United States and by engaging officers in discussion of these themes. For example, at NDU, international officers join a year-long academic course on American identity that addresses these concepts, and they participate in a robust Field Studies Program, traveling to over 15 locations around the country where they are hosted by representatives from every sector of U.S. society.⁶

Relationships and Improved

Understanding. Arguably, the most important outcome of PME programs is the strength of relationships formed between the international officers and their classmates, sponsors, or other contacts here in the United States. Both U.S. and international representatives view these relationships not simply as personal friendships—although in most cases, they are—but as enablers of future

Figure 2. Percentage Increase in Student Confidence

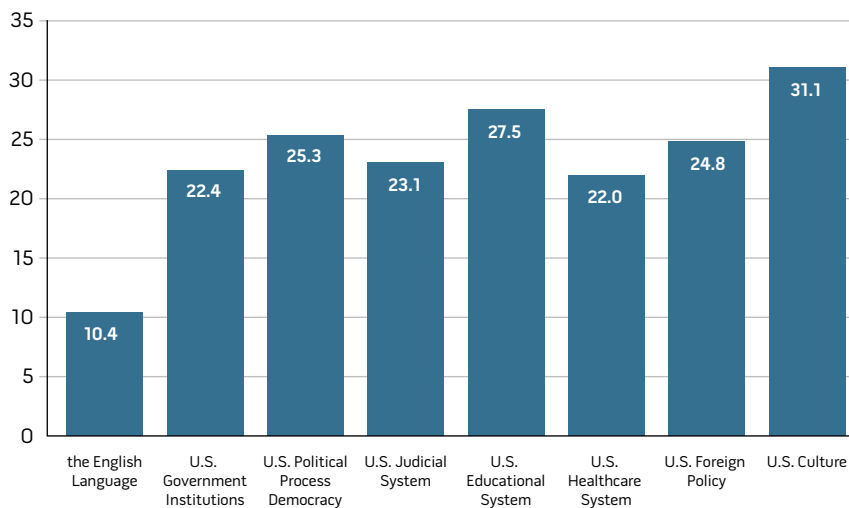
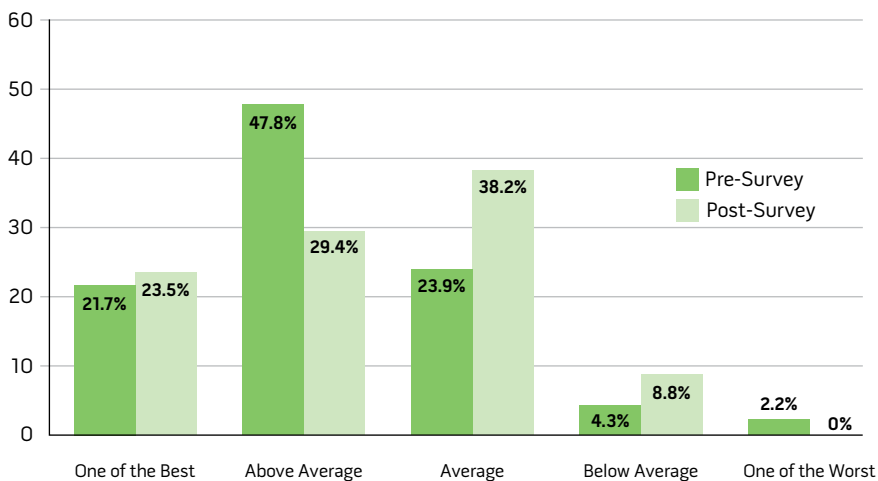


Figure 3. How Do You Think Your Country Ranks in Its Respect for Human Rights?



cooperation, influence, and advancement of interests between their countries. At NDU, heavy emphasis is placed on bonding, networking, and socializing among classmates outside of schoolwork. The international officers form a tight-knit bond with each other and a working relationship with their U.S. counterparts after a year of intense studying, debating in the classroom, and sharing of cultures and perspectives. These outcomes are in line with what the Department of Defense (DOD) has stressed in implementing IMET programs: a desire to develop “rapport, understanding, and communication links” between U.S. and partner armed forces.⁷ This network, coupled with a

surer understanding of and familiarity with the U.S. system, means international graduates are ahead of the curve in their future associations with the United States. General (Ret.) Mieczyslaw Cieniuch, former Chief of General Staff of the Polish Armed Forces, stated, “NDU helped me learn about the American way of life and doing business. This understanding and appreciation of the U.S. culture certainly helped me to establish a good relationship with all my partners and interlocutors from the United States.”⁸

Evidence of Success. Efforts to measure the impact of these programs on international students have been encouraging and illustrate an initial high return on the

U.S. investment. In 2011, a study was undertaken to measure the impact of NDU’s international programs on the resident international students’ attitudes and understanding of the U.S. Government and culture as well as their commitment to democracy and internationally recognized human rights. The study was built around two survey instruments that measured these factors upon the students’ arrival to NDU and again at departure to their home country a year later. The study showed that international students’ understanding of the U.S. governing system improved significantly and that students’ views of democracy and internationally recognized human rights became more nuanced after their year at NDU.⁹

As shown in figure 2, the students’ confidence level in understanding the U.S. Government, institutions, and culture at the conclusion of their time at NDU significantly increased, especially the understanding of culture (an increase of 31.1 percent). The study also found that international students developed a more critical analysis and view of democracy and human rights in their own countries during the year enrolled in the program. The students generally saw their home countries as somewhat democratic in the arrival survey, but they became slightly more critical in the departure survey. In reference to human rights, the question was asked, “Compared to the rest of the world, how does your country rank in its respect for Human Rights?” Figure 3 illustrates the clear downward shift between the arrival and departure surveys. In the arrival survey, a majority of students indicated that they saw their home country as better than average in the realm of Human Rights (69.5 percent). In the departure survey, this dropped to 52.9 percent.¹⁰

In addition to the statistical evidence in this and other survey instruments we have used, there are countless testimonials from students and graduates that illustrate the effectiveness of the programs in promoting understanding and building capacity. One student remarked, “Exposure to American society has enhanced my knowledge on American culture, history, and politics so that I am

better able to understand how the United States sees the world.” Another said, “The education I received at NDU gave me new skills to better analyze events and make decisions. The knowledge I received allows me to better analyze every situation, critically think about problems, and think strategically to find solutions with the collaboration of partners in the security community.”

Our experience and studies such as these give us confidence that the international programs at NDU and other PME schools are creating a high initial return from the U.S. investment in the students and their countries. While here in the United States, strong partnerships of understanding, respect, and commitment to human right and democracy are developed and strengthened among our international friends. But what becomes of those partnerships when these officers return home and take positions of influence in their country?

The Problem: Failure to Maintain Key Relationships Through Continued Engagement

We suggest that international PME programs are largely meeting their objectives during the students’ time in the program. However, once students leave these institutions, there is a dismal track record of maintaining contact with them. The reality is the majority of graduates are never tracked, contacted, or heard from again in their home countries. For U.S. policymakers, agencies, and schools, this not only means losing our ability to continue to achieve program objectives over time but also failing to accurately measure what has been achieved. Long-term return on investment for international military education remains unrealized, or at least unknown.

How few graduates are actually being followed? Beginning in 2001, U.S. law explicitly mandated that records be kept on each IMET student to include the type of instruction received, whether it was completed successfully, and “to the extent practicable” his or her subsequent career and current position.¹¹ Despite the mandate, the Government Accountability Office (GAO) estimates DOD has actually

maintained updated information on only 1 percent of graduates, focusing on the small percentage who reach certain positions of prominence.¹² The online Defense Security Assistance Management System (DSAMS) was created partly to maintain this information, but it contains at best only snippets of data and is not regularly updated or used for this purpose. There is also no requirement to collect contact information for graduates, and many graduates have simply slipped out of reach. Individual schools may be collecting this information more successfully, but they are doing it in an ad hoc and uncoordinated fashion.

Even still, simply collecting the right data on graduates falls short of the intent of IMET and international PME programs, which is to create long-term relationships with graduates and establish global networks of security practitioners. When graduates leave schools like NDU, they largely take with them positive impressions of their time and a deeper understanding of the United States. They are motivated to stay in contact with American classmates, their school, and their international classmates. They are primed to be effective partners in their home country, able to communicate with U.S. representatives and understand the domestic political, economic, and cultural context in which American foreign policy occurs. They are also positioned to provide useful feedback and experience to the schools from which they graduated. Unfortunately, too little effort is made to utilize graduates for these advantages, thus limiting the full realization of program goals.

Roots of the Problem. This problem of tracking graduates is not new. In a 1990 report on the IMET program, GAO also reported “no system for monitoring use of IMET graduates” and no accurate way for DOD to measure the effectiveness of the program.¹³ GAO echoed many of the same concerns in a 2011 report as well as extending this line of thinking to U.S. graduates in a 2013 review of PME programs, saying schools must place a greater emphasis on continuing education and lifelong learning for graduates.¹⁴ Awareness within the security assistance

community may finally be dawning. In the recent Chairman of the Joint Chiefs of Staff Strategy for International Professional Military Education, the Chairman places greater emphasis on the need to “facilitate long-term relationships” with international graduates, in order to “enhance our ability to foster peace and security.”¹⁵

Despite the greater awareness, the current PME system is simply not designed to produce vibrant continuing contact with graduates. In talking with other intermediate and senior PME programs around the country, we have found this engagement happening at different levels. Most schools have opted to do nothing and have lost contact with nearly all graduates; some have built small alumni activities into their current operations but are unable to commit any resources to a formal program; and a few schools have a formal program with innovative efforts under way but are limited in their ability to accomplish its full potential. The common theme through the feedback is that all agree we need to do more to maintain contact with graduates, but lack of policy guidance, limited resources, poor coordination, and an overall absence of focus on this aspect of education constrain these efforts.

Lack of Guidance. The problem begins with an absence of clear guidance as to who should be maintaining contact with graduates. Is it the schoolhouses, the Embassies, or other independent offices within DOD or the State Department that should undertake this effort? Until recently, the only formal guidance on this subject available to schools like NDU was found in a single paragraph of text in the Joint Security Cooperation Education and Training Regulation stating that schools are encouraged to maintain contact through either periodic mailings of school newsletters or a 1-year subscription to any relevant professional publication.¹⁶

Limited Resources. Lack of guidance translates into limited or no resources available to conduct this outreach. There are often no manning billets or positions for continuing engagement within schoolhouses and no dedicated funding streams for alumni activities. Further,

Table. Benefits of Continuing Contact with International Alumni

Value to Graduates	<ul style="list-style-type: none">• Access to continuing education (for example, school library network)• Access to network of security practitioners• Greater voice through direct link to U.S. Government
Value to Schools	<ul style="list-style-type: none">• Access to graduates for assessment of training program• Larger pool of alumni subject matter experts to draw upon for experience• Graduates help build reputation of program and raise quality of students over time
Value to U.S. Government	<ul style="list-style-type: none">• Improved interoperability with allies and partners through shared curriculum• Visible symbol of continuing investment in allied and partner countries• Ability to cut through bureaucratic "red tape" with direct contact to allies and partners• Opening of diplomatic doors• Access to those who understand and are comfortable interacting with the United States

because all funding for international students comes through a reimbursable model of tuition funds, it is quite difficult for schoolhouses to justify dedicating funding or personnel to alumni activities at the expense of current students to whom tuition dollars are tied. To work around this issue, some institutions have turned to non-official personnel to conduct this outreach, by working through nonprofit organizations or private foundations affiliated with the college or university. This may be a successful model; however, recent experience shows schools must be careful in allowing outside organizations such as foundations to perform "inherently governmental functions."¹⁷

Lack of Coordination and Information-sharing. Finally, lackluster coordination between the key actors in the system remains a key obstacle to staying in contact with graduates. In the security assistance universe, the main touch-points for international students are the U.S. offices of defense cooperation (ODCs) in Embassies where personnel assist in selecting, vetting, and sending students, and at schoolhouses where international student offices support their education experience. ODCs have been primarily tasked with keeping accurate graduate information in that country by seeking reports from the defense ministry on the current position of graduates and updating this information online. However, we have found that due to the frequent turnover of ODC personnel and an abundance of tasks on their plates, this information is rarely sought and obtained, let alone communicated

back to the schoolhouse. There is also little incentive for countries to actively report information to the ODC, and occasionally even a disincentive if countries are suspicious of U.S. motives in obtaining this.

When graduate information is obtained, it is rarely shared, either horizontally or vertically. International students often have attended multiple PME programs, and schools would benefit from knowing their backgrounds as well as any outreach efforts of other schools toward them. Graduate information is also rarely shared "up" between schools and DOD or the State Department. "Despite its potential value as part of a broader IMET evaluation effort, training managers do not systematically share this information with State and DOD and are only required to share information on the small percentage of IMET graduates."¹⁸

Potential Benefits of Alumni Outreach

At NDU, we have faced many of these same constraints on alumni engagement but have nonetheless tried increasing our efforts to reach out to graduates. Two years ago, we created a dedicated alumni position, mobilized staff on specific alumni projects, became more active online and in social media, began conducting continuing education seminars, and started seeking updates on graduates in earnest. We have seen substantial benefits come from this engagement and anticipate many other benefits are within reach with additional efforts (see table).

For graduates, maintaining contact is beneficial in providing both further education and access to a broad network of classmates and alumni. Our graduates have increased their use of educational resources available on campus, such as lifetime access to the NDU library and collaboration with faculty and researchers, and have stayed current on security issues by participating in continuing education seminars and forums. Alumni have also found that using the graduate network opens doors to excel in their positions and benefit their countries. For example, 2 years ago, a Russian graduate who was serving as head of the aviation security agency in Moscow contacted our office with a desire to broaden his agency's capabilities through learning from the U.S. system. Using connections at NDU, we helped arrange a counterpart visit between him and the Transportation Security Agency regional director in Washington. Similarly, one of our graduates from the United Arab Emirates (UAE) was assigned to create the new National Defense University of UAE. His first action was to reach back through alumni channels to NDU and ask for assistance, resulting in a long-standing collaboration between the U.S. and UAE defense universities. Many other graduates have used channels directly to their classmates. When the political crisis erupted in Libya in 2011, one of our alumni from Austria led the removal of all Austrian citizens from the country. After encountering issues at the Egyptian border with the chaos of many people fleeing, he contacted his NDU classmate, a general in the Egyptian Army who provided the necessary arrangements to ensure the Austrian citizens passed smoothly. In many cases, the graduates' connection to NDU or their classmates has allowed them to bypass significant red tape to achieve positive gains for their country.

For schools, the value of alumni engagement flows from their improved ability to assess outcomes and draw on the experience of graduates. At NDU, we have used assessment tools such as surveys, interviews, and feedback sessions to observe whether graduates have

used skills obtained at NDU, introduced new ideas into the workplace, published, achieved flag officer rank, and stayed in contact with classmates. Schools are also able to draw from a pool of alumni subject matter experts working around the world to provide perspective on issues and enrich curriculum. Graduates have been able to return and lecture at NDU, help faculty in their research, and write for publications. In several cases, alumni have opened doors to NDU student or faculty groups traveling overseas, augmenting their itineraries with visits to places that would otherwise be inaccessible.

Finally, continuing engagement has value to the U.S. Government over time from a practical and strategic level, although this is most difficult to measure. Graduates are able to work in a more interoperable way with U.S. and international partners. Strategically, the United States is able to nurture relationships with those in key positions of influence. From NDU alone, there are 11 international graduates currently serving as chiefs of defense or secretaries of defense, 15 acting as chiefs of service within their armed forces, and numerous others in key governmental, diplomatic, or business positions around the globe. When expanded to all senior or intermediate PME schools, the success of graduates comprises an enormous network of senior leaders with whom the United States could engage. Referencing Indian graduates specifically, one U.S. Pacific Command country director wrote:

We are looking to ensure we have the visibility on these folks as they emerge . . . into senior leadership positions. From the middle of 2011 until the end of 2013, the three Indian service chiefs were all U.S. PME graduates . . . plus many other influential two and three stars. The Indian chiefs of service personally hand select the attendees to U.S. PME—it is that important to them. Furthermore, we can tell within three to five minutes the Indians that have been through our courses; they are broadly strategically minded, have a good understanding of jointness, and understand our systems (which are quite different from theirs).¹⁹

Even if graduates are not in key policy positions, they can still play a valuable strategic role. For example, several former U.S. ambassadors at NDU have said they wished they had information on NDU international graduates in countries where they served as ambassadors, as they often looked for government or armed forces officials with a familiarity with the United States and an established level of trust with whom to engage. Similarly, at NDU we have been contacted many times by unified commands or task forces asking for information on graduates in their regions—information they were seeking by contacting every senior PME school one by one. While we have been able to provide the information for these requests, we believe if information on graduates was more readily and systematically available to officials abroad, many more benefits would arise from employing the experience of these graduates.

Recommendations

We have distilled several recommendations to help individual schools and the U.S. Government as a whole achieve greater returns on their investments in international military education programs.

Raise Emphasis on Continuing Engagement by Assigning Guidance and Resources. In many cases, specifics are still lacking as to how the U.S. Government can and ought to maintain these relationships. How do individual schools maintain contact with graduates overseas? What personnel, resources, and opportunities are available to assist in this mission? There is a need for more specific guidance from the agency level to schools and to ODCs specifying what information managers should collect, how they should do it, and how it can be appropriately used. Greater guidance would unlock more resources for schools to use in reaching graduates—covering costs of communications systems, publications and materials, alumni events or seminars, recognition ceremonies, and personnel. Some graduates have raised the idea of building in a percentage of each IMET student's tuition cost to cover future alumni connectivity and attendance at

alumni seminars. Though not an IMET program, DOD's Combating Terrorism Fellowship Program provides a good model of a program that has built-in provisions for alumni outreach and provides funds for dedicated staff positions, events, and communication tools.

Take a Joint Approach to Graduate Engagement. The successes of international education programs are repeated many times over at many PME institutions around the country. Currently, other than DSAMS, no common data management system exists to access, update, and share information on graduates. Such a system would enable schools to share information horizontally and enable them to easily communicate to higher levels of State Department and DOD officials what graduate resources are available in certain countries or positions, instead of expecting decisionmakers to painstakingly track this information from each school. This data sharing has occurred on a smaller scale in ways that can be replicated. For example, the Defense Security Cooperation Agency's five regional centers now use the same student management system, which allows for full visibility of the background of international students between the centers and allows the centers to easily share information.

Although graduate engagement should be headquartered at each school, many alumni activities can be carried out in a joint manner. For example, at previous NDU regional continuing education seminars, we have partnered with the regional centers to invite their graduates to participate in the event. Likewise, Army War College graduates have occasionally joined. This only enriches the alumni network and opens more opportunities to individual graduates. Whereas U.S. Armed Forces are culturally divided along service lines, in the eyes of our international partners, any of these schools act as representatives of the United States.

Shift Focus from Tracking Information to Building Relationships. We regret that most U.S. efforts to date in reaching graduates have focused on collecting information, not building relationships. Narrowly focusing on

data collection can imply we are only interested in monitoring graduates for one-way benefit, as if it were an intelligence gathering effort. Instead, focusing on genuinely building relationships through engagement will ultimately provide more lasting and mutual benefits. This engagement ought to happen with all levels of graduates, not just those occupying prominent or strategic positions.

The way in which we build relationships is first by communicating and then finding ways to work together. The most important information that can be retained on graduates is their contact information, such as a simple email address. An email or social media address opens up a range of tools such as e-newsletters, webinars, instant messaging, and real-time feedback. Social media cannot be overlooked as a crucial way to maintain relationships, although not all graduates are capable of or comfortable with communicating in this way. In addition to online outreach, regional or U.S.-based seminars or conferences allow these relationships to be maintained and strengthened over time.

We work together when we find ways to leverage graduates, both as ongoing resources to schools and as potential partners in their home countries, and allow graduates access to our networks and resources. Just as international students in PME courses are often expected to offer a different perspective in a U.S.-dominated academic environment, international graduates can make a unique contribution to schools by enriching their curriculum, contacts, publications, and opinions. For example, one school we spoke to plans to invite international graduates back on campus each year to sit in on courses and give feedback on whether the curriculum is keeping pace with security issues around the world. Likewise, U.S. officials should be aware of these graduates and seek out their assistance and perspective on matters of U.S. policy in their countries. Graduates can be relied on as sounding boards by U.S. officials who need feedback on new ideas or proposals, and they can be effective interlocutors on the other side of the table. Moreover, graduates should be

encouraged to reach out and utilize U.S. opinions, contacts, and resources to the greatest extent possible as full partners. There are many other potential ways to use alumni we have not yet discovered.

Our experience in senior PME international programs convinces us that we are gaining a good return on investment when the students are in residence, both in achieving learning outcomes and influencing perceptions of students. However, in failing to maintain these relationships in the long run, we are missing out on the highest returns and fullest potential of these programs. Effective engagement of graduates across PME schools is entirely possible, but it requires the development of more sound policy, dedication of resources, collaboration, and a creative approach to utilize and engage graduates as part of a robust graduate network.

It is hard to argue against the value of strong international partnerships in today's security environment. Declining U.S. resources and drawdowns of defense budgets continue to bring security cooperation to the forefront in terms of value and effectiveness. There has never been a better time for the U.S. Government to invest in the relationships that have been formed with the body of international military students who have attended PME institutions. This is a low-cost, high-return way to keep our international partnerships strong. JFQ

Notes

¹ Chairman of the Joint Chiefs of Staff, "International Professional Military Education (PME) Strategy," CJCS Guide 1800, August 31, 2011.

² U.S. Government Accountability Office (GAO), *International Military Education and Training: Agencies Should Emphasize Human Rights Training and Improve Evaluations*, GAO-12-123 (Washington, DC: GAO, 2011), 4.

³ Foreign Assistance Act, 22 USC §2347b (1961), "Congressional Declaration of Purpose," available at <www.law.cornell.edu/uscode/text/22/2347b>.

⁴ Wolfgang Koerner, "Security Sector Reform: Defence Diplomacy," *Parliamentary Information and Research Service*, May 17, 2006, available at <www.parl.gc.ca/Content/LOP/researchpublications/prb0612-e.pdf>.

⁵ U.S. Department of State, *Congressional Budget Justification: Foreign Operations* (Washington, DC: Department of State, 2010), 142.

⁶ U.S. Department of Defense, *United States Field Studies Program (FSP) for International Military and Civilian Students and Military-Sponsored Visitors*, DOD Instruction 5410.17 (2006).

⁷ Defense Security Cooperation Agency, *Security Assistance Management Manual*, C10.6.3.1, available at <www.samm.dsca.mil/chapter/chapter-10>.

⁸ General Mieczysław Cieniuch, remarks at NDU Hall of Fame Induction Ceremony, Washington, DC, January 10, 2012.

⁹ Adam Jungdahl and Paul Lambert, "Winning Hearts by Broadening Minds: Measuring the Impact of International Military Assistance at the National Defense University," *The DISAM Annual* 1 (2012), 153.

¹⁰ Ibid.

¹¹ Foreign Assistance Act, 22 USC §2347g (1961), "Records Regarding Foreign Participants," available at <www.law.cornell.edu/uscode/text/22/2347g>. The GAO uses the term "monitor" to refer to tracking alumni in-country. Because this word is often associated with surveillance, we prefer instead to talk about maintaining accurate records or staying in contact with graduates.

¹² GAO, *International Military Education and Training*, 19.

¹³ GAO, *Security Assistance: Observations on the International Military Education and Training Program*, GAO/NSIAD-90-215BR (Washington, DC: GAO, 1990).

¹⁴ GAO, *Joint Military Education: Actions Needed to Implement DoD Recommendations for Enhancing Leadership Development*, GAO-14-29 (Washington, DC: GAO, 2013).

¹⁵ Chairman of the Joint Chiefs of Staff, *International PME Strategy*, A-1.

¹⁶ Joint Security Cooperation Education and Training, 10-54 (2011) Army Regulation 12-15, SECNAVINST 4950.4B, AFI 16-105. 10-54, 186-187.

¹⁷ Office of the Naval Inspector General, *Report of Investigation: Senior Official Case 201103025* (2012), available at <www.secnav.navy.mil/ig/Pages/FOIA/ReadingRoom.aspx>.

¹⁸ GAO, *International Military Education and Training*, 19.

¹⁹ LTC Christopher M. Coglianese, email message to author, December 6, 2013.



Asymmetry Is Strategy, Strategy Is Asymmetry

By Lukas Milevski

Much of the strategic studies literature of the past two decades identifies profound novelty in the conduct and challenges of modern war, novelty that ultimately calls into question the nature and even existence of war. War has allegedly now been transformed from a regular, conventional, purportedly symmetric exercise

into an irregular, unconventional, asymmetric event, which must be understood anew.

Of all the new descriptors for war, “asymmetric” is among the broadest. It has even been suggested that *asymmetry* does not bear definition: “to *define* the term *defies* its very meaning, purpose, and significance.”¹ Some, undeterred

by such extreme pronouncements, have attempted at least to categorize various existing and potential concepts of asymmetry. Thus, Jan Angstrom has identified four different prisms through which asymmetry may be interpreted: “power distribution, organisational status of the actor, method of warfare, and norms.”² Yet despite claims of newness, it has also been observed that asymmetry has infused nearly every, if not every, war in recorded history. (Possibly only the hoplite phalanxes of ancient Greece could be

Lukas Milevski is a Ph.D. Candidate in the Graduate Institute of Political and International Studies at the University of Reading, United Kingdom.

considered properly symmetrical in nearly all respects, for geography, demographics, and so forth make all politics fundamentally asymmetrical to some degree.) Misunderstanding asymmetry poses significant dangers: “our misuse of the terms asymmetry and asymmetric distorts those vital processes and leads us to make major strategic blunders. For example, by focusing on threats rather than enemy strategies we fail to understand their strategic nature, goals, and overall concepts of operations.”³

The question thus arises: how may one fruitfully discuss asymmetry as a separate phenomenon? Perhaps the time has come to abandon the endeavor as unhelpful and rather suggest that asymmetry in war, and even asymmetric strategy, are redundancies. *Asymmetry is strategy, and strategy is asymmetry.* This article argues the point in three parts. First, it suggests that observations of a novel change are overexaggerated. Second, it maintains that no matter the form war may take, the function of strategy is eternal. Third, it proposes that contemporary asymmetric conflicts are all comprehensible through the lens of strategy.

Form over Substance

Theorists of contemporary conflict, whether describing asymmetric or unconventional wars, war among the people, or other iterations of modern armed conflict, usually posit significant change in the character, if not actual nature, of war. Many of them accurately identify and analyze the characteristics of modern interventions. In perceiving significant differences between modern war and wars past, however, they caricature historical conflict.

Thus, Rupert Smith argues that “war as cognitively known to most non-combatants, war as battle in a field between men and machinery, war as a massive deciding event in a dispute in international affairs: such war no longer exists.”⁴ Martin van Creveld propounds the notion that “the demise of conventional war will cause strategy in its traditional, Clausewitzian sense to disappear.”⁵ Fourth-generation warfare theorists such as T.X. Hammes identify generations of

warfare with particular styles of conducting war; third-generation warfare is, for example, maneuver warfare, and fourth-generation warfare “uses all available networks—political, economic, social, and military—to convince the enemy’s political decision makers that their strategic goals are either unachievable or too costly for the perceived benefit. It is an evolved form of insurgency.”⁶

Yet their theories on the changes in war depend upon caricaturing what came before. They have succeeded somewhat in part because many centers of strategic education similarly caricature historical war. These caricatures rely on a Eurocentric perspective of strategic history. Smith’s war as a battle in a field between men and machinery and Hammes’s third-generation warfare as maneuver warfare, for example, both rely on the World Wars, especially World War II. These wars were fought among European or Western polities, all of which have similar strategic cultures. Yet modern interventions primarily take place between Western powers and polities elsewhere in the world, with significant differences in strategic culture. Theorists of change in war are comparing apples with oranges and perceiving change based on such flawed comparisons, which serve only to churn various fashions in strategic thought.

To analyze interventions, comparisons to the Third Afghan War of 1919 or the Rif War of 1919–1926 would much more accurately demonstrate how much war has actually changed. Similarly, conventional war must be compared to conventional war. Notably, Russia’s 2008 invasion of Georgia did not trigger a Georgian insurgency against the Russians, or even against the Abkhazians or South Ossetians. The war remained conventional throughout. The Iraq War of 2003 did transform into an insurgency, but not immediately. The period of a few months between the end of conventional operations and the serious beginning of the insurgency was terribly squandered by the United States, which visibly failed to begin righting the country. Although it would be incorrect to say that this great

strategic and political failure caused the insurgency, it certainly exacerbated it.

Hew Strachan has suggested that “the real problem may well be that our policy has failed to recognise war’s true nature, and so has mistaken changing characteristics for something more fundamental than they actually are.”⁷ This mischaracterization is frequently manifested in the belief, as apparent before Iraq in 2003 and during some of the advocacy for intervention in Syria in 2013, that war is not adversarial, that enemies do not reciprocally interact with, and against, each other. The character of any war is not unilaterally set by any one implicated polity, but by the reciprocal hostility of all those involved. Thus, in not accounting for the enemy’s own initiative against us, the Western powers are blindsided by actions that are then interpreted as integral to the structure of contemporary war rather than as the consequence of something inherent in war, which is more fundamental and eternal.

Asymmetry and Strategy

That which is eternal is strategy, the purposeful threat or use of violence to achieve desired ends. Strategy has no permanent form, although it always retains its enduring substance and function. Strategy has always been practiced, even though before the word’s rediscovery in the 1770s, strategies explicitly labeled as such may not have been expressly planned or implemented.⁸ The core task of strategy may be identified as Everett Dolman does: “strategy, in its simplest form, is *a plan for attaining continuing advantage*.”⁹ Dolman rightly observes that the strategist’s task is usually aided more by advantage than disadvantage. “Advantage,” like strategy, is not defined by a particular form. Advantage may take the form of materiel, political will, a superior grasp of how to translate forces deployed into aims achieved, or so on. Understanding war and all the influences on it is necessarily multidisciplinary; therefore, asymmetry may manifest itself in a similarly wide range.

Strategy may be thus cast in a more absolute manner than merely the



Special Forces Soldier crosses roof of compound during combat with Taliban forces in Bahlozi Village, Maiwand District, Kandahar Province (DOD)

achievement of continuing advantage. Rather, strategy may be interpreted as *the generation and exploitation of asymmetry for the purposes of the war*. Roger Barnett complains that:

*asymmetries arise if opponents enjoy greater freedom of action, or if they have weapons or techniques available to them that one does not. Perpetrators seek to void the strengths of their adversaries and to be unpredictable. They endeavor to take advantage of an ability to follow certain courses of action or to employ methods that can be neither anticipated nor countered effectively.*¹⁰

Yet this is the very essence of strategy. Strategy is an adversarial act; the enemy also has a will, a capability, and a vote in the outcome. This reciprocal nature of strategy is a primary source of strategy's nonlinearity, for defeat may beget renewed defiance and alternative attempts to achieve one's goals, rather than the desired submission. Thus, Edward Luttwak, for instance, identifies the very pinnacle of strategic performance as "the suspension, if only brief, if only partial, of the entire predicament of strategy."¹¹ The predicament of strategy is the enemy.

The pinnacle, therefore, is the removal of the enemy's ability, however temporarily, to influence outcomes. Suffering from a position of weakness in an asymmetric relationship restricts one's abilities to influence outcomes based on that relationship. To generate asymmetry effectively is to be, although not necessarily the only way to be, a skilled strategist.

The generation of asymmetry is the basis of much, if not most, strategic theory, particularly power-specific theories such as those pertaining to seapower or airpower. Command of the sea or of the air cannot mean anything other than the generation of a major operational asymmetry in either of those warfighting domains relative to the enemy. Similarly, the very idea of massing and applying one's forces against the decisive point, a theme in both Antoine-Henri Jomini's and Carl von Clausewitz's works, is to generate asymmetry in a particular location, to achieve the desired wider effects. The debates about the revolution in military affairs and transformation are also ultimately about generating significant asymmetry, albeit in the form of a particular silver bullet. Cold War nuclear strategy was similarly meant to establish asymmetries of commitment,

even when theorists might not be able to make operational sense of asymmetries of capability, particularly in the theories of Thomas Schelling. The strategic theories of Basil Liddell Hart were so steeped in the generation of asymmetry that it apparently affected his understanding of the moral component of strategy. He focused relentlessly on the indirect approach to create situations in which the enemy would be utterly helpless, therefore hopeless, and so would surrender without undue bloodshed, thereby removing killing from the concept of morality in strategy. Instead, "strategy is the very opposite of morality, as it is largely concerned with the art of deception," in reality not because killing had no place in morality, but because killing had no place in his idea of good strategy.¹²

Asymmetry is thus clearly compatible with conventional warfare, simply because it is good strategy. During World War II, the conventional war par excellence, the Allies ultimately established major asymmetries in military-industrial production and logistics, on the sea, and in the air over all the Axis countries. World War I was a bloody stalemate on the Western Front for so long in large part because until 1918 neither side was

able to generate the asymmetries required to break it. The belligerents who generated the most important asymmetries ultimately won. Not all asymmetries are equal; some may be more immediate than others, some may be ultimately more damaging to one's ability to achieve desired goals than others, and so on. Effective asymmetry, like effective strategy, is context-sensitive.

Asymmetry is strategy, strategy is asymmetry. Conrad Crane of the U.S. Army War College is reputed to have suggested that "there are two types of warfare: asymmetric and stupid."¹³ Generating effective asymmetry is good strategy. To condemn rhetorically our opponents for generating asymmetry reveals our conditioning born of understanding recent history through the prism of wishful thinking, of expecting one's enemies to be poor strategists such as those faced in 1990–1991, 2001, and 2003. Wishful thinking, operationalized as unrealistically optimistic assumptions, does not usually lead to strategic success, as our experience of the variably labeled "war on terror" or "Long War" clearly indicates.

One might counter that conventional asymmetries on land, sea, and air are far more easily understood than unconventional asymmetries such as guerrilla warfare. This may indeed be the case, but so what? One may understand a threat and still be incapable of countering it. German General Fridolin von Senger und Etterlin, who had participated in the Italian campaign of 1943–1945, once likened operating under Allied air supremacy to playing chess against an opponent who could play three pieces each turn to his one. No amount of understanding of the threat can help alleviate a situation if that understanding cannot be turned into operational plans and successful outcomes. This is just as true of conventional asymmetries as of unconventional ones. In fact, conventional asymmetries are usually the more dangerous of the two for their ultimate political effects are usually greater, as the experience of warlords from Darius III to Napoleon to Adolf Hitler may attest. Each lost his empire to enemies who were ultimately more capable of

generating effective asymmetry. Relatively few unconventional asymmetries have had the historical effect equivalent to losing an empire. One of the few pertinent, albeit inexact, examples is the American Revolutionary War, but even that war was "hybrid" rather than purely unconventional.¹⁴

Strategy in Contemporary War

Asymmetry today is most commonly associated with insurgency and irregular foes. Contemporary theories on strategies for counterinsurgency also implicitly emphasize the generation of effective asymmetry against the so-called asymmetric enemy. Unlike the generation of conventional asymmetries, many of which tend to be domain-oriented, contemporary counterinsurgency theory emphasizes asymmetry from the perspective of the population's support, through the provision of security and other services, including effective governance. David Galula is frequently identified as the progenitor of this theory. It is nevertheless significant that his proposed strategic blueprint for counterinsurgency only begins with the destruction or expulsion of insurgents as an organized body and ends, after the organization of local communities into effective and self-sustaining political entities, with the destruction of the last of the insurgents.¹⁵

Force does not lack utility against a foe that is generating unconventional asymmetry. Indeed, the very form of that asymmetry reveals a significant concern about one's own conventional military superiority over the insurgent. Unconventional asymmetry is guerrilla warfare, arising from military weakness and infused with concern for the survival of the insurgent force. Without that force, the insurgency is likely to fail. Galula noted that "in any situation, whatever the cause, there will be an active minority for the cause, a neutral majority, and an active minority against the cause."¹⁶ A neutral majority will acquiesce to whichever party appears most likely to succeed. One of the most publicly visible features of such a measurement is the apparent effectiveness of the respective

armed forces. The truism that the counterinsurgent loses if he does not win, but the insurgent wins if he does not lose, is indicative of this. Once the counterinsurgent, superior in strength, fails to win and so withdraws from the conflict, the only remaining viable power in the country will be the insurgent force. This truism is, of course, true only in the context of intervention because the counterinsurgent ultimately *must leave*; it is not an iron law of insurgency as such, as the example of Sri Lanka may attest.

This observation is not new to contemporary war. C.E. Callwell, one of the major luminaries of historical British strategic thought on small wars, offered an explanation at the end of the 19th century: "It is a singular feature of small wars that from the point of view of strategy the regular forces are upon the whole at a distinct disadvantage as compared to their antagonists." In battle, however, regular troops have the tactical advantage: "Since tactics favour the regular troops while strategy favours the enemy, the object to be sought for clearly is to fight, not to manoeuvre, to meet the hostile forces in open battle, not to compel them to give way by having recourse to strategy."¹⁷ The imbalance of military power between intervener and insurgent was, and remains, the basis for the guerrilla's choice of strategy.

It is noteworthy in this context that, of the four great theorists of insurgent warfare, T.E. Lawrence, Mao Zedong, Vo Nguyen Giap, and Ernesto "Che" Guevara, only Lawrence did *not* theorize the eventual transition from guerrilla to relatively, if not absolutely, conventional warfare for the final campaigns definitively to seize power from the government forces. Lawrence, of course, fought as part of a larger conventional operation commanded by General Edmund Allenby and so had no need to turn his fighters into a conventional force. This is not to argue that members of the Taliban are running around the Hindu Kush with Mao's little red book in their pockets, but rather that these authors identified the limits of guerrilla warfare. Thus, not even insurgency may violate the fundamental truth which J.C. Wylie observed: "the ultimate determinant in

war is the man on the scene with the gun. This man is the final power in war. He is control. He determines who wins.”¹⁸

The enemy relies upon unconventional asymmetry if he believes himself unable to succeed without it. The Taliban in Helmand Province only turned back to tried-and-tested guerrilla tactics after suffering disastrous casualties in futile frontal assaults on British bases. This adaptation coincided with the loss of widespread local support, as “the cost of aligning themselves with the Taliban turned out to be very high for many communities in terms of destruction and loss of life,” as well as with consequent Taliban attempts to regain some local legitimacy and support.¹⁹ The generation of asymmetry through guerrilla tactics has both advantages and disadvantages, which must be examined with respect to the function of strategy, that is, the conversion of violence into desired political effect for both the insurgent and the counterinsurgent.

The basis of strategy is war, the purpose of which “is some measure of control over the enemy.” Control is a rarely defined term whose limits are quite broad, being “neither so extreme as to amount to extermination . . . nor . . . so tenuous as to foster the continued behavior of the enemy as a hazard to the victory.”²⁰ The pattern of events in war is driven by the reciprocal interaction of adversaries, “a contest for freedom of action.”²¹ Since control pertains to freedom of action, one might identify three different categories of control. The weakest form of control is merely the denial of control, or preventing the enemy from unduly restricting one’s own freedom of action. Once a belligerent is relatively strong enough, he may attempt to take control and threaten actively to limit his opponent’s freedom of action. The final type of control is its exercise after having taken it, to prosecute the war to a successful conclusion. Much of strategic theory assumes that a belligerent without freedom of action or the ability to pursue his political goals will ultimately abandon his endeavor.

Unconventional asymmetry is capable only of denying control to the superior enemy. Despite being the weakest form of control, it remains potent. A strategy



Special Forces Soldier exits building during operations in Arghandab District, Afghanistan (U.S. Army/Gino Palu)

based upon the accumulated effect of minor actions and continued elusiveness to deny control of the operational pattern of the war presents significant difficulties for the opposing side. Presenting no single set of targets and acting against and among civilians across geographies larger than their opponents may completely secure provide the counterinsurgent with a wide array of potential choices, whose strategic worth may be estimated but hardly known. Thus, Harry Summers caustically noted that during the Vietnam War, the United States identified up to 22 different wartime objectives.²² This plethora of choice encourages unproductive or even counterproductive actions and contradicting policy goals on the part of the conventionally superior force. For instance, in Afghanistan, U.S. policies simultaneously require the local warlords to be liquidated for purposes of state-building and to be preserved to fight the Taliban.²³ Unconventional asymmetry targets the stronger foe’s strategy rather than the enemy himself.

The counterinsurgent, if unable to bring force or other tools effectively to bear to weaken the insurgency, merely marks time with blood. Time is a precious commodity in strategy and must be used wisely, but the substantial intellectual challenge facing the counterinsurgent places significant obstacles on the path of so doing.

Despite its deleterious effects on the stronger opponent’s strategic performance, unconventional asymmetry is a serious strategic gamble. Although it denies control to the enemy, the insurgents themselves also do not gain control over the pattern of the war. Both sides tend to have the maximum freedom of action possible in an otherwise reciprocally adversarial context. The Viet Cong might skulk into Saigon to plant explosives, but the Marines could hold Khe Sanh, within spitting distance of the Ho Chi Minh Trail, which was absolutely vital to the Viet Cong and the North Vietnamese army in South Vietnam. In such a situation, barring any dramatic changes, rarely



M1 Abrams tanks maneuver in streets of Tall Afar, Iraq, as they conduct combat patrol (U.S. Air Force/Aaron Allmon)

is there a clear indication of who holds the advantage until the conflict itself actually ends.

Strategy poses a difficult challenge due to the nonlinearities involved, many of which stem from the active presence of an independently acting adversary. Yet on the sliding scale of difficulty, the generation of asymmetry through guerrilla warfare may almost be a leap of faith. Although the skilled guerrilla retains initiative in being able to choose his own battlefields, the power of decision is preserved for his foe. The denier of control has no direct influence on the perception of his efforts in the opposing headquarters; he cannot impose a victory, but can only wait until his opponent acquiesces to defeat. Although today insurgents are able to fight figuratively in the media as well as literally on the ground, the pressure of public opinion seems to count for less in wartime than in peacetime because of the other pressures war generates: “The declaration of war, and more

immediately the use of violence, alters everything. From that point on, the demands of war tend to shape policy, more than the direction of policy shapes war.”²⁴

The generation of asymmetry through use of guerrilla tactics may be a strategy that Western powers find difficult to defeat, despite more than a decade of constant experience with attempting to combat it. It is nevertheless fundamentally the same phenomenon as generating asymmetry through commanding the sea or the air and may be understood with the same basic toolbox of strategic concepts. British mastery of the seas largely bewildered French attempts to defeat it for over a century and resulted in the French development of a number of methods by which to strike at British command of the sea without directly challenging it, including the *guerre de course* and the later *jeune école*, which was obsessed with the potential of torpedo boats. Today the roles are reversed, for the weaker belligerent has bewildered the

Western powers and left them scrambling to determine how to combat the threat.

Many time-tested methods of defeating guerrillas directly are unacceptable to liberal powers today. As David Kilcullen puts it, “Indeed, any given state’s approach to counterinsurgency depends on the nature of the state, and the concept of ‘counterinsurgency’ can mean entirely different things depending on the character of the government involved.”²⁵ These methods may also be inappropriate for the specific conditions in which Western powers find themselves. Treating counterinsurgency as social work is more amenable to Western sensitivities than treating it as war. Although counterinsurgency definitely is the latter, it may well be both. Violence remains the base coinage of strategy, but this does not rule out the utility of counterfeits or other instruments of political power. One must remember that these tools are merely used as replacements for violence in specific circumstances where they may effectively

take the place of force. War is war, but war is also politics. The other instruments of political power do not lose relevance once violence begins, but their utility is tempered by the introduction of force.

Moreover, it may be possible that today, compared to all prior historical experience, it is easiest for liberal powers to track and target insurgents. This is due to a number of factors, including the widespread use of new communications and other technologies, and new techniques to use this technology.²⁶ Taking the fight directly to the insurgents has become a plausible option for liberal democracies in a way that would not have previously been allowed, with massive cordons and conscription of locals to serve in temporary militias. With an increasing ability to strike desirable insurgent targets directly and relatively precisely comes an opportunity, in theory but also necessarily tempered by the actual circumstances of practice, to render relatively ineffective the generation of asymmetry through guerrilla tactics. The particular character of specific asymmetries does not change the fact that they all may be comprehended through the lens of strategy.

Conclusion

Rupert Smith is skeptical of the idea of asymmetric warfare. He rightly indicates that “the practice of war, indeed its ‘art,’ is to achieve an asymmetry over the opponent. Labeling wars as asymmetric is to me something of a euphemism to avoid acknowledging that my opponent is not playing to my strengths and I am not winning.”²⁷ Smith’s euphemism implies that the opponent is practicing strategy better than the Western powers are; since the practice of strategy determines how any particular polity engages in warfare, the implications of poor strategic practice are grave.

Asymmetry as now commonly used—to denote a supposedly particular new type of war—is not a useful term and, for some, implies strategic ethnocentric hubris that “assumes there is only one truth and model for warfare, and that we alone have it.”²⁸ In fact, today and historically, most strategies seek to generate asymmetry as a way of minimizing the enemy’s

vote on the character and outcome of the war. Lawrence Freedman once defined strategy as “the art of creating power.”²⁹ Given that power is a necessarily relational quality—for one cannot have power in the absence of an entity on or against which it may be exercised—the generation of asymmetry is the restriction and minimization of the enemy’s effective power vis-à-vis oneself and the multiplication and maximization of one’s own against that adversary.

Labeling only a certain segment of strategies as asymmetric risks obscuring the enormous real asymmetric advantages liberal democracies have over those insurgents who purportedly employ the asymmetric strategies. This practice threatens conceptually to detach asymmetric warfare from war and strategy by treating it as something else, and in doing so it contributes toward preventing the Western powers from fully and effectively employing force against weaker challengers, as the popularity of asymmetry in strategic literature is a self-reinforcing symptom of our diluted grasp on strategy. Asymmetry will ever remain strategy, and strategy will ever remain asymmetry. JFQ

Notes

¹ Jesse G. Chace, “Defining Asymmetric Warfare: A Losing Proposition,” *Joint Force Quarterly* 61 (2nd Quarter 2011), 124.

² Jan Angstrom, “Evaluating Rivalling Interpretations of Asymmetric War and Warfare,” in *Conceptualising Modern War*, ed. Karl Erik Haug and Ole Jørgen Maaø, 31 (London: Hurst & Company, 2011).

³ Stephen J. Blank, *Rethinking Asymmetric Threats* (Carlisle Barracks, PA: Strategic Studies Institute, 2003), v.

⁴ Rupert Smith, *The Utility of Force: The Art of War in the Modern World* (London: Penguin Books 2006), 1.

⁵ Martin van Creveld, *The Transformation of War* (New York: The Free Press, 1991).

⁶ T.X. Hammes, *The Sling and the Stone: On War in the 21st Century* (St. Paul: Zenith Press 2004), 2, 3.

⁷ Hew Strachan, “Introductory Essay: The Changing Character of War,” in *Conceptualising Modern War*, 25.

⁸ Beatrice Heuser, “Strategy Before the Word: Ancient Wisdom for the Modern World,” *RUSI Journal* 155, no. 1 (February/March 2010), 36–42.

⁹ Everett C. Dolman, *Pure Strategy: Power and Principle in the Space and Information Age* (New York: Frank Cass, 2005), 6.

¹⁰ Roger W. Barnett, *Asymmetrical Warfare: Today’s Challenge to U.S. Military Power* (Washington, DC: Potomac Books, 2003), 15.

¹¹ Edward N. Luttwak, *Strategy: The Logic of War and Peace* (Cambridge: Belknap Press, 2001), 4.

¹² Basil Liddell Hart, *Strategy* (New York: Meridian, 1991), 220.

¹³ Quotation from Emile Simpson, *War from the Ground Up: Twenty-First-Century Combat as Politics* (London: Hurst & Company, 2012), 140.

¹⁴ Williamson Murray, “The American Revolution: Hybrid War in America’s Past,” in *Hybrid Warfare: Fighting Complex Opponents from the Ancient World to the Present*, ed. Williamson Murray and Peter R. Mansoor, 72–103 (Cambridge: Cambridge University Press, 2012).

¹⁵ David Galula, *Counterinsurgency Warfare: Theory and Practice* (Westport, CT: Praeger Security International, 2006), 55.

¹⁶ *Ibid.*, 53.

¹⁷ C.E. Callwell, *Small Wars: Their Principles and Practice* (Lincoln: University of Nebraska Press, 1996), 85, 91.

¹⁸ J.C. Wylie, *Military Strategy: A General Theory of Power Control* (Annapolis, MD: Naval Institute Press, 1989), 72.

¹⁹ Theo Farrell and Antonio Giustozzi, “The Taliban at War: Inside the Helmand Insurgency, 2004–2012,” *International Affairs* 89, no. 4 (2013), 854.

²⁰ Wylie, 66, 70.

²¹ André Beaufre, *An Introduction to Strategy*, trans. R.H. Barry (London: Faber and Faber, 1965), 110.

²² Harry G. Summers, Jr., *On Strategy: A Critical Analysis of the Vietnam War* (New York: Presidio Press, 1995), 98.

²³ Mark Peceny and Yuri Bosin, “Winning with Warlords in Afghanistan,” *Small Wars & Insurgencies* 22, no. 4 (September 2011), 603–618.

²⁴ Hew Strachan, “Strategy in the Twenty-First Century,” in *The Changing Character of War*, ed. Hew Strachan and Sibylle Scheipers, 508 (Oxford: Oxford University Press, 2011).

²⁵ David J. Kilcullen, *Counterinsurgency* (London: Hurst & Company, 2010), 155.

²⁶ Michael T. Flynn, Rich Juergens, and Thomas L. Cantrell, “Employing ISR: SOF Best Practices,” *Joint Force Quarterly* 50 (3rd Quarter 2008), 56–61; Mark Urban, *Task Force Black: The Explosive True Story of the SAS and the Secret War in Iraq* (London: Little, Brown, 2010).

²⁷ Smith, 4.

²⁸ Blank, 15–16.

²⁹ Lawrence Freedman, “Strategic Studies and the Problem of Power,” in *War, Strategy and International Politics: Essays in Honour of Sir Michael Howard*, ed. Lawrence Freedman, Paul Hayes, and Robert O’Neill (Oxford: Clarendon Press, 1992).



Senior Airmen program Wireless Gate Release System before airdrop at Bagram Air Field (U.S. Air Force/Evelyn Chavez)

Is Military Science “Scientific”?

By Glenn Voelz

The term *military science* generally describes the body of theories, concepts, and methods for employing armed forces. However, as an academic discipline it is ill defined, drawing from a patchwork of curricula including history, foreign affairs, security studies, leadership, operations management, and systems engineering, as well as other elements of the physical and social sciences. Notably, the Department of Defense dictionary does not even provide a definition.

Lieutenant Colonel Glenn Voelz, USA, is Chief of the Intelligence Control Division, Directorate for Intelligence (G2), U.S. Army Africa.

This vague categorization is somewhat reflective of the term’s diminished status from its 19th-century usage when *Military Science* was frequently capitalized and placed alongside Physics, Philosophy, and other well-established academic disciplines.

An irony of the term’s decline is that it occurred over a period when military professionals increasingly conceptualized their discipline in the terminology and metaphors of science. This transformation was driven in part by the institutionalization of officer education programs emphasizing the formalized study of military theory. A second factor, rapid industrialization, firmly established science and technology as the central

pillars of American military power and arguably the foundational elements in approaches to doctrine and planning. These trends reinforced the proposition that the practical application of military theory, as expressed through strategy, doctrine, and planning, was becoming more of a science and less of an art. This perspective has reached an apex in recent decades, epitomized by doctrinal methodologies seeking to reduce decisionmaking to formulaic processes—not unlike the methods used by chemists mixing compounds for desired effect. In particular, there has been a tendency toward instrumental applications of descriptive theory attempting to distill complex social dynamics into bounded problem statements

that fit neatly into proscribed planning schemas and process solutions.¹

Military science certainly shares some basic traits with the physical sciences in the use of observation, description, measurement, and structured analysis supporting causal inferences or explanatory hypotheses. However, military science remains distinct from the physical sciences in significant ways, most notably in the absence of controlled, replicable experimentation as means of validating theory. For this and others reasons, the conceptual foundations of the field reside more appropriately in the realm of the social sciences. While this conclusion may be intuitively obvious to most military professionals, its practical implications are increasingly overlooked and are reflective of a deep and persistent strain of “scientism” within the intellectual foundation of American approaches to military theory, doctrine, and planning.²

Origins of American Military Scientism

Observers have long suggested a distinct techno-scientific orientation as the defining characteristic of American approaches to strategy, doctrine, and planning. Early military theory in the United States was based largely on inherited European traditions profoundly influenced by Newtonian logic with emphasis on deterministic relationships and predictable linear interactions between forces.³ Discovery of laws describing the natural universe led to the search for similar constants governing interactions among armies in the field. Such early examples of “military scientism” reflected a growing belief that warfare, like other natural phenomena, could be analyzed to reveal basic patterns and predictable characteristics.

These precedents deeply influenced early American approaches to military theory requiring that authoritative scientific principles serve as the basis for doctrinal approaches, while technological innovation came to be viewed as the transformational element in the history of warfare. The founding of West Point in the early 19th century reflected these influences, particularly under the early

leadership of superintendent Sylvanus Thayer, who firmly entrenched a technical and engineering-based curriculum as the preferred intellectual foundation for military leaders. This approach was reinforced under Professor Dennis Hart Mahan, who was instrumental in transferring European knowledge and practices to the Academy with particular emphasis on engineering, fortifications, ballistics, and topography as core elements of military education.

Within this context, military theorist Baron de Jomini emerged as perhaps the most influential theorist in 19th-century America. The Swiss-born officer held that all strategy was “controlled by invariable scientific principles” and attempted to reduce its conduct to prescriptive rules deeply rooted in empirical methods and analysis of historical example.⁴ Indeed, his “scientifically” derived concepts of mass, maneuver, and lines of operation remain central to American doctrine and military theory to this day.

Carl von Clausewitz was the other dominant influence on late 19th-century American military thinking. With his emphasis on complexity and ambiguity, Clausewitz is often viewed as the theorist more relevant to modern “nonlinear” warfare, yet his vocabulary also reflects the powerful influences of Renaissance-era science, particularly his use of Newtonian analogies—force, mass, center of gravity—to describe the nature of armed conflict.⁵ Indeed, central to Clausewitzian thought is the concept of “friction,” illustrating the role that chance and uncertainty play as determining factors in war. Like Jomini, Clausewitz shared the view that knowledge of science combined with practical experience and deep study of history was fundamental in preparation for command. However, he was less convinced of the utility of universal principles and sacrosanct theory as guides to the conduct of war. Rather, Clausewitz suggested that the purpose of theory was to educate the mind of a leader rather than “accompany him to the field of battle.”⁶ Furthermore, he cautioned against the tendency for theory to furnish commanders with positive doctrines and systems to be used “like mental appliances.”⁷

Within this intellectual milieu evolved the concurrent phenomena of military professionalization and industrialization, both serving to reinforce America’s emerging techno-scientific approach to warfare. Lessons of the Civil War awakened theorists to the criticality of mobility, logistics, and industrial production as central aspects of strategic calculation. Additionally, the decades prior to World War I marked a period of intense scientific, technological, and industrial innovation transforming the practice of warfare with the introduction of radio, submarines, airplanes, automobiles, machineguns, and high explosives.

Theorists and planners were not only embracing the promise of new technology but also examining how scientific methods and modern management practices could be transferred from the laboratory and factory floor to the battlefield. Development of the modern staff system and functional specialization reflected this impulse, necessitated in part by the increasingly complicated management tasks associated with mass mobilization and logistical demands of industrial age warfare. This evolution also demanded more formalized systems of military training and education with an emphasis on structured methodologies and codified doctrine. Just as scientific management practices rationalized the process of industrial production, military theorists attempted to bring “order, regularity, and predictability” to the practice of war.⁸

Among influential 20th-century military theorists, B.H. Liddell Hart was one of the more devout believers that the scientific study of warfare would reveal “a few truths of experience which seem so universal, and so fundamental, as to be termed axioms.”⁹ Though best known for his advocacy of the “indirect approach” and tenets of maneuver warfare, Hart’s thinking reflected an increasingly influential pedagogical perspective viewing history as the laboratory of military science. “If the study of war in the past has so often proved fallible as a guide to the course and conduct of the next war,” he noted, “it implies not that war is unsuited to scientific study but that the study has not been scientific enough in spirit and method.”¹⁰



New York Air National Guard's 109th Airlift Wing flies LC-130 over Greenland on mission to resupply remote science research outposts (DOD/Fred W. Baker II)

J.F.C. Fuller, another dominant intellectual influence of the interwar period, took this notion to its logical conclusion and argued for direct application of scientific methodologies to the study of warfare, asserting nothing less than his desire “to do for war what Copernicus did for astronomy, Newton for physics, and Darwin for natural history.”¹¹ Through exhaustive historical analysis of warfare from antiquity to the modern era, Fuller became convinced that such methods would “enable the student to study the history of war scientifically, and to work out a plan of war scientifically, and create, not only a scientific method of discovery, but also a scientific method of instruction.”¹²

The views of Hart and Fuller reflected a growing confidence in the promise of scientifically managed warfare based on technological innovation and empirically derived approaches. This phenomenon was not limited to land warfare. Strains of such thinking were clearly present in Alfred Thayer Mahan’s

theories on seapower and the interplay of technology, geography, and tactical principles. Airpower theory was equally driven by techno-scientific approaches exemplified by influential thinkers such as Giulio Douhet, Billy Mitchell, and Hugh Trenchard, who variously promoted strategies based on innovative technologies linked with theoretical yet largely unproven principles of employment and effect.

World War II came closer than any modern conflict to validating the notion that the coupling of technology and scientific management could deliver desired and predictable strategic ends. Paul Kennedy’s recent study of the conflict masterfully depicts a “scientists’ war” highlighting the remarkable achievements of mid-level engineers and managers who developed technical, organizational, and process innovations to overcome many of the war’s biggest challenges. Kennedy focuses particularly on issues such as convoy security, strategic bombing, and

amphibious landings, where rapid fielding of technical solutions combined with doctrinal and tactical adaptability delivered significant and measurable advantages that proved decisive in winning the war.¹³

By this analysis, World War II may be read as vindication of the techno-scientific approaches advocated by Jomini, Hart, and Fuller. However, one must consider whether the war represented an exemplar or an isolated aberration. First, one is struck by the remarkable symmetry in means and method of the major combatants, particularly in terms of technological sophistication, industrialization, organizational structures, and, to some degree, doctrinal approach. Certainly when contrasted with other conflicts of the modern era, it is the similarities between combatants more than the differences that seem noteworthy. Moreover, Kennedy notes that many of the central military challenges of the conflict—issues of time, distance, and production—were problems particularly well suited to structured

analysis and technical and managerial solutions. Multiple elements central to wartime strategy such as convoy security and strategic bombing provided relatively straightforward feedback loops enabling clear analysis, unambiguous experimentation, and rapid implementation of functional solutions.

In any case, lessons of victory profoundly influenced subsequent approaches of the Cold War era. From the tactical to the strategic level, the military turned to applied science, operations research, and systems analysis to address the most complex national security challenges of the postwar period. Characteristics of the principal Cold War adversaries—structured, homogenous, hierarchical, and doctrinally based—served to reinforce the conclusion that military planning and decisionmaking might be mastered through algorithms and process models. The field of intelligence as much as any other became defined by such approaches. Technical collection capabilities managed by centralized bureaucracies proved remarkably effective at producing detailed information on highly structured conventional threats. In other respects, the rise of the Cold War-era technoscientific regime was necessitated by the increasingly complicated demands of managing a massive and widely dispersed standing military. Theorist Martin van Creveld observed that the expanding scope of military operations, logistics networks, and occupational specialization increasingly demanded centralized control and the leveraging of science, mathematics, and advanced communications to enable effective coordination on such a massive scale.¹⁴ This trend naturally reinforced reliance on systems analysis, operational research, and statistical methodologies as basic tools for military decisionmaking and planning.

These trends had a profound influence during the Vietnam conflict on approaches employed by Defense Secretary Robert McNamara, particularly efforts to translate tactical feedback into quantifiable metrics for analyzing and guiding strategic level decisionmaking. Antoine Bousquet describes the concept of “cybernetics” evolving out of World

War II that engendered an “understanding of war which strove to frame the use of military force into an activity totally amenable to scientific analysis, to the detriment of other forms of thought.”¹⁵ However, these shortcomings did little to challenge the prevailing notion that warfare could be analyzed and managed with scientific precision. Bousquet cites as a high point of this trend the advent of theories formalized under the rubric of “revolution in military affairs” (RMA) in the decades following Vietnam.

The essence of RMA maintained that technological innovation and integrated advances in weapons, information processing, communications, organizational management, and doctrinal approaches would be the primary drivers of future military advantage. RMA emphasized operations research and systems analysis to frame strategy and planning decisions as engineering problems to be solved through data collection and analysis, presuming that measurable risk and outcome probabilities could be estimated with reasonable confidence through adherence to doctrinal methods. These process-oriented methods became increasingly formalized and to this day dominate the pedagogical approach to professional military education.

Even with the end of the Cold War, military theory and doctrinal development continued to reflect the persistent influence of the techno-scientific approaches, notably with concepts such as network-centric warfare and effects-based operations, ideas closely related to the cybernetic methods of the Vietnam era and later RMA efforts. These doctrinal theories were premised on analyzing the battlefield environment as a holistic system of interdependent nodes and causal linkages that could be identified and acted upon with measured and predictable effect. This process was enabled by conceptual models such as operational net assessment and system-of-systems analysis. These models apply computational tools, algorithms, and data-intensive analyses to disaggregate key dynamics of a given operational environment and then revisualize their environments as coherent and holistic systems.

After a decade of conflict defined by unconventional adversaries, complex environments, and ambiguous operational endstates, a new era of military scientism is already taking form. The contours of this next evolution might be described as “post-Newtonian, post-Jominian.” Army Design Theory has emerged as the conceptual basis of a new approach to planning in complex environments. Meanwhile, military theorists are looking to fields such as advanced mathematics, theoretical physics, and biology for insights into complex system behavior and modeling intervention strategies. Other efforts are exploring chaos theory and related fields for tools to analyze environmental propensities of conflict zones, emergent security instabilities, and mapping system dynamics of terrorist networks and insurgencies. Despite a new vocabulary, the essence of these approaches remains firmly grounded in the basic presumptions of the technoscientific regime. By all evidence, military scientism remains as powerful an influence as ever in the American tradition.

Fatal Striving: Hayek, Scientism, and the Limits of Useful Knowledge

Friedrich Hayek identified a similar phenomenon in his own field of economics, notably articulated during his 1974 Nobel Prize lecture in which he cautioned colleagues against misapplication of scientific-like methods to tasks for which they were unsuited. Hayek expressed concern that “confidence in the unlimited power of science is only too often based on a false belief that the scientific method consists in the application of a ready-made technique, or in imitating the form rather than the substance of scientific procedure, as if one needed only to follow some cooking recipes to solve all social problems.”¹⁶ His criticisms were directed at the intersection of the social sciences and public policy where he saw vague imitations of scientific methodologies applied inappropriately to management of complex social phenomena. He labeled such practices intellectual “charlatanism” intended primarily for the purpose of

lending legitimacy and pretense of precision to policy proscriptions amounting to little more than blind tinkering in areas where fundamental uncertainty prevailed. Indeed, Hayek could well have been speaking of military science when he described the curious task of economics as demonstrating “to men how little they really know about what they imagine they can design.”¹⁷

As a young soldier in the Austro-Hungarian army along the Italian front during World War I, Hayek certainly did not lack exposure to the complexity and arbitrariness of armed conflict. Later in his career, he described the inherent challenges of decisionmaking in environments characterized by fragmentary information. He was particularly interested in how such systems resisted submission to hierarchical, centralized planning—a notion directly challenging the fundamental premise of deliberate design.¹⁸ Though not a military theorist *per se*, Hayek’s insights into the use of knowledge, function of complex systems, and dangers of scientism all offer important lessons for the contemporary strategist, planner, and student of military theory.

A foundational element of Hayek’s worldview relates to his observations concerning the “unavoidable imperfection of man’s knowledge.”¹⁹ The phrase should not be misunderstood as resignation to intellectual nihilism. Rather, it reflects a profound insight about the nature of information, particularly pertaining to environments where data is dispersed, tacitly understood, or in forms resistant to detection, collection, and analysis, thus rendering it too subjective to be a basis for scientifically valid conclusions. In this sense, Hayek describes the essence behind Clausewitz’s famous dictum that intelligence reports in war are often “contradictory; even more are false, and most are uncertain.”²⁰ As a result, theory formation in the social sciences is often a function of information availability.²¹ This situation naturally promotes forms of selection bias when information critical to understanding system behavior is too disaggregated for systematic collection or simply ignored due to its uncertain significance. Bousquet as well as military theorist

Martin van Creveld identified such “information pathologies” during the Vietnam conflict where pseudo-scientific approaches to strategy evolved based on the most easily quantifiable characteristics of the battlefield, thereby conflating counting with understanding.²²

A widely circulated recent paper concerning intelligence in Afghanistan noted that even after a decade of war, the American military still finds “itself unable to answer fundamental questions about the environment in which we operate.”²³ The authors posit that a central problem has been the inability to aggregate useful information existing at the lowest levels for use by higher level decisionmakers, noting that the ground soldier or local development worker is generally best informed about their particular environment, while the path “up through the levels of hierarchy is normally a journey into greater degrees of cluelessness.” The paper identifies the central obstacle to gathering and acting upon relevant information as a matter of inadequate organizational structure. Conversely, Hayek would say that the basic issue is not a result of flaws in organizational structure, but rather something more fundamental about the nature of knowledge in complex systems. He points out that circumstances defining outcomes in complex environments are rarely, if ever, fully accessible to the social scientist, policymaker, or military planner, no matter how information is collected and acted upon.

To some degree, this situation reflects the inescapable reality of military science and the fundamental epistemological challenge of analyzing complex social phenomena. With historical example as its laboratory, military theory relies on *ex post facto* analysis of what are essentially natural experiments. This entails several limitations. As a mode of analysis, historical narrative is fundamentally linear and deterministic by nature. Its aim is to find causality, thereby minimizing the role of chance. It veils complexity and shies from ambiguity. Its vernaculars tend toward the anecdotal, interpersonal, and spectacular. History does not always know what it does not know. Ultimately, what it provides is reasoning by induction—drawing

general rules from specific examples. It is non-empirical in that it relies on uncontrolled data. Perhaps most importantly, as a basis for applied theory, it lacks mechanisms of validation through experimental replication—the essence of scientific methodology.

In his recent book, Jim Manzi suggests the limited practical utility of the nonexperimental social sciences, noting these fields are generally “not capable of making useful, reliable, and non-obvious predictions for the effects of most proposed policy interventions.”²⁴ However, in the case of military science, historical interpretations often become proxy for theory or, at the very least, the basis for instrumentalist approaches to operational decisionmaking. Unlike in the physical sciences where a hypothesis may be proposed, tested, and potentially disproved, military science generally does not offer falsifiable propositions. This characteristic, according to Karl Popper, is what distinguishes science from pseudo-science and separates technical prediction from mere “prophecy.”²⁵ Clausewitz was sensitive to these limitations as well, noting that “no empirical science, consequently also no theory of the art of war, can always corroborate its truths by historical proof.”²⁶ Notwithstanding General George Patton’s assertion that the successful soldier must know history, recent scholarship by Daniel Kahneman, Phillip Tetlock, Nassim Talib, and others suggests substantive limitations in applying historical pattern analysis as a basis for predictive decisionmaking, particularly in the case of unstructured problems and complex systems.

Much of Kahneman’s work on bias and systematic error in expert judgment focuses on the limitations of derived heuristics in fields dependent on analysis of historical case study.²⁷ This mode of theorizing reinforces a powerful human tendency to think in terms of association, metaphor, and inferred causality, with cognitive strategies giving rise to rules of thumb based on crude pattern recognition. Kahneman suggests such techniques feed overconfidence based on the certainty of hindsight, leading planners to view the world as far more coherent and orderly than it is. Others have termed this



Command element from Arkansas Army National Guard's 142nd Fires Brigade looks over map of Woodruff County in eastern Arkansas in effort to deploy troops in support of evacuation operations due to flooding (DOD/Chris Durney)

tendency “folk science” whereby humans naturally create “illusions of explanatory depth” in their analysis of complex functions, often entirely unaware how this masks inaccuracies in understanding.²⁸ All of these factors entail what Kahneman calls the “planning fallacy,” or tendency to underestimate the difficulty of implementing a plan while simultaneously overestimating one’s ability to shape future outcomes.

However superficially military planning methodologies may resemble scientifically derived processes, Hayek reminds us that the enormous predictive power of the physical sciences is based on laws derived from experiments with relatively few variables that may be isolated and carefully measured, whereas complex social phenomena inevitably involve indeterminable variables either unmeasurable or unknown to the observer. Even in the best of circumstances, use of scientific-like methods of analysis offer little more than crude pattern prediction

or only a generalized understanding of system dynamics.

Clausewitz famously observed that “three quarters of the factors on which action in war is based are wrapped in a fog of greater or lesser uncertainty.”²⁹ Hayek certainly would agree. He reminds us that in fields where essential complexity exists, the planner must understand that “he cannot acquire the full knowledge which would make mastery of the events possible.”³⁰ Even as the methodologies of the physical sciences are lavishly imitated, the nature of the problems facing military planners cannot produce equally structured outcomes. One significant reason is that intelligence can never resemble the process of data collection in a laboratory, no matter the level of technical sophistication.

Conclusion

Having rediscovered the primacy of Clausewitzian ambiguity, some theorists now propose Army Design Theory as a

means to disentangle complex causality and deliver improved strategies of intervention. It is at this point where caution is warranted. An unfortunate symptom of military scientism has been the tendency for planners to conflate the precision of their tools (weapons and systems) with the methods of their application (theories and doctrine). While the technologies of modern warfare function primarily in a Newtonian universe, methods of their application still reside stubbornly in a Hayekian one. Confusion over this point gets to the heart of the dilemma with military scientism.

Arguably much of what passes for military planning is less analytically rigorous than what meets the eye. The fixtures of doctrinal orthodoxy have created an aura of pseudo-scientific infallibility in the military planning process, rendering its outputs impervious to rational critique. However, too often doctrine is little more

than a fig leaf concealing a process driven by gut-feeling heuristics and unsubstantiated causal suppositions. Whereas doctrine should serve the useful function of providing a common language and frame of reference, it also has the undesirable effect of reinforcing the cult of expertise, thereby discouraging integration of diverse tools and nontraditional thinking. This is where it becomes dangerous. As Malcolm Gladwell has noted, whereas incompetence is the malady of the novice, overconfidence is the disease of the expert.³¹ And it is generally the expert who possesses the greatest potential for creating disasters.

Clausewitz was well aware of the potential dangers of scientism and warned that “much greater is the evil which lies in the pompous retinue of technical terms—scientific expressions and metaphors” that “lose their propriety, if they ever had any, as soon as they are distorted, and used as general axioms, or as small crystalline talismans.”³² In this respect, a healthy dose of Hayekian thinking provides a natural “dampening effect” against unrealistic aspirations. While Hayek’s insights dealt primarily with functions of economic markets, the same dynamics apply to military conflict or any other human activity defined by conditions of uncertainty, analytical ambiguity, and predictive indeterminacy. What a Hayekian worldview demands is that one trade certainty for humility, appreciate the limits of useful knowledge, and recognize that plans do not represent extension of the will. Skepticism must be the order of the day, placing the burden of proof on the doctrinarian.

As proscription for correcting the worse abuses of military scientism, leaders might benefit from considering methods from other fields that at first glance may not seem intuitively similar to military operations such as biology, epidemiology, or meteorology. These disciplines may offer helpful examples for how military planners can better appreciate the natural limitations of their craft, improve techniques of meta-cognition, and gain greater sensitivity to the uses and abuses of probability. Likewise, repositioning military science as an academic discipline

of equal stature with established social sciences will invite both scrutiny over our methods as well as beneficial cross-pollination and improved awareness of our biases.

In the end, we must seek a defensible space between helpless indifference and the present hubris that drives the lofty ambitions of many military planners. One must appreciate that in some situations intuition, training, and experience are simply not enough to endow one with sufficient awareness to predict outcomes with a reasonable degree of certainty. Indeed, the ability to recognize these limits and approach them with humility and intellectual honesty is perhaps the truest mark of a professional. JFQ

Notes

¹ *Descriptive* theory based on retrospective analysis where variables and environmental conditions cannot be fully known or controlled, versus *predictive* theory offering falsifiable propositions subject to experimental testing and validation.

² *Scientism* as applied by Friedrich Hayek, Karl Popper, and others to describe inappropriate application of scientific-like methods to contexts where they do not clearly fit or with insufficient empirical evidence to support scientifically valid theories; also processes designed to appear science-like yet lacking rigorous procedural, methodological, or analytical standards.

³ Notably in Antoine Bousquet, *The Scientific Way of Warfare: Order and Chaos on the Battlefields of Modernity* (New York: Columbia University Press, 2009).

⁴ John Shy, “Jomini,” in *Makers of Modern Strategy: From Machiavelli to the Nuclear Age*, ed. Peter Paret, 146 (Princeton: Princeton University Press, 1986).

⁵ Among others, see Alan Beyerchen, “Clausewitz, Nonlinearity and the Unpredictability of War,” *International Security* 17, no. 3 (1992), 59–90, available at <www.clausewitz.com/readings/Beyerchen/CWZandNonlinearity.htm>.

⁶ Carl von Clausewitz, *On War*, trans. James John Graham (London: Trübner, 1873), book 2, chap. 4.

⁷ Ibid.

⁸ Bousquet, 30.

⁹ B.H. Liddell Hart, *Strategy of the Indirect Approach* (London: Faber and Faber, 1954), 234, available at <<http://archive.org/stream/strategyofindire035126mbp#page/n15/mode/2up>>.

¹⁰ B.H. Liddell Hart, *Why Don't We Learn from History* (Ann Arbor: Hawthorn Books, 1972), 16, available at <<http://pkpolitics.com/files/2008/05/liddell-hart-why-dont-we-learn-from-history.PDF>>.

¹¹ J.F.C. Fuller, *The Foundations of the Science of War* (London: Hutchinson, 1926), available at <www.cgsc.edu/Karl/download/csipubs/FoundationsofScienceofWar.pdf>.

¹² Ibid., 35.

¹³ Paul Kennedy, *Engineers of Victory: The Problem Solvers who Turned the Tide in the Second World War* (New York: Random House, 2013).

¹⁴ Martin van Creveld, *Command in War* (Boston: Harvard University Press, 1985), 106.

¹⁵ Antoine Bousquet, “Cyberneticizing the American War Machine: Science and Computers in the Cold War,” *Cold War History* 8, no. 1 (2008), 77–102.

¹⁶ Friedrich Hayek, “The Pretense of Knowledge,” *American Economic Review* 79, no. 6 (1989).

¹⁷ Friedrich Hayek, *The Fatal Conceit: The Errors of Socialism* (Chicago: University of Chicago Press, 1988), 76.

¹⁸ Friedrich Hayek, “The Use of Knowledge in Society,” *American Economic Review*, 4 (September 1945), 519–530, available at <www.econlib.org/library/Essays/hykKnw1.html>.

¹⁹ Ibid., 530.

²⁰ Carl von Clausewitz, *On War*, ed. and trans. Michael Howard and Peter Paret (Princeton: Princeton University Press, 1984), 117.

²¹ Hayek, “Pretense of Knowledge.”

²² Van Creveld, 240.

²³ Michael T. Flynn, Matt Pottinger, and Paul D. Batchelor, *Fixing Intel: A Blueprint for Making Intelligence Relevant in Afghanistan* (Washington, DC: Center for a New American Security, 2010), available at <www.cnas.org/files/documents/publications/AfghanIntel_Flynn_Jan2010_code507_voices.pdf>.

²⁴ Jim Manzi, *Uncontrolled: The Surprising Payoff of Trial and Error for Business, Politics, and Society* (New York: Basic Books, 2012), xi.

²⁵ Karl Popper, *The Poverty of Historicism* (New York: Routledge, 2002).

²⁶ Clausewitz, *On War*, trans. Graham, book 2, chap. 6.

²⁷ Daniel Kahneman, *Thinking Fast and Slow* (New York: Farrar, Straus, and Giroux, 2011).

²⁸ Leonid Rozenblit and Frank Keil, “The Misunderstood Limits of Folk Science: An Illusion of Explanatory Depth,” *Cognitive Science* 26, no. 5 (2002), 521–562.

²⁹ Clausewitz, *On War* (Princeton), 104.

³⁰ Hayek, “Pretense of Knowledge,” 7.

³¹ Malcolm Gladwell, C-SPAN interview with Brian Lamb, November 30, 2009.

³² Clausewitz, *On War*, trans. Graham, book 2, chap. 6.



Chairman and Admiral Samuel J. Locklear, USN, commander, U.S. Pacific Command, talk before departing Camp Smith, Hawaii (DOD/D. Myles Cullen)

The Best Man for the Job?

Combatant Commanders and the Politics of Jointness

by R. Russell Rumbaugh

The U.S. military today fights jointly. A joint commander—reporting to the Secretary of Defense—commands all Service components during military operations. And as a key sign of this jointness, com-

batant commanders no longer come solely from a single Service as they once did. In fact, the combatant commanders and their control of operations are often considered the greatest expression of jointness.

Yet the historical record suggests combatant commanders are not as joint as thought; a review of all combatant commanders by Service shows that each military branch has been represented roughly equally for the past 30 years.

This consistent balance strongly suggests that Service-based prerogatives still play a role in selecting who commands even the operational commands. If inter-Service politics pervades even the selection of combatant commanders, how much more might it affect those parts of the military commonly acknowledged as less joint—especially acquisition?

Such visible evidence of inter-Service politics belies the more hopeful claims for jointness, underlining that jointness

R. Russell Rumbaugh is Director, Budgeting for Foreign Affairs and Defense, and Senior Associate at The Stimson Center, Washington, DC.

is not a synonym for a unified military but rather a description of a loose collaboration among the Services. The U.S. military must stop using jointness as a euphemism and accept a loss of Service prerogative to ensure more effective defense administration and, more importantly, a more effective fighting force.

The Combatant Commands and Jointness

Combatant commanders sit at the pinnacle of operational command in the U.S. military system. Though the U.S. military is organized, trained, and equipped by the four Services—the Army, Marines, Navy, and Air Force—it is used by the combatant commanders. That is, when forces are tasked to a mission, they come under the charge of the combatant commander who plans and executes operations using forces from all the Services together. Combatant commands are divided between geographic and functional commands. For the geographic commands, the U.S. military divides the entire world into six commands that oversee all forces conducting missions in those regions: European, Pacific, Central, African, Northern, and Southern. The functional commands are Transportation, in charge of getting troops and equipment around the world; Strategic, responsible for operating all U.S. nuclear forces; and Special Operations, not surprisingly, in charge of all special operations forces. During operations, the combatant commander is responsible for effectively using and integrating forces from all Services. But when not tasked to a mission, these forces all belong to an administrative command, which reports through the chain of each distinct Service.

In the past, that administrative chain owned by the Services tended to overshadow the operational chain. Even in World War I, General John Pershing, commander of the American Expeditionary Force (AEF) in France, jockeyed with General Peyton March, the Chief of Staff of the Army in Washington, over what each had responsibility for and what the reporting chain was. According

to Pershing's Chief of Staff General James Harbord, as quoted by Kenneth Allard:

General Pershing commanded the AEF directly under the President and Secretary of War, as the President's alter ego. No military power or person was interposed between them. . . . No successful war has ever been fought commanded by a staff officer in a distant capital. . . . The organization effected in our War Department . . . scrupulously preserves the historic principle that the line of authority runs directly from the highest in the land to the highest in the field.

Allard notes, however, that “that principle was not as clear to some people as it apparently was to General Harbord.”¹

In World War II, the Joint Chiefs of Staff (JCS) arose as the body to adjudicate between the needs and desires of the theater commanders—though one of the four chiefs was Admiral William Leahy who was Chief of Staff to President Roosevelt, not one of the Services. After the war, the JCS was enshrined statutorily, creating blurry responsibility for the Service chiefs who were in charge of both the overall welfare of their Services and U.S. military operations.

President Dwight Eisenhower set out to clarify this confusion in 1958 when his reorganization plan explicitly made the chain of command direct from President to Secretary of Defense to combatant commanders, cutting out the Service chiefs. But this clarity existed only in theory because, in practice, the Service chains continued to exercise significant influence over the Service component commands overseen by each combatant command. The Goldwater-Nichols Department of Defense Reorganization Act of 1986 explicitly acknowledged this subversion of Presidential and legislative intent and succeeded in ending it.

Supporters of jointness rightly point to Goldwater-Nichols as a watershed moment in empowering the combatant commanders and true joint operations. Since then, most agree U.S. military operations have more effectively drawn on forces from all Services and wielded them as a powerful force that cuts across all domains. Combatant commanders no

longer represent their parent Service but the national interest. They are the best expression of how joint the U.S. military has become.

The Combatant Commands and the Services

Sitting at the pinnacle of operational command and exemplifying military jointness, combatant commanders are assumed to be chosen solely based on who is the best person for the job, regardless of what Service the commander comes from. Yet the consistent proportionality by Service of combatant commanders suggests that the Service they come from, and not only merit, matters in selection.

All the men (it has been only men so far) who have served in these positions have been accomplished people who have achieved a great deal in their careers, as one would expect. But considering these people individually ignores that the pool from which commanders are pulled only includes accomplished people with significant achievements; thus, such achievements may not tell us much about how or why each officer is selected. Acknowledging each officer as individually accomplished does not explain the continuity over time.

In the rare times when combatant commanders and their selection are considered systematically rather than individually, it is usually from a Service-centric perspective that bemoans an underrepresentation by one Service or another. For instance, a 2008 *Air Force Magazine* article titled “Why Airmen Don’t Command” purported to chronicle that Air Force officers are underrepresented in regional combatant commands.² Another example is a 2007 article in which “Retired Army Maj. Gen. Robert Scales, former head of the Army War College who holds a Ph.D. in history from Duke University, said he could find no prior period when the Army was so engaged overseas and so underrepresented at top levels.”³

These arguments not only miss but also obscure the most important aspect of who has commanded combatant

Chart. Combatant Commanders by Service

	Traditional Era																						
Year	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64	65	66	67	68	69
USEUCOM	A	A	A	A	A	A	A	A	A	A	F	F	F	F	F	F	A	A	A	A	A	A	A
USPACOM	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N
USSTRATCOM/SAC	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F
USSOUTHCOM/CARIBCOM		A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A
USJFCOM/ACOM/LANTCOM		N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N
USNORTHCOM/SPACECOM/ADCOM/CONAD								F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F
USSOCOM/REDCOM/STRICOM																A	A	A	A	A	A	A	A
USCENTCOM (FECOM)	A	A	A	A	A	A	A	A	A	A	A												
USTRANSCOM (NECOM)					F	F	F	F	F	F													
USAFRICOM (ALCOM)	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F

Chart. Combatant Commanders by Service (continued)

	Traditional Era (continued)																Rise of the Marines							
Year	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85	86	87	88	89	90	91	92	
USEUCOM	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	
USPACOM	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	
USSTRATCOM/SAC	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	
USSOUTHCOM/CARIBCOM	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	
USJFCOM/ACOM/LANTCOM	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	
USNORTHCOM/SPACECOM/ ADCOM/CONAD	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	
USSOCOM/REDCOM/STRICOM	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	
USCENTCOM (FECOM)														A	A	A	M	M	M	A	A	A	M	
USTRANSCOM (NECOM)																			F	F	F	F	F	
USAFRICOM (ALCOM)	F	F	F	F	F	F																		

Chart. Combatant Commanders by Service (continued)

	Rise of the Marines (continued)								Post-Rumsfeld												
Year	93	94	95	96	97	98	99	00	01	02	03	04	05	06	07	08	09	10	11	12	13
USEUCOM	A	A	A	A	A	A	A	F	F	F	M	M	M	M	A	A	A	N	N	N	F
USPACOM	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N
USSTRATCOM/SAC	F	N	N	F	F	N	N	N	N	N	N	N	M	M	M	F	F	F	F	F	F
USSOUTHCOM/CARIBCOM	A	A	A	A	A	M	M	M	M	A	A	A	A	A	N	N	F	F	F	F	M
USJFCOM/ACOM/LANTCOM	N	N	M	M	M	N	N	N	A	A	N	N	N	F	F	M	M	M	A		
USNORTHCOM/SPACECOM/ ADCOM/CONAD	F	F	F	F	F	F	F	F	F	F	F	F	N	N	F	F	F	N	N	A	A
USSOCOM/REDCOM/STRICOM	A	A	A	A	A	A	A	A	F	F	F	F	A	A	A	N	N	N	N	N	N
USCENTCOM (FECOM)	M	M	A	A	A	M	M	M	A	A	A	A	A	A	N		A	A	M	M	A
USTRANSCOM (NECOM)	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F
USAFRICOM (ALCOM)																A	A	A	A	A	A

Legend: A-Army, N-Navy, F-Air Force, M-Marine Corps

* For the majority of 2008, U.S. Central Command did not have a confirmed commander. Disestablished commands in parentheses; lineal descendants demarked by slashes. U.S. European Command, 1947–; U.S. Pacific Command, 1947–; U.S. Strategic Command, 1992–; SAC (Strategic Air Command), 1946–1992; U.S. Southern Command, 1963–; CARIBCOM (Caribbean Command), 1947–1963; U.S. Joint Forces Command, 1999–2011; ACOM (Atlantic Command), 1993–1999; LANTCOM (Atlantic Command), 1948–1992; U.S. Northern Command, 2002–; SPACECOM (Space Command), 1985–2002; ADCOM (Air Defense Command), 1975–1986; CONAD (Continental Air Defense Command), 1954–1975; U.S. Special Operations Command, 1987–; REDCOM (Readiness Command), 1971–1987; STRICOM (Strike Command), 1962–1971; U.S. Central Command, 1983–; FECOM (Far East Command), 1947–1957; U.S. Transportation Command, 1987–; NECOM (Northeast Command), 1950–1956; U.S. Africa Command, 2008–; ALCOM (Alaska Command), 1947–1975

commands: leaders representing an even balance among the military Services.

To demonstrate how well balanced across the Services the combatant commanders have been, we have to acknowledge two points: because the number of combatant commanders is so small we cannot just consider any given moment in time, and there have been changes over time in how the Services are represented in the combatant commands. Once we have accounted for these two points, we can offer an objective, quantitative comparison to see if inter-Service politics does affect how combatant commanders are chosen.

On the first point, there are currently only 9 combatant commanders, as many as there have ever been except for the 4 years after the creation of U.S. Africa Command (USAFRICOM) and before the dissolution of U.S. Joint Forces Command (USJFCOM), when there were 10. That means changes of just one commander can cause big swings in the percentage by Service, and since the average commander's tenure is less than 3 years, there are a number of changes in the slate of commanders. At any given moment, such changing rosters can give the impression of an unbalanced slate of commanders, substantiating those looking to believe a Service is underrepresented. To correct for these swings, we need to look at the combatant command rosters over time, which is easily done by considering the roster by combatant command by Service by year. So our basic unit is a flag officer from whichever Service held a combatant commander for the bulk of every year (commanders by Service by year). Even then, there is only a small sample size. But we can look over any time period we want and have a standard way to compare the balance of commanders by Service. See the chart for the history of the combatant commanders displayed this way.

As to the second point, times have changed since the original Unified Command Plan (UCP) was signed in 1946. But we must sort out what has changed. I argue there have been three distinct periods in the history of the combatant commands: the traditional era up

until 1986, the rise of the Marines from 1986 until 2001, and the post-Donald Rumsfeld era since.

Traditional Era

In the traditional era from 1946 until 1986, combatant commands were largely extensions of the Services. Each had its role in the world, the unified commands were how it executed that role, and therefore the commander of each command came from that parent Service. This is not to say that the commanders did not command forces from all the Services. In fact, the UCP was intended to acknowledge one Service's dominance over the others in region or mission, as the official history of the UCP states: "The impetus for the establishment of a postwar system of unified command over US military forces worldwide stemmed from the Navy's dissatisfaction with this divided command [between General of the Army Douglas MacArthur and Fleet Admiral Chester W. Nimitz] in the Pacific."⁴ The initial UCP did not actually resolve which five-star flag officer was in charge of the other, instead enshrining separate commands for the Army and Navy in the Pacific and further cementing the connection between the military Services and commands. Though jockeying continued between the Services over the shape of the commands and what regions or missions each controlled, five commands lasted throughout the 40 years of the traditional era: the Navy had Pacific Command and Atlantic Command, the Army had European Command and what became Southern Command, and the Air Force had the Strategic Air Command. The Army had two other commands: MacArthur's Far East Command, which was disestablished in 1957, and Strike Command, which was created in 1961, transitioned to Readiness Command, and eventually served as the administrative basis for U.S. Special Operations Command. In addition, the Air Force was responsible for various air defense commands.

Over the entire 40 years, there was only one instance where a commander

did not come from the traditionally associated military Service: from 1957 to 1962, the Air Force's Lauris Norstad commanded U.S. European Command (USEUCOM), a traditional Army command. The chart shows the long, unbroken years of single-Service combatant commands. Of course, we should not be surprised that during this traditional era the combatant commands were dominated by the Services. The traditional era is defined by the dominance of the Services over the combatant commands, and ending that dominance was one of the major goals of the 1953 and 1958 reorganizations, the recommendations of a Blue Ribbon Defense Panel in 1970, and the Goldwater-Nichols Act of 1986.

The Rise of the Marines

Goldwater-Nichols did succeed in breaking Service dominance of the combatant commands, but the legislative victory alone did not alter the pattern of who commanded each combatant command. Instead, the break required the rise of the Marine Corps as a full-fledged Service. Of the first four commands to be commanded by an officer not from its traditionally associated Service, three were commanded by Marines. The chart shows the late appearance of the Marines in red, at the first permanent break in the traditional affiliations.

The first Marine combatant commander was General George Crist of U.S. Central Command (USCENTCOM), who assumed command in November 1985, nearly a year before Goldwater-Nichols was signed into law. Maybe the more important law was the one signed in October 1978, which made the Commandant of the Marine Corps a full member of the Joint Chiefs of Staff. A year later, the Commandant exercised this new authority to join the Chief of Naval Operations in opposing the other members of the Joint Chiefs and arguing for creating the predecessor to USCENTCOM rather than assigning forces for the Middle East to the Army-controlled Readiness Command. This argument led to the creation of USCENTCOM's predecessor

under a Marine lieutenant general. Though an Army general commanded USCENTCOM when it was formally established in 1983, Crist then assumed command after which a “longstanding gentlemen’s agreement among the service chiefs called for an Army general to relieve the Marine.”⁵ This rotation held for 20 years until Army General John Abizaid replaced Army General Tommy Franks in the middle of the Iraq War.

The next break in traditional arrangements came in 1994 when a Navy admiral assumed command of the newly created U.S. Strategic Command, successor to the Air Force–run Strategic Air Command. With the end of the Cold War, the Navy was willing to subordinate its nuclear submarines to a consolidated Strategic Command, with the provision that the command would rotate between the Navy and Air Force.

The end of the Cold War and the new jointness of Goldwater-Nichols also underpinned the next Marine combatant commander, General John Sheehan at Atlantic Command in 1994. Under direction of Chairman of the Joint Chiefs of Staff Colin Powell, Atlantic Command had begun a transition from a predominantly maritime regional command to what was called a “joint force integrator” command. Reflecting this change, “Speculation in the past had been that [the present commander’s] replacement would come from the ranks of the Army or Air Force, even though the command has been considered a maritime command for nearly 50 years.”⁶ However, the Marine was given the job, which meant the Marines had assured their ascension by keeping a combatant command even as USCENTCOM rotated back to the Army.

Three years later, a Marine was the fourth break in the traditional relationship between the Services and commands, as General Charles Wilhelm took the traditionally Army-dominated U.S. Southern Command. The traditional era was over, and the Services no longer could assume control over the commands that had once seemed like hereditary fiefdoms. Goldwater-Nichols created the statutory authority, the end

of the Cold War created a strategic break from past assumptions, and, maybe most importantly, the rise of the Marine Corps proved a dramatic internal force to break the traditional relationship between the military services and the combatant commands.

Post-Rumsfeld Era⁷

Though the next break in traditional arrangements came before his tenure, Secretary of Defense Donald Rumsfeld forced the advent of a new era that seems to be holding.

Ironically, the next break after the rise of the Marines could be described as a rearguard action to restore the prerogatives of the military Services. In 2000, Air Force General Joseph Ralston replaced Army General Wesley Clark at USEUCOM, a traditional Army command. Though seemingly an example of breaking traditional relationships, Clark has implied that because he defended a combatant commander’s prerogatives in the face of Service resistance, he was replaced by a commander more inclined toward a Service perspective.⁸ In this case, one effect of Goldwater-Nichols may have overshadowed another.

But when Secretary Rumsfeld came to office, he was clear about his intention to break the traditional associations. As Andrew Hoehn, Albert Robbert, and Margaret Harrell state, “Rumsfeld was unsure, especially in the case of service leadership, that officers chosen by the current leadership—and, potentially, in the image of the current leadership—were best suited to question the status quo and lead a major transformation effort.”⁹ Also, Secretary Rumsfeld succeeded in putting nontraditional officers into commands: Marines were put into U.S. Strategic Command and USEUCOM, traditionally Air Force and Army commands, respectively. Navy admirals were put into U.S. Southern Command (USSOUTHCOM) and USCENTCOM, which despite the rise of the Marines had remained the province of generals from the ground forces. Another Navy admiral commanded U.S. Northern Command (USNORTHCOM), in charge of the

continental United States and traditionally the province of the Air Force for air defense. And an Air Force general was the first non-sea Service commander of U.S. Joint Forces Command, the descendant of Atlantic Command. All these changes are reflected in the hodgepodge the chart becomes after Rumsfeld takes office.

However, Secretary Rumsfeld’s failure may be the most interesting case. In 2004, Rumsfeld nominated Air Force General Gregory Martin to head the U.S. Pacific Command (USPACOM), which had only been led by Navy admirals since its inception in 1947. One news story commented: “The Navy will cash a lot of chips to keep this from happening,” a retired general officer stated. “Get ready for the fight of the century.”¹⁰ After questioning at his confirmation hearing by former Navy officer Senator John McCain about his role in awarding the air refueling tanker contract, General Martin withdrew his name, and a Navy admiral eventually took command of USPACOM, which to this day has only been commanded by a Navy admiral.

With the departure of Secretary Rumsfeld, the selection of combatant commanders reverted to a process closer to the traditional one. No further challenge to the Navy’s hold of USPACOM has appeared, and Strategic Command has reverted to command by the Air Force. But the new jointness still holds. Since Rumsfeld’s departure, a Navy admiral was given USEUCOM, an Air Force general USSOUTHCOM, and an Army general USNORTHCOM, all firsts.

Frustrated Jointness

Times have changed. The combatant commanders’ role in U.S. foreign policy and their relationship to the military Services have changed. But having acknowledged that change and by looking over time, we can assess whether inter-Service politics plays a role in selecting combatant commanders. The military Services today are represented in the combatant commands almost evenly, suggesting inter-Service politics still matters, though not in the same way as during the traditional era.

Table. Combatant Commanders by Service by Year

	By Numbers			By Percentage		
	Traditional	Rise of Marines	Post-Rumsfeld	Traditional	Rise of Marines	Post-Rumsfeld
	1947–1985	1986–2000	2001–2013	1947–1985	1986–2000	2001–2013
Army	109	47	32	37	35	27
Navy	77	32	36	26	24	30
Air Force	111	39	38	37	29	32
Marine Corps	0	15	14	0	11	12
	297	133	120			

During the traditional era, the Army, Navy, and Air Force allocated the combatant commands based on Service prerogatives. The Navy had fewer years of combatant commands because it did not share in the changing air defense commands the Air Force held or the functional command of first Strike and then Readiness Command the Army held. Of course, that was because the Navy did not want to be included in these commands: “The Navy and Marines wanted the Unified Command Plan to state that STRICOM [Strike Command] would consist only of Army and Air Force units. [Secretary of Defense Robert] McNamara refused but did not integrate Navy and Marine units into the command.”¹¹ During the traditional era, inter-Service politics and their effect on combatant commands were blatantly open.

Yet despite a supposed decrease in Service influence, the balance of commands among the Services is more pronounced in the periods since the traditional era. With the rise of the Marines, the balance of command among the big Services closed to within 6 percentage points. The Navy kept its slightly smaller number and the Army had a slightly greater number by having three full-time combatant commands and its rotation in USCENTCOM. The Marines—newly represented from 1986 on—receive less than half the commands than the other Services receive in any period, but are actually disproportionately represented compared to the Corps’ share of the number of general officers, which is slightly under 10 percent.

The trend toward balance continued in the post-Rumsfeld era with ever

greater parity, even though Secretary Rumsfeld had set out to diminish Service influence. In fact, during Secretary Rumsfeld’s tenure, the Army, Navy, and Air Force, respectively, had 18, 18, and 19 commands by year, with the Marines getting the other 8. The table displays the combatant commanders by Service by year, and the numbers and percentages show how evenly the commanders are pulled from the Services.

This balance is not just about appearances. The historical data are statistically consistent with a pattern of the three big Services each getting 3 out of 10 commands and the Marines getting the tenth. That is true for every period since the traditional era: from 1986 on, from 1986 to 2000, during Secretary Rumsfeld’s tenure from 2001 to 2007, or from 2001 on.¹² In fact, even the geographic combatant commands are shared roughly evenly from 2001 on with no statistically significant difference. The Air Force is getting a greater share of geographic commands today than ever before, a reality nearly the opposite of the Service-centric concern cited earlier. As mentioned, the sample is a small one, so swings of one or two can have a big effect on the distribution across Services. Yet when the slate of commanders is considered over time rather than just as a snapshot, there is a remarkable consistency of balanced representation among the Services.

The consistency suggests there is a need to treat the Services equally when combatant commands are allocated. Because, over time, each Service gets its share of men assigned to combatant command, there is only a slight change on the “rotating schedule that gave the

services ‘turns’ placing their top talent into specific positions, whether or not the person selected was the best fit for the position. This custom afforded each service a fair share of the top military positions,” which Hoehn, Robbert, and Harrell argue existed before Secretary Rumsfeld.¹³ Though it is highly unlikely that this balance among the Services is by chance, the balance itself does not prove that Service prerogatives cause it. But I would argue each Service is treated equally because today, more than a quarter of a century since Goldwater-Nichols, the Services still have independent political power, and the Secretary of Defense and President must be sensitive to that power. The Services in their own turn accept a fair share division of plums like combatant commands in order to keep the peace among themselves. This peace prevents significant inter-Service rivalry, but does so by accepting a shared and constrained role rather than forcing a full debate for the benefit of the civilian policymakers on the best man or Service or joint force for any given task.

Why It Matters and What to Do

If inter-Service politics still affects the most joint aspect of the U.S. military—the combatant commands—it most likely affects other aspects of the military, maybe even the outcomes of operations. To placate Service prerogatives, a commander or even the President may accept a less than strategically optimal set of forces or tasks. By doing so, a commander may, in turn, compromise U.S. national security objectives. Though almost no one argues that the skewing by Service interests today is as bad as it was in operations such as Grenada in 1983, it can still matter. Rajiv Chandrasekaran reported an example from Afghanistan and claims it affected the entire war effort:

The Marine commandant, Gen. James Conway, was willing to dispatch thousands of forces to Afghanistan as soon as the president approved a troop increase [but his] stipulations effectively excluded Kandahar. . . . Helmand was the next best option, even if it was less vital. . . . The consequences

were profound: By devoting so many troops to Helmand instead of Kandahar, the U.S. military squandered more than a year of the war.¹⁴

When inter-Service politics interferes with U.S. national security objectives, it is a matter of grave concern.

Affecting actual operations is the most severe effect of inter-Service politics, but it appears to be a rare occurrence. Much more common is the effect inter-Service politics has on the day-to-day running of the Pentagon, especially acquisition, where few observers would claim jointness has made much headway. Though Goldwater-Nichols attempted to reform the administrative side of the Defense Department as well as the operational, it was less successful. Inter-Service politics remains a potent force. For instance, a team from the Institute for Defense Analyses stated, “we found no instance in which the [Joint Capabilities Integration and Development System (the military’s joint requirements generating)] process significantly altered any solution originally proposed by a military service.”¹⁵ Requirements in turn have been cited as the primary cause for cost growth, and even irrelevancy, in acquisition programs, suggesting inter-Service politics lies at the heart of the administrative problems within the Department of Defense.

Maybe the presence of inter-Service politics is not so bad, and nothing needs to be done. After all, the Services represent hundreds of years of tradition and, for the most part, have achieved U.S. national security objectives. But the presence of inter-Service politics does undermine two popular theories: First, jointness has successfully integrated the four Services into an almost unified fighting force and achieved efficiency and commonality through the administrative and acquisition systems. Yet the presence of strong inter-Service politics suggests that jointness has served more as cover to allow the Services to remain dominant in their traditional roles and missions without fear of encroachment. And second, it suggests that the Services offer their unique paradigms of war to compete for who can best achieve U.S. national

security objectives. Yet instead of encouraging competition, inter-Service politics seems to have created a form of collusion among the Services despite their distinct strategic paradigms, and—as in the case of Afghanistan—that collusion may even affect operations.

At the least, we should stop pretending that jointness has fundamentally eroded Service political power and the Services serve as independent checks on each other. By questioning the platitudes that obscure operational and administrative choices, more salient factors such as cost, Servicemembers’ lives, and national security objectives can better inform policymakers’ decisions.

At the most, those in the uniformed military should more openly acknowledge their parochial concerns and either argue that their parochial perspective better achieves U.S. national security objectives than others’ perspectives or abandon them. The Secretary of Defense and his staff should consider inter-Service politics the primary problem facing U.S. defense and look to weed out its clouding of policy choices. And the President and Congress should consider whether structural reform is needed to change the bargaining advantages that create today’s inter-Service politics.

Today, the United States enjoys operational commanders with more authority than ever before to assemble and wield a joint force. Once selected, the combatant commanders represent national authority, not their parent Service. But even in this area of the greatest advance in jointness, inter-Service politics still intrudes. Though each of our combatant commanders has been an accomplished individual who has served his country well, he has also represented the underlying inter-Service politics that characterizes U.S. national defense. In other areas with less progress toward diminished Service political power, inter-Service politics looms even larger, creating many of the outcomes bemoaned so often. Until the U.S. military can truly be considered as a whole force, and not as distinct and separate baronies, U.S. national security will suffer. JFQ

Notes

¹ C. Kenneth Allard, *Command, Control, and the Common Defense* (New Haven: Yale University Press, 1990), 84–85.

² Rebecca Grant, “Why Airmen Don’t Command,” *Air Force Magazine*, March 2008.

³ “Army Brass Losing Influence,” Associated Press, June 15, 2007.

⁴ Ronald H. Cole et al., *The History of the Unified Command Plan: 1946–1993* (Washington, DC: Joint History Office, Office of the Chairman of the Joint Chiefs of Staff, 1995), 11.

⁵ Bernard Trainor, “Now Chiefs Fight for Command Nobody Wanted,” *The New York Times*, July 22, 1988.

⁶ Jack Dorsey, “Marine Expected to Win Top Post with Atlantic Command,” *The Virginian-Pilot*, August 26, 1994.

⁷ The latter two eras could be combined and called the joint era and it would still be an analytically descriptive distinction from the traditional era. But the extra division highlights the development of the changes and the acceleration under Secretary Rumsfeld.

⁸ David Kaiser, “The General in His Labyrinth,” *Los Angeles Times*, September 23, 2001.

⁹ Andrew R. Hoehn, Albert A. Robbert, and Margaret C. Harrell, *Succession Management for Senior Military Positions: The Rumsfeld Model for Secretary of Defense Involvement* (Santa Monica, CA: RAND, 2011), 23.

¹⁰ Elaine Grossman, “Rumsfeld Set to Shake Up Leadership at Two Key Combat Commands,” *Inside Defense*, May 13, 2004.

¹¹ Cole et al., 4.

¹² Performing a Chi-square test with three degrees of freedom, each period, respectively, has a p-value of 0.681, 0.392, 0.908, and 0.828. No period is statistically significant compared to the null hypothesis.

¹³ Hoehn, Robbert, and Harrell, 8.

¹⁴ Rajiv Chandrasekaran, “Obama’s troop increase for Afghan war was misdirected,” *The Washington Post*, June 22, 2012. Excerpt from *Little America: The War within the War for Afghanistan* (New York: Knopf, 2012), 64–66.

¹⁵ Gene Porter et al., *The Major Causes of Cost Growth in Defense Acquisition*, IDA Paper P-4531 (Alexandria, VA: Institute for Defense Analyses, December 2009), ES-11.



A Potent Vector

Assessing Chinese Cruise Missile Developments

By Dennis M. Gormley, Andrew S. Erickson, and Jingdong Yuan

Dennis M. Gormley is a Senior Lecturer and Cruise Missile Expert in the Graduate School of Public and International Affairs at the University of Pittsburgh. Dr. Andrew S. Erickson is an Associate Professor in the Strategic Research Department at the U.S. Naval War College. Dr. Jingdong Yuan is an Associate Professor in the Department of Government and International Relations at the University of Sydney. This article draws on the authors' book *A Low-Visibility Force Multiplier: Assessing China's Cruise Missile Ambitions* (NDU Press, 2014).

The numerous, increasingly advanced cruise missiles being developed and deployed by the People's Republic of China (PRC) have largely flown under the public's radar. This article surveys PRC cruise missile programs and assesses their implications for broader People's Liberation Army (PLA) capabilities, especially in a Taiwan scenario.

This article draws on findings from a multiyear comprehensive study of Chinese cruise missiles based exclusively on open sources. More than 1,000 discrete Chinese-language sources were considered; several hundred have been incorporated in some form. In descending level of demonstrated authority, these Chinese sources include PLA doctrinal publications (for example, *Science of*

Campaigns) describing how cruise missiles might be used in operational scenarios; specialized technical analyses (*Winged Missiles Journal*) from civilian and military institutes detailing many specific aspects of such weapons and their supporting infrastructure; didactic PLA discussions (*Modern Navy* and *People's Navy*); generalist deliberations on the development trajectory and operational use of cruise missiles (*Naval and Merchant Ships* and *Modern Ships*); and unattributed speculation on a variety of Web sites. To be accessible to a general audience, this article includes only a fraction of the several hundred citations found in the full study, together with several related sources.

These Chinese sources were supplemented with a wide variety of English-language sources, including—in descending level of demonstrated authority—U.S. Government reports, analyses by scholars and think tanks, and online databases. The authors drew on their combined technical, arms control, and Chinese analysis experience to compare and assess information for reliability.

The result is a study whose details must be treated with caution, but whose larger findings are likely to hold.

Overview

China's military modernization is focused on building modern ground, naval, air, and missile forces capable of fighting and winning local wars under "informatized conditions." The principal planning scenario has been a military campaign against Taiwan, which would require the PLA to deter or defeat U.S. intervention. Beijing is now broadening this focus to its Near Seas (Yellow, East, and South China seas) more generally.

The PLA has sought to acquire asymmetric "assassin's mace" technologies and systems to overcome a superior adversary and couple them to the command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) systems necessary for swift and precise execution of short-duration, high-intensity wars.

A key element of the PLA's investment in antiaccess/area-denial (A2/

AD) capabilities is the development and deployment of large numbers of highly accurate antiship cruise missiles (ASCMs) and land-attack cruise missiles (LACMs) on a range of ground, naval, and air platforms. China's growing arsenal of cruise missiles and the delivery platforms and C4ISR systems necessary to employ them pose new defense and nonproliferation challenges for the United States and its regional partners.

Military Value

Chinese writers rightly recognize cruise missiles' numerous advantages. Cruise missiles are versatile military tools due to their potential use for precision conventional strike missions and wide range of employment options. Although China appears heavily focused on precision conventional delivery, cruise missiles could also be employed to deliver nuclear, biological, or chemical weapons. Due to their superior aerodynamic flight stability compared to ballistic missiles, cruise missiles—by conservative estimates—enlarge the lethal area for biological attacks by a factor of 10.

Modern cruise missiles offer land, sea, and air launch options, allowing a "two-stage" form of delivery that extends the already substantial range of the missiles themselves. They may also be placed in canisters for extended deployments in harsh environments. Because cruise missiles are compact and have limited support requirements, ground-based platforms can be highly mobile, contributing to prelaunch survivability. Moreover, cruise missiles need only rudimentary launch-pad stability, enabling shoot-and-scoot tactics.

Since cruise missile engines or motors do not produce prominent infrared signatures on launch, they are not believed to be detectable by existing space-warning systems, reducing their vulnerability to post-launch counterforce attacks. The potential combination of supersonic speed, small radar signature, and very low altitude flight profile enables cruise missiles to stress naval- and ground-based air defense systems as well as airborne surveillance and tracking radars, increasing the likelihood that they will successfully

penetrate defenses.¹ Employed in salvos, perhaps in tandem with ballistic missiles, cruise missiles could saturate defenses with large numbers of missiles arriving at a specific target within a short time.

At the same time, optimal employment of cruise missiles imposes significant requirements: accurate and timely intelligence, suitable and ideally stealthy and survivable delivery platforms, mission planning technology, command, control, and communications systems, and damage assessment. China has lagged in these areas, but its experts recognize their importance, and the relevant Chinese organizations are working hard to make progress.

Institutional and Organizational Actors

China began introducing ASCMs into its inventory in the late 1950s. The Fifth Academy under China's Ministry of National Defense was assigned the lead role in coordinating national efforts in ASCM research, design, and licensed production. Established in 1956 with U.S.-trained scientist Qian Xuesen as its first director, the Fifth Academy was instrumental in China's cruise missile development. Acting on guidance from the Central Military Commission, in 1958 the PLA Navy (PLAN) headquarters built an ASCM test site at Liaoxi, Liaoning Province.

Following several bilateral agreements, the Soviet Union transferred Type 542 KS-1 Komet (North Atlantic Treaty Organization [NATO] designation: SSC-2A Salish) shore-to-ship and Type 544 P-15 Termit (NATO designation: SS-N-2A Styx) antiship missiles, models, and technical data to China beginning in 1959. Moscow was to assist Beijing with these and other missile programs. The P-15 would provide the basic foundation for China's future development of more advanced ASCMs and eventually LACMs.

In 1960, Nanchang Aircraft Manufacturing Company established an assembly line to initiate ASCM production; it would later produce Shangyou-, Haiying-, and Yingji-series ASCMs. Despite the departure of Soviet advisors

in September 1960, China conducted its first successful missile test that November. In 1964, China's first ASCM, a license-produced version of the P-15, passed factory tests. The following year, its first flight test was successful. In late 1967, the resulting "Shangyou-1" missile was approved for production, and it entered service in the late 1960s.²

As part of China's efforts to develop an indigenous defense industry base, cruise missile programs received high-level political support from the beginning. In 1969, Zhou Enlai reportedly approved the establishment of a Military Industry Enterprise Base to produce ASCMs. Top leaders allocated funding and human capital and helped protect programs from political interference during the Cultural Revolution.

Yet this support has an important caveat: political leaders placed the highest priority on nuclear and ballistic missile programs given their strategic deterrence function. Cruise missiles, while prioritized more highly than aircraft and some other armaments, suffered from their logical application as armaments for the air force and navy and were subordinated to ground forces. Moreover, as the early Nanchang connection indicates, ASCMs were initially developed within China's aviation industry. This fact, and the industry's connection to a politically suspect PLA Air Force (PLAAF), imposed significant limitations.

Cruise missile programs therefore encountered more problems and registered slower progress than their ballistic missile counterparts. Not until the late 1960s and early 1970s was China able to produce its own modified derivatives of early Soviet-model cruise missiles. While recent years have witnessed remarkable progress in ASCMs such as the YJ-62 and LACMs such as the YJ-63/AKD-63 and DH-10, China continues to rely on foreign technological support—particularly Russian and Ukrainian design assistance.

To address persistent problems in its defense research, development, and acquisition system, China has converted numbered ministries to corporations, encouraged competition (with mixed results), and separated military

requirements and evaluations (General Armaments Department) from civilian defense industry management and production (formerly the Commission of Science, Technology, and Industry for National Defense, now the State Administration for Science, Technology, and Industry for National Defense). China has simultaneously worked to maximize access to foreign technology and employs an extensive bureaucracy to facilitate its transfer (very effectively) and absorption (less effectively).

China's cruise missile design, research, development, and manufacturing are now concentrated in a single business division within one of two state aerospace conglomerates, the China Aerospace Science and Industry Corporation (CASIC) Third Academy. One of seven design academies under CASIC—which has over 100,000 employees—the Third Academy is China's principal research and development (R&D) and manufacturing entity for cruise missiles; all others are secondary. Established in 1961, the Third Academy has been involved in the design and development of 20 types of cruise missiles, including the indigenous Haiying- and Yingji-series and their export versions.³ Today, it boasts 10 research institutes and 2 factories, with over 13,000 employees, including 2,000 researchers and around 6,000 technicians.

China's aviation industry remains involved in cruise missile R&D and production. Hongdu Aviation Industry Group (formerly Nanchang Aircraft Manufacturing Company), under Aviation Industry Corporation of China, produced Feilong-series cruise missiles for export.⁴

Finally, for three decades China has marketed a wide range of indigenously produced cruise missiles (and other weapons systems) through China Precision Machinery Import and Export Corporation (CPMIEC), the CASIC Third Academy's export management branch. Established in 1980, CPMIEC is a member of the Xinshidai Group and jointly owned by CASIC and the Chinese Aerospace Science and Technical Corporation.

Antiship Cruise Missile Developments

Like other nations, China has come to regard ASCMs as an increasingly potent means of shaping the outcome of military conflicts and thereby also strengthening peacetime deterrence. China has developed its own advanced, highly capable ASCMs (the YJ series) while also importing Russian supersonic ASCMs, which have no operational Western equivalents. (See table 1 for a list of Chinese ASCMs.)

China's most sophisticated and threatening imported Russian ASCMs include the 3M80E and 3M80MVE Moskit (NATO designation: SS-N-22 Sunburn) and the 3M54E Klub (NATO designation: SS-N-27B Sizzler). China's *Sovremenny*-class destroyers (Project 956E and 956EM) boast the supersonic Sunburn ASCMs that were first delivered to China in 2000–2001. The Project 956E ships carry the early 3M80E missile with a range of 120 kilometers (km), while the Project 956EM destroyers have the 3M80MVE that has an optional longer range (240 km) through the incorporation of a second, high-altitude flight profile setting. But this longer range comes at a price, as a 3M80MVE missile using the higher altitude profile would be detectable at much greater distances and thus more vulnerable to attacks from advanced air defense systems, such as Aegis. Both missiles execute sea-skimming attacks at an altitude of 7 meters and perform terminal maneuvers to reduce the target's point defense systems effectiveness. The Sunburn is reported to have a speed of Mach 2.3 and has a 300-kilogram (kg) semi-armor piercing warhead.⁵

Eight of China's *Kilo*-class submarines are Project 636M variants fitted with the Klub-S missile system, which includes the 3M54E/SS-N-27B Sizzler ASCM—also known earlier as Novator Alpha. This missile is unique in that it combines a subsonic, low-altitude approach with a supersonic terminal attack conducted by a separating sprint vehicle. The 3M54E's cruise range is 200 km at a speed of Mach 0.6–0.8. This is followed by the release of a solid-rocket-propelled,

sea-skimming sprint vehicle that travels the last 20 km to the target at a speed of Mach 2.9. The 3M54E ASCM has a 200-kg semi-armor-piercing warhead.

As in so many other areas, even as China seeks the best foreign systems available, it continues to develop increasingly capable indigenous systems. Of China's foremost indigenous ASCMs, the YJ-82 and YJ-83/83K are the most widely deployed, while the YJ-62 is among the most advanced. The YJ-82 is a solid-rocket-propelled, submarine-launched missile contained in a buoyant launch canister that is, for all intents and purposes, identical to the U.S. submarine-launched Harpoon. While credited with a range of 42 km, the lack of a solid-rocket booster, as with the surface-ship-launched YJ-8/8A, strongly suggests that the YJ-82's range will be shorter. The missile has a speed of Mach 0.9 and a terminal sea-skimming attack altitude of 5 to 7 meters, and it carries a 165-kg high-explosive fragmenting warhead.⁶

The YJ-83/83K missile represents an evolutionary improvement over the YJ-8/8A and the exported C802. Entering service with the PLAN in 1998–1999, the YJ-83 missile has the same propulsion system as the export C802 missile but uses an indigenous CTJ-2 turbojet instead of the French-made TRI 60-2. By replacing the bulky electronics and inertial reference unit (IRU) of the YJ-8/8A/C802 with digital microprocessors and a strap-down IRU, additional volume was made available to increase the YJ-83's range to 180 km at a speed of Mach 0.9. The air-launched YJ-83K has a rated range of 250 km at the same speed. Both the YJ-83 and 83K possess a slightly larger high-explosive fragmenting warhead of 190 kg. The YJ-83 is the main ASCM of the PLAN and is currently outfitted on virtually every surface combatant in active service. The YJ-83K can be carried by large and small aircraft alike and has been seen on JH-7/A fighter-bombers and H-6 bombers. The export variant of the YJ-83/83K is the C802A and the air-launched C802AK.⁷

In September 2005, China unveiled the C602 ASCM for the first time. The

Table 1. PLA Antiship Cruise Missiles (Major Systems)

Type	Manufacturer	Launch Platform	Range (km)	Payload (kg)	Speed	Guidance (inertial/terminal)
YJ-7 (C-701)	CASIC Third Academy	Ground, ship, air	25	30.5	Subsonic	Electro-optical/active radar
YJ-62 (C-602) and YJ-62A	CASIC Third Academy	Ship— <i>Luyang II</i> , ground	280–400 (YJ-62A)	210	Subsonic	Inertial/active terminal guidance
YJ-8 series (CSS-N-4 Sardine/C-801)	CASIC Third Academy	Ship, submarine, (YJ-82), air (YJ-81)	42	165	Subsonic	Inertial/active terminal guidance
YJ-83 (CSS-N-8 Saccade/C-802) multiple variants	CASIC Third Academy	Ship, ground, air	120 (ground/ship), 130 (air)	165	Subsonic	Inertial/active radar
YJ-83A/J (C-802A) multiple variants	CASIC Third Academy	Ship, submarine (?), ground, air	180 (ground/ship), 250 (air)	165	Subsonic	Inertial/active radar
YJ-91/KR-1 (Kh-31P)	Zvezda-Strela, Russia; indigenized by China	Ship, air (PLAAF/PLAN)	15–110	87–90 kg HE blast/fragmentation	Supersonic	Passive/Anti-radiation
AS-13 Kingbolt (Kh-59MK)	Raduga, Russia	PLAAF Su-30MKK	45–115	320 kg AP HE or 280 kg cluster	Subsonic	Inertial and TV/electro-optical
SS-N-22/Sunburn 3M80E Moskit; 3M80MVE (improved variant)	Raduga (Russia)	Ship; Project 956 <i>Sovremenny</i> destroyers; 3M80MVE on Project 956EM <i>Sovremenny</i> destroyers	120–240 (3M80MVE)	300	Supersonic	inertial/active/passive
SS-N-27B/Sizzler	Novator (Russia)	Submarine— <i>Kilo</i> Project 636M	200	200	Supersonic	INS/active
CH-SS-NX-13		Submarine— <i>Song, Yuan, Shang</i> , to be deployed on <i>Tang</i>	?	?	?	?

Source: Dennis M. Gormley, Andrew S. Erickson, and Jingdong Yuan, *A Low-Visibility Force Multiplier: Assessing China's Cruise Missile Ambitions* (Washington, DC: NDU Press, 2014), 18–19.

small-scale model was clearly larger than the one of the C802 nearby, and the system brochure boasted of a longer range (280 km), global positioning system (GPS) guidance—an unprecedented claim—and a larger semi-armor-piercing warhead (300 kg). The missile size was roughly consistent with large round launch canisters that had started showing up on coastal defense test sites and the Type 052C destroyers then under construction in 2004. The indigenous YJ-62 is very similar to the YJ-83 technologically and largely reflects an evolutionary change in size. While many

journals, articles, and Web sites quote the YJ-62's range as 280 km, this value is only appropriate to the export C602. China has limited the range of its export cruise missiles in conformance with the Missile Technology Control Regime restrictions of 300 km. The YJ-62 itself has a true range on the order of 400 kms. The long range likely necessitated the need for satellite navigation, and the YJ-62 is described as having the ability to use both GPS and Beidou constellations. The missile's speed is between Mach 0.6 and 0.8, and it executes a sea-skimming terminal attack at 7 to 10 meters. With

Table 2. PLA Land-attack Cruise Missiles

Type	Manufacturer	Launch Platform	Range (km)	Payload (kg)	Speed	Guidance
YJ-63/KD-63	CASIC Third Academy/CHETA	Air (H-6H and H-6K bomber)	200	500	Subsonic	INS/(?)/Passive Electro-optical terminal guidance
DH-10/CJ-10	CASIC Third Academy/CHETA	Ship, ground (3 canister on TELs)	1,500+	500	Subsonic	INS/Sat/TERCOM/Probable DSMAC for terminal guidance
KD-88	CASIC Third Academy/CHETA	Air	180–200	165	Subsonic	Inertial; active terminal guidance
KD-20/YJ-100	CASIC Third Academy/CHETA	Air	1,500–2,000	500	Subsonic	INS/Sat/TERCOM
Possible DH-2000	CASIC Third Academy/CHETA	Submarine	?	500	Subsonic	?
YJ-91/KR-1 (Kh-31P)	Zvezda-Strela, Russia; license-produced by China	Air (PLAAF/PLAN)	15–110	87–90 kg HE blast/fragmentation	Supersonic	Passive/Antiradiation
AS-13 Kingbolt (Kh-59MK)	Raduga, Russia	PLAAF Su-30MKK	115	320 kg AP HE or 280 kg cluster	Subsonic	Inertial and TV/electro-optical

Source: Gormley, Erickson, and Yuan, 25–26.

the exception of the Type 052C destroyers, the YJ-62 is only deployed in mobile coastal defense batteries.⁸

Finally, China has been working diligently on producing its own supersonic cruise missiles after the failed YJ-1/C101 and HY-3/C301. Both the YJ-12 and YJ-18 are undergoing tests and represent the next phase in China's ASCM capabilities. The YJ-12 appears to be a considerably lengthened Russian Kh-31-type missile and is speculated to have a range of 250 km and a speed of Mach 2.5. The YJ-12 is probably an aircraft-carried weapon only. Thus far, only certain H-6 bombers have been seen with a long pylon necessary to support a large missile with an integrated ramjet/booster propulsion system.⁹

The YJ-18 appears to be a Chinese copy of the 3M54E Klub. This missile has been described as having a cruise range of 180 km at Mach 0.8 and a sprint range of 40 km at Mach 2.5 to 3.0. It has been reported to be submarine torpedo tube-capable, which is consistent with

the CH-SS-NX-13 missile discussion in the Department of Defense's 2010 and 2011 annual reports to Congress. The YJ-18 has also been characterized as being able to be launched from a surface ship's vertical launching system (VLS), which is consistent with the capabilities of the generalized or universal VLS being fitted to the new Type 052D destroyer.¹⁰

Along with the growing improvements in ASCM performance, the PLAN has begun to expand its training and has become more diverse and realistic in recent years with increasing focus on cruise missile operations. Beijing has furnished its ASCMs with improved guidance and has started to implement satellite navigation capabilities. Most of the PLAN warships now have a dedicated over-the-horizon (OTH) targeting system, either the Russian-supplied Mineral-ME, or the indigenous version. Still, OTH targeting remains a challenge.

Chinese researchers are studying how to best overcome Aegis defenses and target adversary vulnerabilities. ASCMs

are increasingly poised to challenge U.S. surface vessels, especially in situations where the quantity of missiles fired can overwhelm Aegis air defense systems through saturation and multi-axis tactics. More advanced future Chinese aircraft carriers might be used to bring ASCM- and LACM-capable aircraft within range of U.S. targets.

A consistent theme in Chinese writings is that China's own ships and other platforms are themselves vulnerable to cruise missile attack. But China appears to believe it can compensate by further developing its capacity to threaten enemy warships with large volumes of fire.

Land-Attack Cruise Missile Developments

China has deployed two subsonic LACMs, the air-launched YJ-63/AKD-63 with a range of 200 km and the 1,500+ km-range ground-launched DH-10. (See table 2 for a list of Chinese LACMs.) Both systems benefited from ample technical assistance from foreign sources, primarily the Soviet Union/Russia. The first-generation YJ-63 is an air-launched LACM that employs an electro-optical (EO) seeker with man-in-the-loop steering via a command data link. This missile reportedly reached initial operating capability in 2004, was first seen in 2005 in Internet photography, and is right at the cusp as to when China incorporated satellite navigation in some of their weapons systems. It is currently unknown if the YJ-63/AKD-63 has this ability.¹¹ In addition to the YJ-63, two other LACMs use some sort of a command data link to feed back the data gathered from the EO sensor: the YJ-83KH and the K/AKD-88.¹² The second-generation DH-10 has a satellite navigation/inertial guidance system, but may also use terrain contour mapping for redundant midcourse guidance and a digital scene-matching sensor to permit an accuracy of 10 meters. Development of China's *Beidou/Compass* navigation-positioning satellite network is partly intended to eliminate dependence on the U.S. GPS for guidance.

Beijing has purchased foreign systems and assistance to complement its own indigenous LACM efforts. From Israel, it has received Harpy antiradiation drones with standoff ranges of 400+ km. It is conceivable that China may also have the Russian Klub 3M-14E SS-NX-30 LACM, which can be launched from the PLAN's Project 636M *Kilo*-class submarines and deliver a 400-kg warhead to a range of 300 km. But there is little evidence at present to support this possibility.

While current DH-10 ground-launch cruise missiles and YJ-63/AKD-63 air-launched systems are most relevant for a Taiwan contingency, there are strong signs that China is expanding its inventory to include both air-launched and ship-launched LACMs. An air-launched version of the DH-10, called the CJ-20, has reportedly been tested on the H-6 bomber, which has the capability to carry four CJ-20 LACMs externally.

China's Weapon Test Ship *Dahua* 892 has experimented with on-deck canister launchers that contain either YJ-18 ASCMs or DH-10 LACMs for at-sea testing.¹³ Although most PLAN surface combatants have a limited capacity of 8 to 16 canister launchers—meaning tradeoffs between ASCMs and LACMs—China's apparent interest in a sea-launched DH-10 strongly suggests that future PLAN destroyers, such as the new Type 052D, will likely be equipped with a new vertical launching system, with a greater capacity to carry both ASCMs and LACMs.

Should China add large numbers of air- and sea-launched LACMs to its already substantial inventory of ground-launched cruise missiles, it would significantly extend the range of the PLA's capacity to employ LACMs to deal with contingencies beyond Taiwan and the rest of its immediate maritime periphery.¹⁴ Time and dedicated effort will increase the PLA's ability to employ LACMs, even in challenging combined-arms military campaigns.

Cruise Missile Platforms

A given type of cruise missile can typically be launched from many different

platforms. Over the past decade, the PLA has commissioned numerous new, modernized ships, submarines, and aircraft capable of launching cruise missiles. China has produced a new array of frigates and destroyers that carry sophisticated medium- to long-range ASCMs, and some PLAAF/PLAN aviation aircraft can carry LACMs in addition to ASCMs. *Song*-, *Kilo*-, and *Yuan*-class diesel submarines are equipped with Russian and indigenous ASCMs. *Shang*-class nuclear-powered submarines have or will have ASCMs, as will their Type 095 follow-ons when they enter service.¹⁵ China thus appears to be making a concerted effort to develop its delivery capabilities from air, surface, and subsurface platforms simultaneously. In the near term, China will likely continue to expand its cruise missile inventory and precision delivery capabilities.

Cruise Missile Employment, Doctrine, and Training

China's new ASCM and LACM programs—like its current military modernization efforts more broadly—are focused on preparing for contingencies in the Taiwan Strait and other proximate disputed areas, which clearly include the possibility of U.S. intervention. The land, sea, and air components of such a contingency would involve ASCMs and LACMs. China appears to believe in the value of large-scale attacks in all three domains.

Since President Bill Clinton's decision to deploy two aircraft carriers to waters near Taiwan in response to China's March 1996 ballistic missile tests, PLA planners have focused on U.S. aircraft carriers as the main threat to the success of such PLA missions. Chinese strategists have thus sought ways to target U.S. carrier strike groups (CSGs); Chinese specialists are acutely aware of carrier vulnerabilities, having conducted a wide variety of research directed toward threatening aircraft carriers with "trump cards" such as cruise missiles. *Aegis* ships are also viewed as essential targets; without their protection, carriers are much more vulnerable to attack.

Various Chinese writings and the logical employment of forces China has been developing suggest that in the event of a maritime conflict with U.S. forces, the PLAN is likely to undertake massive multi-axis ASCM attacks against U.S. CSGs and their *Aegis* air defense perimeters. The PLAN's focused experimentation and training in long-range sea strike, its variety of indigenous ASCM weapons, and modernization of ASCM delivery platforms may yield a high probability of success for this effort.

Potential Employment in a Taiwan Scenario

Chinese ASCMs and LACMs could be used in conjunction with other A2/AD capabilities to attack U.S. and partners' naval forces, land bases, and sea bases that would be critical for U.S. efforts to respond to a Chinese attack on Taiwan. While cross-Strait relations are relatively stable at present, Beijing worries that that could change, and in any case wants to achieve reunification in peacetime, supported in part by its increasing military advantage over Taiwan.

Operating in tandem with China's huge inventory of conventionally armed ballistic missiles, LACMs could severely complicate Taiwan's capacity to use its air force to defend against Chinese attacks. Chinese military planners view LACMs as particularly effective against targets requiring precision accuracy (for example, airfield hangars and command and control facilities). They also view large-salvo attacks by LACMs and ballistic missiles as the best means to overwhelm enemy missile defenses.

Chinese planners emphasize the shock and paralytic effects of combined ballistic and LACM attacks against enemy airbases, which could greatly increase the effectiveness of follow-on aircraft strikes. These effects depend significantly on the number of launchers available to deliver missiles. China currently has between 255 and 305 ballistic missile and LACM launchers within range of Taiwan, which are capable of delivering sustained pulses of firepower against a number of critical airfields, missile defense sites, early warning radars, command and control



JH-7A fighter-bomber carrying KD-88 land-attack cruise missiles and drop tanks (Courtesy Sino Defense)

facilities, logistical storage sites, and critical civilian infrastructure such as electrical distribution.¹⁶

Proliferation Implications

If China's past record of proliferating ballistic missiles and technology is any indication of its intentions vis-à-vis cruise missile transfers, the consequences could be highly disruptive for the nonproliferation regime and in spreading A2/AD capabilities. China has sold ASCMs to other countries, including Iran. Beijing is suspected of furnishing Pakistan with either complete LACMs or components for local assembly.

China is not a full member of the 34-nation Missile Technology Control Regime (MTCR) but has pledged to adhere to the MTCR's guidelines for missile and missile technology exports. Beijing began seeking MTCR membership in 2004 but has thus far been denied due to concerns about its poor proliferation record. The reason why China represents a critical wildcard regarding the further spread of cruise missiles is that Beijing's current compliance with its pledge to

follow MTCR guidelines is problematic, especially regarding cruise missiles and unmanned aerial vehicles. China needs not only to improve its commitment to address shortcomings in implementation and enforcement but also to work with exporters on improving their compliance with export control regulations and increase its own governmental capacity to deal with the explosive growth of exporting industries across China's huge landmass. This would require significant efforts on China's part. However, if China becomes a fully compliant MTCR member, it would be an important achievement in limiting widespread LACM proliferation.

Conclusion

China has invested considerable resources both in acquiring foreign cruise missiles and technology and in developing its own indigenous cruise missile design and production capabilities. These efforts are bearing fruit in the form of relatively advanced ASCMs and LACMs deployed on a wide range of older and modern air, ground, surface-ship, and subsurface platforms.

To realize the full benefits, China will need additional investments in all the relevant enabling technologies and systems required to optimize cruise missile performance. Shortcomings remain in intelligence support, command and control, platform stealth and survivability, and post-attack damage assessment, all of which are critical to mission effectiveness. To employ cruise missiles to maximum effect, the PLA needs to be able to locate targets at a distance, to deploy its air, surface, and submarine platforms within range of those targets, and then to execute a complex, carefully orchestrated joint air and missile campaign—potentially over many days. Operational success also requires accurate, near-real-time intelligence and post-attack assessment capabilities.

A successful campaign depends on both human and technical factors—extremely well-trained military personnel who have practiced these routines in diverse ways over many years and the command and control architecture needed to deal with complex combined-arms operations. Chinese planners envision establishing a Firepower

Coordination Center within the Joint Theater Command, which would manage the application of air and missile firepower. Separate coordination cells would be created to deal with missile strikes, airstrikes, special operations, and ground and naval forces. Absolutely critical to achieving the delicate timing separating waves of missile strikes designed to leverage the effectiveness of subsequent aircraft attacks is developing the skill to coordinate and deconflict large salvos of missiles and waves of aircraft operating in multiple sectors. Chinese doctrine calls for such attacks, but the PLA's ability to execute such a complex joint campaign against a capable adversary has never been demonstrated.

The future development of China's cruise missile systems will depend on multiple factors. One is the role of ASCMs/LACMs in Chinese defense doctrines and military campaign strategies and their relative cost-effectiveness compared to other weapons systems. Second, cruise missile development, and indeed China's overall defense modernization, will be determined by the government's priorities as Beijing assesses its economic, social, and defense needs against the security environment and real and perceived threats. Third, U.S. military developments, including missile defenses, its own deployment and use of offensive weapons, and its intentions, will influence how China will react and thus the role of cruise missiles within PLA doctrine and force structure. Finally, the capabilities of China's defense industry will continue to be a critical factor in whether Chinese cruise missiles can continue to develop and close the technical gap with other major powers such as the United States and Russia.

ASCMs and LACMs have significantly improved PLA combat capabilities and are key components in Chinese efforts to develop A2/AD capabilities that increase the costs and risks for U.S. forces operating near China, including in a Taiwan contingency. Effective ASCMs give the PLAN an expeditionary capability and the ability to deploy and take on other navies. LACMs give China new conventional strike options. These

apply most to Taiwan, where ground-, air-, and sea-based systems could be employed, but some Chinese LACMs also have the range to reach Japan and the U.S. territory of Guam and will provide a limited capability wherever the PLAN can deploy. China plans to employ cruise missiles in ways that exploit synergies with other strike systems, including using cruise missiles to degrade air defenses and command and control facilities to enable follow-on airstrikes.

Defenses and other responses to PRC cruise missile capabilities exist, but they require greater attention and a more focused effort. They include the development of more effective missile defenses, technical countermeasures, and creative operational responses. Missile defenses against large-volume Chinese LACM threats will need special attention, if the poor U.S. performance against Iraq's primitive and small number of LACMs in Operation *Iraqi Freedom* is an indicator of U.S. weaknesses vis-à-vis such threats. JFQ

Notes

¹ To be sure, the combination of all three of these aspects is difficult to achieve. A supersonic missile is usually not stealthy, particularly from an infrared perspective, and such missiles tend to fly higher to get decent engagement ranges. To delay detection and thereby reduce reaction time, subsonic missiles typically use low-altitude flight profiles. Combining all of them into one missile is difficult to do, and China currently lacks a missile with all three of these characteristics. Information presented by Christopher P. Carlson at the Workshop on Open Source Exploitation, sponsored by Naval War College and Potomac Foundation, Vienna, VA, March 3, 2014.

² A good synopsis of Chinese antiship cruise missiles (ASCM) development can be found in Wang Wei, "Development of the PLA-Navy's Anti-ship Missile," *Shipborne Weapons* 5 (May 2008), 35–47.

³ For instance, the HY-2/4 ASCMs have been exported as the C-201/201W.

⁴ This series is essentially defunct, having not competed well with the export versions of the HY and YJ series.

⁵ *Russia's Arms and Technologies: The XXI Century Encyclopedia—Naval Weapons*, Volume III (Moscow: Arms and Technologies Publishing House, 2001); Machine Building Design Bureau marketing brochure—3M80E antiship attack missile-weapon complex. For 3M80MVE

characteristics, see the Tactical Missiles Corporation JSC Web site at <http://eng.ktrv.ru/production_eng/323/507/541/?PHPSESSID=b56ca0fa59423f9a752a0ccdc67eb72a>.

⁶ Christopher P. Carlson, "China's Eagle Strike—Eight Anti-Ship Cruise Missiles: YJ-81, YJ-81, and C802 (Part 2)," Defense Media Network, February 6, 2013, available at <www.defensemedianetwork.com/stories/chinas-eagle-strike-eight-anti-ship-cruise-missiles-yj-81-yj-82-and-c802/>.

⁷ Ibid.

⁸ "C602: Anti-Ship Missile Weapon System," China National Precision Machinery Import and Export Corporation marketing brochure, 2010.

⁹ Christopher P. Carlson, "YJ-12 Photographic Analysis," February 2014; "Chinese YJ-12 Supersonic Anti-Ship Missile Revealed," *Chinese Military Review*, January 2013, available at <<http://chinesemilitaryreview.blogspot.com/2013/01/chinese-yj-12-supersonic-anti-ship.html>>.

¹⁰ Christopher P. Carlson, "Deciphering the Eagle Strike-8 Family of Anti-Ship Cruise Missiles," presentation at Workshop on Open Source Exploitation.

¹¹ "PLA's Tactical Air-To-Surface Missiles (Part 1)," *SinoDefence*, February 18, 2014, available at <<http://sinodefence.com/2014/02/18/plas-tactical-air-to-surface-missiles-part-1/>>.

¹² Pan Wenlin, "Small Gas-Turbine Unit and China's Antiship Cruise Missiles," *Shipborne Weapons* 8 (August 2010), 14–25; "KD-63 (YJ-63), K/AKD-63," *Jane's Air-Launched Weapons*, January 28, 2014, available at <www.janes.com>.

¹³ "Navalized DH-10 LACM," *China Defense Blog*, July 25, 2012, available at <<http://china-defense.blogspot.com/2012/07/navalized-cj-10-lacm.html>>.

¹⁴ James C. Bussert, "China Destroyer Consolidates Innovations, Other Ship Advances," *Signal*, December 1, 2013, available at <www.afcea.org/content/?q=node/11972>.

¹⁵ *Military and Security Developments Involving the People's Republic of China 2013*, Annual Report to Congress (Washington, DC: Office of the Secretary of Defense, 2013), 4, available at <www.defense.gov/pubs/2013_china_report_final.pdf>.

¹⁶ *Military and Security Developments Involving the People's Republic of China 2009*, available at <www.defense.gov/pubs/pdfs/China_Military_Power_Report_2009.pdf>. Figures were derived from the chart on page 66 of the 2009 report. Only CSS-6 and CSS-7 missile launchers and DH-10s were considered. As the most important factor in delivering pulses of power, missile launchers (not missiles) were the focus. Like aircraft launched from carriers, missiles launched are the appropriate measure of the intensity of fire within a unit of time.



In addition to their daily duties within Combat Logistics Battalion 6, Marine Expeditionary Brigade—Afghanistan, Marines also serve as FET members to establish rapport with locals (U.S. Marine Corps/Justin Shemanski)

Blurred Lines

Cultural Support Teams in Afghanistan

By Megan Katt

Megan Katt is a Research Analyst in the Center for Stability and Development at the Center for Naval Analyses. She is a co-author (with Jerry Meyerle and Jim Gavrilis) of the book *On the Ground in Afghanistan: Counterinsurgency in Practice* (Marine Corps University Press, 2012).

Allowing women in combat is a highly controversial subject. Yet regardless of their official military occupational specialty (MOS), female Servicemembers have often found themselves in combat situations—most recently in Iraq and Afghanistan. In both combat zones, male and female Servicemembers alike

have conducted counterinsurgency and stability operations—so-called irregular warfare activities that lack clearly defined “frontlines” against enemies who do not wear uniforms. These types of operating environments forcefully negate any biological sex combat restrictions as the lives of both men and women are at risk.

Along with the highly trained and capable special operations forces (SOF) operating in remote locations throughout Afghanistan, lesser known teams of female Soldiers, Marines, and Sailors have worked to develop enduring relationships with Afghan women. These enabling units, which evolved from earlier female engagement efforts and ultimately became known as Cultural Support Teams (CSTs), have supported SOF units conducting village stability operations (VSO). While skirting Department of Defense (DOD)-imposed restrictions on women in combat that had been in place since 1994, the women on CSTs faced substantial personal and physical risk. By stepping “outside the wire” to converse with locals, they placed themselves in harm’s way,¹ engaged in firefights, and, in some cases, were specifically targeted by insurgents. At a time when the U.S. military is pulling back from a large-scale irregular warfare mission in Afghanistan and trying to rebalance the Armed Forces for more traditional operations, it is worth examining whether these types of all-female teams will be relevant to future operating environments.

Based primarily on author interviews with CST and SOF personnel,² this article describes the CST program; why it was created and how it evolved from previous efforts; how some CST members were selected and trained; the types of activities that members of these teams conducted; the challenges that arose; and the lessons that can be drawn from their experiences. While this article does provide some background on gender policy restrictions, it does not argue either for or against making combat positions available to women. The nature of conflict in these types of environments belies the idea that women can simply be kept out of combat. Therefore, this article focuses on what some female Servicemembers were able to accomplish executing population-focused operations under the combat restrictions in place at the time. It concludes by discussing potential implications of the sexual policy restrictions debate on the future of a CST-like capability.

Moving across “Frontlines”

Women’s roles in the military have necessarily evolved over the past several decades, while still limited by DOD restrictions on the types of positions they could fill. In 1988, DOD created the so-called Risk Rule, which excluded women from units that had a high probability of engaging in ground combat, hostile fire, or capture.³ In 1994, DOD replaced that regulation with the Direct Ground Combat Definition and Assignment Rule, otherwise known as the DOD Combat Exclusion Policy, which restricted the assignment of women to units below the brigade level whose primary mission was to engage in direct ground combat.⁴ According to the policy, female Servicemembers were restricted from jobs in a primary MOS of ground combat, such as in the infantry. Yet with these rules in place, women have increasingly been allowed to serve in a wider range of combat support roles, including as explosive ordnance disposal technicians, military police, interpreters, drivers, and working dog handlers. In irregular warfare, where frontlines are nonexistent, many of these supporting jobs can take women into the line of fire, often with little ground combat training.

Counterinsurgency and stability operations in Iraq and Afghanistan challenged U.S. forces to identify friend from foe as they operated among civilians, including many women and children. Perceived indiscriminate use of force and culturally prohibited contact between male Servicemembers and local women (for instance, during night raids) angered local populations and proved counterproductive to the overall mission. In an effort to avoid these confrontations and show more respect for the local culture, U.S. forces largely ignored the female population. Insurgents, in turn, took advantage of these cultural sensitivities by disguising themselves in women’s clothing to avoid detection during searches. Men wearing traditional burkas—full body cloaks worn by some Muslim women—could escape the military’s grasp by blending in with women.

To counter this insurgent tactic in Iraq, the U.S. military developed what became known as the Lioness Program. As part of this initiative, the military posted female Soldiers and Marines at control points to interdict and search women for weapons, explosives, and other contraband. However, these teams were staffed in ad hoc fashion by female Servicemembers who were pulled from their regular duties and who received minimal training for these new responsibilities. In addition, the narrowly focused program did not provide opportunities for persistent engagement with the female population.

In an attempt to develop better relationships with Iraqi women and identify sources of instability, the Marines developed the Iraqi Women’s Engagement Program. Unfortunately, not much is written about the program—in part possibly due to potential controversy over women being placed in combat situations. What little is known is that a group of female Civil Affairs (CA) Marines reportedly began the program in Al Anbar Province in 2006. The uniformed women aimed to build trust with local women by discussing their concerns over cups of tea. Later, these efforts also included talking to women during sewing clinics and medical engagements. The indirect effect of these engagements was a nascent dialogue on the factors of instability in the area.

Providing Opportunities for Engagement

The Iraq experience, although limited, highlighted the positive effects of female engagement in that type of environment and the need for a similar tool in Afghanistan. In a society with limited women’s rights and restrictions on contact between the sexes, Afghan women were culturally off-limits to outside men. Male Servicemembers ran the risk of showing disrespect to locals if they engaged with women during patrols, raids, or other operations. As in Iraq, Soldiers and Marines realized there was a need to fill that gap, as well as to build rapport with the female portion of the population. This requirement



FET Team 11 members in Helmand Province listen to other Marines talk about their deployment experiences (U.S. Marine Corps/Katherine Keleher)

resulted in the Female Engagement Team (FET) initiative, which combined the Lioness Program's efforts to search women with the Iraqi Women's Engagement Program's efforts to address underlying causes of instability, merging them into even broader operational roles.

The Army and Marine Corps assembled FETs on an ad hoc basis upon the request of maneuver units. As a result, female Servicemembers already on the ground were pulled from their regular jobs and had little or no time to train for their additional FET responsibilities. Moreover, because these women did not have a ground combat MOS or any of the training that would accompany it, some have argued that this staffing put them and the men serving alongside them at greater risk.⁵

The first reported FET was assembled on an ad hoc basis to support a specific cordon and search operation in western Afghanistan in February 2009. The team, which consisted of female Marines and

a female interpreter, provided the same search function that the Lioness Program had in Iraq. Yet the team also visited with Afghan women in their homes and distributed humanitarian supplies in an effort to develop goodwill. Later that year, a similar FET was established after insurgents were able to escape a military cordon by dressing like Afghan women. These early FETs largely conducted short-term search and engagement missions.

In late 2009, the commander of the International Security Assistance Force (ISAF) institutionalized the FET concept by directing all deploying military units to create all-female teams to develop and improve relationships with Afghan women. To quickly fill the requirement, initial FET training was limited and ranged from just a few days to months. Generally speaking, training focused on combat activities but also included some instruction on Afghan culture, language (Dari or Pashto), use of interpreters, and other softer skill sets relevant to operating among the population.

By 2010, the Army and Marine Corps began to send dedicated FETs, which ranged from two to five women per FET, to support battalion and company commanders across an area of operation. The first trained, dedicated, and full-time Marine FETs arrived in Southwest Afghanistan in the spring of 2010. Depending on the need, FETs, sometimes augmented by a female interpreter or medic, accompanied all-male infantry patrols in Helmand Province. Similar to the Afghan women who needed to be escorted by a male relative in public, female Servicemembers needed to be escorted by their male colleagues outside the wire due to force protection restrictions.⁶ This created resource constraints for units every time they took FETs outside the wire. While FETs were generally sent to areas that had largely been cleared of insurgents, they still took a combat-training refresher course and carried M-4 carbine rifles with the full expectation that they would be exposed to combat situations.

Marine FETs conducted a range of engagements during their 7-month tours. Generally, after a team arrived in a village, female Marines went door to door to engage women and learn about the area and villagers' concerns. Once inside an Afghan compound, they removed their weapons and body armor as a sign of respect. They also replaced their helmets with headscarves to be culturally sensitive. In many areas, the FETs found that Afghan men were also willing to engage with them. Yet while the FET members could listen to the concerns and issues raised by villagers, in many cases they did not have the authority or capability to address them. In addition, some criticized the FET program because the teams were unable to create lasting effects due to the episodic and temporary nature of their engagement as coalition forces moved through an area, never to return.

In addition to engagement, each FET was tasked with a variety of responsibilities—perhaps more than the name of the program implies. In addition to engaging with and gathering information from Afghan families, they distributed information, facilitated CA programs (for example, distributed school supplies and opened schools or clinics), supported female-focused governance and development projects (developing women's centers, providing micro-grants), held key leader engagements and women only-shuras, conducted medical outreach, assisted with cordon and knock operations, and searched women.

Developing a SOF-Specific Female Engagement Capability

Meanwhile, similar female engagement capabilities were quietly being developed within the special operations community to fit mission requirements. The ISAF commander began to pressure U.S. Special Operations Command (USSOCOM) to develop its own FET-like capabilities to embed with SOF units to assist with engaging Afghan women in support of direct operations. Marine Corps Forces Special Operations Command (MARSOC) was one of the first to experiment with using an FET in 2010 by pulling one

Marine officer, two enlisted personnel, and a Navy corpsman from their day jobs to support a Special Operations Task Force (SOTF) in this new role.⁷ Because these women lacked specific training and were pulled from their regular duties, the effort was less than seamless; however, this did not dissuade MARSOC from the concept. Instead, MARSOC deployed a female unit with the sole purpose of conducting the FET mission in an organic capability to support a SOF unit in June 2010.

The SOF female engagement program was formally created in 2010 under the direction of the USSOCOM commander. The United States Army Special Operations Command, Naval Special Warfare Command, and MARSOC expanded on the FET concept by developing what became known as Cultural Support Teams (CSTs). The term itself took sex out of the equation; however, the teams still solely comprised female Servicemembers. The primary difference between the two was that FETs were used to soften coalition forces' footprint as they moved through an area, whereas CSTs were designed to provide persistent presence and engagement—a key tenet of population-focused operations conducted by SOF.

These two-person CSTs were given a wider mission set to support SOF conducting “non-direct ground combat missions,” specifically village stability operations. As part of VSO, small SOF teams aimed to disrupt the insurgency and foster stability in relatively remote villages where the Afghan government was not represented by its own security forces. Special operators engaged influential local leaders in an effort to recruit community defense forces, empower local governance, and bolster economic development—all in an effort to expand the reach of the Afghan government and disrupt insurgent influence. The CSTs provided an opportunity for SOF to communicate with Afghan women, something they had been limited from doing previously due to cultural sensitivities. In short, VSO became a loophole for female Servicemembers to operate alongside the most highly trained—and exclusively male—forces on the battlefield.

Identifying Suitable Candidates

Per USSOCOM's directive, each of the Services began to recruit female Servicemembers to work alongside the military's most elite units. Some Services solely recruited volunteers, whereas others, which had larger operating requirements, reportedly assigned personnel to these teams. Because these CSTs are designed to support SOF teams at the lowest levels, the qualification requirements and selection process of these women has been demanding. Each Service conducts a thorough assessment to locate candidates who are both physically and mentally fit. Like special operators, the Services look for specific selection criteria in identifying suitable candidates. Many women have reportedly been turned down during the assessment process.

MARSOC evaluators held female candidates to the standards similar to MARSOC male special operators, known as Critical Skills Operators (CSOs), since they would be working alongside each other. MARSOC candidates needed top physical fitness test and general technical scores. Prior deployment experience was also a factor. If women met these criteria, MARSOC psychologists then administered the same four psychology exams that potential CSOs receive to ensure that their personalities and psychological profiles were compatible with the individuals with whom they would deploy and that they could make the necessary adjustments to keep up with the distributed, fast-paced nature of the Afghanistan mission. Finally, MARSOC evaluators conducted an oral interview with eligible candidates to gauge interest and determine whether they could “think on their feet” to make quick decisions on the ground.

The qualified Marines ultimately selected for MARSOC CSTs came from a variety of occupational specialties, ranging from judge advocate to military police officer to automotive maintenance technician. The most common occupational fields included logistics, communications, and military police, investigations, and corrections. Most were enlisted personnel ranging from sergeant to gunnery sergeant. In addition, Marine

teams were also often supplemented by medically trained Sailors, such as Independent Duty Corpsmen.

Preparing Women to Be SOF Enablers

Subtle differences also existed in how each Service trained its female candidates for the mission. According to many accounts, individual augmentees received varying amounts of training to fill the emerging requirement. As the program expanded, the Services slowly developed their own formalized training packages for CSTs. For example, MARSOC developed a series of training organized into blocks. For a total of 109 days, its female volunteers were trained to the same standards as other MARSOC enablers:

- The first block of instruction began by focusing on engagements and rapport-building with an Afghan focus. MARSOC hired female subject matter experts in negotiations and Afghan culture (tailored to the region in which the women would deploy) for both discussion and practical application. CST members learned about Afghanistan, Afghan values, and the nuanced roles of women in that society.
- The second block of instruction taught female Servicemembers the basics of how CSTs would fit into the MARSOC intelligence process, as well as additional instruction on combative training, riot control, and increased observation and situational awareness. In addition, CST candidates participated in the MARSOC intelligence course's culminating exercise, which not only gave them a chance to practice what they had learned but also allowed the MARSOC students the opportunity to leverage every asset available to them to complete their mission.
- The third block of instruction focused on civil-military operations (CMO). MARSOC sent its candidates to the Marine Corps Civil Military Operations School to receive CMO training, at the end of which

students received an additional MOS in CA. CMO skills are particularly useful in an irregular environment and provided CSTs with an additional capability they could bring to their assigned SOF team if CA personnel were unavailable.

- The fourth block of instruction consisted of the basic MARSOC special operations training course, which all MARSOC enablers attend in order to prepare for the rigors of a combat deployment with a MARSOC SOTF, company, or team. There, CST candidates received an introduction to SOF operations and learned how CSOs operate. In addition, the course provides a basic combat skills refresher course (that is, "shoot, move, and communicate") to dust off those skills and add a special operations approach. CST candidates were also trained to master the weapon (an M-4 rifle and/or a pistol) that they were assigned and would carry with them during their deployments. Even though CSTs have supported nondirect combat missions, they have still operated in a combat environment. As an integrated member of a special operations team, each CST member had to be prepared to engage in direct combat in case a situation took a kinetic turn.
- The fifth block of instruction included MARSOC's full-spectrum survival, evasion, resistance, and escape course, which incorporates field survival basics, including hostage and detainee operations. In addition to preparing them for survival, it helped prepare them mentally and physically by gaining a better understanding of the other women they would deploy with and their limitations.

Additionally, CST candidates received training in tactical questioning, basic medical skills, and tactical driving—all of which made them more useful to the special operations team to which they would be attached and created additional opportunities to get outside the wire to engage with the local population.

Finally, MARSOC provided them with interactive software and books so that they could learn Dari. By August 2013, a total of 18 Marines and 5 Sailors had completed MARSOC's CST training program, which then deployed with even higher numbers from the other Services.

Deploying with SOF

The first formalized CSTs from the Army and Marines began to deploy in two-woman teams in early 2011. Due to DOD restrictions below the battalion level, CSTs were formally attached to larger special operations units—generally SOTFs—and then distributed throughout the battlespace as needed. Not every VSO site and SOF unit received a CST. Instead, attachments were based on demand. After a special operations team secured a VSO site and identified a need for a CST, the SOTF attached one based on the team's capabilities. In addition to initially attaching them to units, the SOTF could rearrange CSTs based on mission requirements and CST members' individual skill sets. In many cases, teams have been split—sometimes over different districts—to divide responsibilities and leverage particular skill sets based on local needs (such as medical care).

CSTs have supported a broad spectrum of activities across all three lines of operations: security, governance, and development. Special operations teams have incorporated CSTs differently into their missions depending on the local situation. As designed, many have accompanied special operators into villages on patrols to engage and help build rapport with local women, much like FETs. There have also been cases in which CSTs have effectively engaged women and children after alleged civilian casualty incidents. By developing relationships with the local population and sharing the information (sometimes time-sensitive information) that they gather with their teams, special operators can develop a more complete picture of the operating environment than was previously attainable. Like FETs, CST activities include providing medical support and humanitarian assistance, conducting key leader



Afghan children gather around FET member during shura to discuss current local issues (U.S. Marine Corps/Andrea M. Olguin)

engagements, exploring girls' education issues, and performing searches on the female population. In many cases, CST members have established rapport with locals, exchanged cell phone numbers, and been invited to visit women's homes. Their capabilities are also broader than those of FETs. CSTs can follow special operators into areas after they have been secured, including after raids. In those situations, CSTs then use search and seizure techniques to find hidden items on females (for example, weapons or contraband)—and, like FETs, occasionally uncover a militant dressed as a woman.

CST activities can be largely dependent on location and the permissibility of the environment. In northern Afghanistan, for example, governance and development were primary goals in 2012. At one site, a CST member with medical training focused on conducting medical engagements. At another site, her CST partner worked with the Ministry of Education to reform education syllabi. Around the same time in

western Afghanistan, CST accomplishments included opening a clinic and a girls' school, in addition to organizing a women-only shura. CST members also worked with government ministries, such as the Department of Women's Affairs and the Labor Union, in an advising role.

Finally, a CST member could also provide value to the team by conducting tasks related to her MOS, such as communications, CA, or driving.

Recurring Challenges

CSTs, like their predecessors, have received mixed reviews. While their operational impact is difficult to measure, many special operations teams have spoken highly of the enabling capabilities they have provided in the execution of VSO in persistent situations, particularly in gathering information. In other cases, special operations teams either have not known how to best use their capabilities or have not been able to due to limitations based on the security situation. Like other

enabling capabilities, there has also been the risk that abilities did not measure up to expectations or that personalities would clash.

In my discussions with both CST and SOF members, a number of recurring challenges emerged. CST members discussed challenges with integrating into teams, misperceptions of their capabilities, and a lack of capable female interpreters. Special operators identified additional challenges such as site selection, security limitations and considerations, and sexual tension between CST and SOF members.

Some CST members indicated that it could be difficult to integrate with a special operations team as an outsider to a "band of brothers"—a concern similarly raised by members of other enabler units (for instance, CA) as well. In northern Afghanistan, one CST Soldier described her team's integration with an Army Operational Detachment–Alpha (ODA) as a train wreck. The SOF unit had misperceptions about the capabilities



Marines practice speed and tactical reloads while training to become augments for FETs (U.S. Marine Corps/Ryan Rhoads)

of her team. In situations such as those, CSTs can run the risk of turning into a hindrance for the special operations team and can therefore be underutilized. In that case, it took time for the women to gain the operators' trust and understanding. That same CST was later moved to a different site where the resident ODA made the team an extension of its own team. She believed that the primary difference between the two experiences was that the second ODA was already familiar with the capabilities they could provide and how best to use them.

Finding qualified female interpreters was another issue identified by several interviewed CST members. In some areas, such as western Afghanistan, it may be culturally acceptable to use a male interpreter. However, that is generally not the case in ethnically Pashto areas. And while it can be relatively easy to find male interpreters, there are generally far fewer mentally and physically fit female interpreters. One CST started its deployment with a young female interpreter who spoke a different dialect from the one spoken in their assigned area. That same CST later received a different interpreter with impressive language capabilities; however, she was older and her physical ability was limited, which in turn limited team mobility. At another location, a CST member

indicated that her team's interpreters could not keep up on long patrols, in effect slowing the special operators down. Therefore, without a good interpreter, the CST could not effectively do its job.

According to some special operators, security has been a limiting factor in assigning CSTs to different sites. Some operators suggested that CSTs could potentially be more useful to gain buy-in by engaging with female villagers during the initial stages of VSO when the area is less permissive. However, due to DOD-imposed restrictions, CSTs were instead introduced to the village later when the area was relatively secure and male Servicemembers had already developed local relationships. Similarly, some areas were more receptive to CSTs. At some of the locations where CSTs were assigned, Afghan women were either uninformed or unwilling to share information, which hindered a CST's ability to complete its mission.

Ultimately, in some situations, special operators determined that the costs of using CSTs outweighed the benefits—that is, in some cases, CSTs were not worth the risk for the team due to protocols and security considerations. One special operator explained that it could be manpower-intensive to bring CST members out to a shura or on a mission.

If a CST member took up a seat, it meant that she had taken the place of another operator (with his own supplementary capabilities). In addition, taking a CST member anywhere usually required bringing along an interpreter and a security patrol. As a result, even though two women were on each CST, often only one would go out on each mission. That made it easier for the team to patrol and meant that they did not need to take additional operators with them for security purposes, possibly requiring an additional vehicle.

Finally, operators expressed concerns about sexual tension and activity impacting unit effectiveness, an argument frequently cited in studies on women in combat. Working long hours in close quarters and in sometimes austere conditions has the potential to bring people together in any job. Some have suggested that sexual relationships have had the potential to impact daily operations and unit cohesion. In addition, there have been some complaints about a lack of maturity of both men and women. Yet this issue may have been mitigated at VSO sites that had strong leadership.

Implications for the Future

The FET and CST programs were emergent mission-specific requirements, which the Services met by initially recruiting female Servicemembers out of hide from other units as individual augmentees. In particular, CSTs in Afghanistan opened the door for female troops to operate alongside special operations units in the battlefield. They were specifically selected and trained to work with SOF as part of VSO. The Marine Corps ended its use of CSTs in Afghanistan in 2013 because of the drastic change in mission when SOF moved out of villages into overwatch positions. However, as the U.S. military continues to withdraw from Afghanistan and looks to prepare and posture itself for the future, it should consider whether CSTs are truly an enduring requirement for SOF, which will continue to conduct irregular warfare activities around the globe and could benefit from this enabling capability.

The conflicts in Iraq and Afghanistan reflect the likely future of combat—non-linear and population-focused—and will increasingly place female Servicemembers in combat situations. Both men and women have fought and died in these combat environments. Partly as a result, DOD has recently relaxed its restrictions on women in combat. In February 2012, DOD modified the 1994 Combat Exclusion Policy to increase the overall number of positions available to women.⁸ Then, in February 2013, DOD eliminated the exclusion policy and began to allow each Service to determine any restrictions specific to its members.⁹ Each Service is now examining potential roles for women in future operating environments.

The results of these studies may help the Services determine whether FETs and CSTs are necessary in future operating environments. For example, if the Services do choose to open all positions to women, these all-female teams may not be necessary once units are fully integrated; more trained women will potentially be available on the battlefield to regularly engage with female counterparts during patrols and meetings or after raids. If they do choose to leave restrictions in place for women in combat, the Army and Marine Corps may want to consider institutionalizing an FET-like capability within each infantry battalion, with special attention to the CA skill sets found necessary in Afghanistan. The resource commitment would be relatively small and would maximize a unit's effects in population-focused operations. Similarly, USSOCOM may ultimately decide that female Servicemembers should not be allowed to serve in a special operations-specific MOS. If that is the case, the potential still exists for SOF to benefit from CSTs in other theaters.

Regardless of the policy restrictions debate and the Services' findings, the need for a CST-like capability will endure as SOF continue to operate in irregular battlefields all over the world. While the VSO mission was designed expressly for Afghanistan, its roots are in traditional SOF missions, such as counterinsurgency, stability operations, and foreign

internal defense. In these population-centric missions, CSTs can help provide access to roughly half of the population through engagement activities. In addition, CSTs could be enormously beneficial during SOF training missions with partner nations. In countries that have female soldiers or police, the addition of women to an otherwise all-male team could give them greater access and placement during a Joint Combined Exchange Training event.

Looking ahead, the question ultimately becomes whether the military believes that this enabling capability is worth keeping at a time when every program is increasingly scrutinized due to ongoing budget cuts. However, if the program is dissolved now and the capability is needed again in the future, it will cost a lot of resources—in both money and manpower—to begin anew. Therefore, by evolving the program to provide SOF with this type of enduring enabling capability, it may ultimately save resources in the long run.

As part of this evolution, the SOF community should ensure that the lessons learned in Afghanistan are institutionalized. Ultimately, the bulk of the challenges identified herein have little to do with gender policy restrictions. Some of the issues, such as capability misperceptions and clashing personalities, are similarly faced by other types of (all-male) enablers and can possibly be resolved as the CST program matures. For example, challenges of CSTs integrating into special operations teams may be overcome with additional combined training opportunities. In addition, CST assignments would need to be monitored by leadership and adjusted as needed. While the issue of deploying CSTs in heavy fighting areas may possibly be a result of policy restrictions, it may also be a command decision. With limited numbers of CSTs, it is practical for a commander to ensure that they face less risk.

SOF may need to examine the need for CSTs on a mission-by-mission basis. Some have argued that the culture in parts of the Middle East and South Asia may be somewhat unique in terms of sex segregation. In many parts of the world,

male Servicemembers may be able to converse freely with female locals without the same traditional cultural implications. Yet in any culture, women may generally feel more comfortable being engaged with—and, when necessary, searched by—other women. Even in the United States, women prefer and often insist on female Transportation Security Administration staff patting them down at airports, if necessary. It is not unreasonable to expect similar preferences in other countries. Therefore, the special operations community should more closely examine how it could use or re-tool this enabling capability for different types of environments. JFQ

Notes

¹ In October 2011, First Lieutenant Ashley White, USA, became the first Cultural Support Team member killed in the line of duty when an improvised explosive device (IED) detonated in southern Kandahar Province. See David Zucchino, "A Counterinsurgency Behind the Burka," *Los Angeles Times*, December 11, 2011. More recently, First Lieutenant Jennifer Moreno, USA, was killed in an IED attack in October 2013. See Gretel C. Kovach, "Female Soldier Killed on SpecOps Mission," *San Diego Union Tribune*, October 8, 2013.

² The author also researched open source material and the Marine Corps Lessons Learned System for additional information.

³ David F. Burrelli, *Women in Combat: Issues for Congress*, R42075 (Washington, DC: Congressional Research Service, May 9, 2013), available at <<http://fas.org/sgp/crs/natsec/R42075.pdf>>.

⁴ Department of Defense (DOD) Memorandum, "Direct Ground Combat Definition and Assignment Rule," January 13, 1994.

⁵ See, for example, Lia B. Heeter, "Women in Combat: Policy Barriers are Being Removed," *Marine Corps Gazette*, July 2013.

⁶ Ann Jones makes this observation in "Woman to Woman in Afghanistan," *The Nation*, October 27, 2010.

⁷ Trisha Talton, "MARSOC Looks to Women for New Mission," *Marine Corps Times*, November 14, 2009.

⁸ DOD, *Report to Congress on the Review of Laws, Policies and Regulations Restricting the Service of Female Members in the U.S. Armed Forces*, February 2012.

⁹ DOD Memorandum, "Elimination of the 1994 Direct Ground Combat Definition and Assignment Rule," January 24, 2013.



Laser-guided bombs line flight deck of aircraft carrier USS *John F. Kennedy* in preparation for air strikes against Iraq during Operation *Desert Storm* (PH2 Lipski)

Determining Hostile Intent in Cyberspace

By Ramberto A. Torruella, Jr.

Okay, bogies have jinked back at me again for the fifth time. They're on my nose now. Inside of 20 miles."

This was the report made by Commander Steven Collins, USN, Radar Intercept Officer (RIO) of Gypsy 207, prior to arming his F-14's radar-guided missiles. Two Libyan MiG-23 Floggers

were inbound to the *John F. Kennedy* Carrier Strike Group. Two F-14 Tomcats of VF-32 were assigned to intercept. The Tomcats flew low, lost in the radar clutter kicked up by the sea's surface, maneuvering several times to stay out of the Libyan fighters' engagement envelope. The Americans maintained a constant fire control lock on their opponents. The MiGs matched each American maneuver unerringly, ignoring the radar lock warnings growling in their cockpits. Because the radar on the MiG fighters could not detect the Americans

through the clutter, the Libyans relied on guidance from shore-based radar stations for a ground-controlled intercept. The MiGs kept their noses pointed toward the Americans, hoping their radar would burn through the clutter and give them a chance to shoot first. It was clear the Libyans wanted a fight. It was clear they had *hostile intent*.

"13 miles. Fox 1! Fox 1!" the RIO shouted as the missiles left the rails of the Tomcat, initiating an engagement that would end with two MiGs destroyed and two Libyan pilots lost at sea (paraphrased

Commander Ramberto A. Torruella, Jr., USN, is the Joint Staff J8 Models and Analysis Information Technology Support Branch Chief.

from “Splash Two MiGs,” an account of the 1989 Gulf of Sidra Incident).¹

According to the Joint Chiefs of Staff, *hostile intent* is defined as the threat of imminent use of force against the United States, U.S. forces, or other designated persons or property.² It is the indication, the *belief*, a commander has that an adversary is about to attack. That belief provides the groundwork for “anticipatory self-defense,” an American legal concept that allows a commander to attack before being attacked.³

From the point of view of the American pilots, the Libyan pilots showed hostile intent by flying a vector toward the American Carrier Strike Group, constantly maneuvering to threaten the American interceptors, and ignoring the obvious warning signal of American fire control radar locked onto their aircraft. Libyan actions gave the Americans the *belief* that an attack was imminent. The Americans launched their own missile strike as a result: a clear case of anticipatory self-defense, a preemptive attack that spoils the anticipated attack of an enemy. Interestingly, from the Libyan point of view, the Americans also clearly showed hostile intent by constantly illuminating the Libyan fighters with their fire control radar, the last step the Libyans would detect prior to an American missile attack.

Determining hostile intent is often not this clear, but in this instance, within the physical realm of fighter jets, radars, and missiles, the evidence strongly suggests that both parties demonstrated hostile intent.

This is rarely the case in cyberspace.

Information as a Weapon, Cyberspace as an Abstraction

The cyberspace realm is an abstraction, with components located in a physical space but operations occurring in a nonphysical space, where the terrain is data and information is used as a weapon. This is not new. The ancient Phoenicians pioneered information as an abstraction when they laid the foundation for our alphabet, an abstraction necessary for transmitting concepts via the written word. Medieval Arabs developed our number system, an abstraction

necessary to communicate complex calculations. Commanders from Alexander the Great to Napoleon used both of these abstractions to send dispatches in clear text and code—to communicate with subordinates, coordinate actions in real space, and hide their intentions from opponents. Eventually, special signal corps evolved to encrypt, transmit, receive, and handle messages, first at the rate of the written word and the horse, then at the rate of signal flags, telegraphs, and flashing lights. Code breakers ancient and modern fought a silent war to understand enemy signals and gain access to enemy information.

But it was not until the late 20th century, when improvements in communication and computing technology raised the volume and velocity of data flow from dozens of words per minute to 1.5 trillion words per minute, that the information domain gained enough significance to be treated as a warfare area in its own right.⁴ An adversary with access to a commander’s data flow now possessed a far richer set of information regarding intentions and operations. More importantly, if an adversary could deny the commander necessary information or, better yet, *change* information needed to make a decision, disastrous effects could occur in real space. For instance, what if the Libyans were able to fool the American radars and combat systems into believing their MiGs were farther away or on a different vector? Would confusion have ensued? Would the world be lamenting (or celebrating) a different outcome?

This is not the first time, and probably not the last, that a change in technology caused an abstraction to evolve into a warfighting domain. Consider the concept of the high ground. In the 6th century BCE, the military philosopher Sun Tzu plainly articulated the benefit of operations from the higher ground; a commander has greater visibility over enemy movements and is better situated to defend against attack.⁵ It was even axiomatic in ancient times that military possession of higher ground would greatly increase the chance of combat success. During the late 18th century, however, the French Revolutionary

Army experimented with a technology that turned that land-based abstraction (*hold the high ground*) into the start of a useful warfighting domain; it started using balloons for aerial reconnaissance of the battlefield.⁶ Soon, other countries experimented with using balloons for observation, bombing the enemy, or increasing the range of communications. Most experiments met with modest success; the technology simply was not robust enough to deliver consistent battlefield results.

But once the airplane was invented, everything changed. Aerial reconnaissance became consistent and soon was vital to events on the ground. Artillery spotting was added to the airman’s list of vital tasks as well as reconnaissance deep inside of enemy lines. Change occurred again when the first airman aimed a pistol at an enemy observer in another aircraft. An arms race quickly ensued—planes increased in number, specialized in purpose, and carried specially developed weapons meant to shoot down other aircraft. They flew faster and higher and fought for dominance of the air. Commanders now prioritized effects in the air over direct effects on the ground, and air warfare, a new warfighting domain, was born.

Hostile Intent in an Abstract Domain

Cyber warfighters learn from the evolution of other domains, especially with regard to the legal authorities associated with the use of force and armed combat, the Law of Armed Conflict. Just as aviators learned to apply the Law of Armed Conflict in their new domain, so will commanders who operate in the cyber domain.

Cyberspace has its own unique challenges. Attributing a cyber attack is difficult at best because commanders are rarely ever sure of the source of an attack or intrusion, and establishing the forensic evidence needed to be certain is a time-consuming and often imprecise science. Intentions are even harder to discern. For example, does malware beaconing to an Internet protocol address in China indicate an attempt to steal data? Is it a



F-14D Tomcat conducts mission over Persian Gulf region (U.S. Air Force/Rob Tabor)

precursor for establishing a botnet? Is the malware even Chinese? Is placing malware even considered a use of force? Unfortunately, there is little to no international consensus on what constitutes a use of force in cyberspace.⁷

This article discusses the legal authorities to use force in cyberspace. It discusses what constitutes the use of force in cyberspace and how a commander can determine if an opponent intends to use force against the United States or its assets and interests. The article builds on a rubric developed by Michael Schmitt to help identify hostile intentions in cyberspace and, using a spectrum of cyber activity developed by Gary Brown and Owen Tullos, suggests in general what may be appropriate responses to hostile intent. Finally, the article briefly addresses the legal roles, responsibilities, and authorities required for addressing the different types of cyber attacks with an eye to identifying and responding to hostile intent.

Classifying Use of Force in Cyberspace

Article 2, Paragraph 4, of the United Nations (UN) Charter specifically states that “All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations.” Force, in this case, does not mean coercion, but the use of *armed* force as a tool of coercion or persuasion. Matthew Waxman notes that the framers of the UN Charter did not set out to end coercive behaviors in international relations, but to end *war* as a legitimate tool of policy except in the case of self-defense. The prohibition against force is a prohibition against armed attack.⁸

Waxman also notes that when the framers set about to prohibit the use of force, they took an *instruments*-based

point of view instead of an *effects*-based point of view of limiting coercion.⁹ This means that the framers intentionally sought to limit *how* coercion could be performed in international politics, not limit the *effects* of coercion on a target nation. For instance, armed attacks and kinetic strikes are not authorized, nor are blockades, bombardments, or any other classic use of military power, except in self-defense or as authorized by the UN Security Council for the peace and security of the international community. However, diplomatic isolation and economic coercion are perfectly authorized by the charter. A nation can target an embargo against another nation, but it cannot conduct a naval blockade without the express authorization of the Security Council. Both actions may have the same effect on the targeted nation—severe economic damage as a form of coercive pressure—but the charter explicitly prohibits a blockade and not an embargo.

This creates a difficulty when dealing with potentially hostile actions that occur in cyberspace. By their very definition, cyber actions occur in an abstract realm of data representation, not physical force. So even if a cyber action causes tremendous destruction by overloading an electric grid or shutting down a critical energy pipeline, legally speaking, the cyber action is not necessarily a prohibited use of force.

Andrew Folz notes that several legal frameworks have evolved that address the gap in the way international law views force in cyberspace. Almost all shift away from a strictly instruments-based view. The first is an effects-based approach where the “quantum of damage and not the means of attack” determines if an action in cyberspace is a prohibited use of force.¹⁰ This approach only looks at the damage done as a result of the attack and ignores how an attack was delivered. While this framework is relatively simple to apply, it represents a major break from the way the international community already deals with issues of force by completely setting aside the instruments-based framework. Blockades and embargoes would essentially become the same thing, and the international community would lose major tools in conducting international relations. What is worse, it would lead to a subjective assessment of what constitutes a hostile action in cyberspace. If a quantum-of-damage approach is used, the critical question would be who determines what a sufficient amount of damage is to constitute a prohibitive use of force. Each nation, having different strengths and capabilities in the cyber realm, would draw different conclusions.

Another framework is to consider the “kinetic equivalency”¹¹ of a cyber action, where an action in cyberspace only constitutes the use of force if the damage caused by the action could also have been caused by kinetic attack.¹² Overloading an electric grid or shutting down an energy pipeline with a cyber action can now be considered a use of force because those effects could also have been accomplished with a missile or bomb. While this test stays more true to the instruments-based

view of prohibited coercion, it really does not address all actions in the cyber realm, such as painting false targets in an opponent’s radar. No damage was done so there is no kinetic equivalency. Those areas still remain gray.¹³

Duncan Hollis also considers a “target-based” framework, where any attack, cyber or kinetic, on a nation’s critical infrastructure should be construed as a prohibited use of force.¹⁴ However, this framework suffers from the same limitations as the quantum-of-damage framework in that each nation will define what is considered critical infrastructure based on the strategic interests of the nation. A cyber attack on gold mining production in the United States may be treated as a routine crime, but South Africa may consider its gold mining infrastructure critical to its national interests and would construe such an attack as a prohibited use of force.

The Schmitt Analytical Framework

One framework that stays true to the instruments-based method of determining what force is prohibited, yet provides an effective metric for determining whether a cyber action constitutes a use of force, is that presented by Professor Michael Schmitt of the Naval War College. After an interview, Andrew Folz noted that Professor Schmitt’s framework had bridged the gap between an instruments view of force and effects in cyberspace:

Professor Schmitt recognized that discerning the use-of-force threshold is really about predicting how states will characterize and respond to cyber incidents in light of prevailing international norms. To aid in such predictions, his framework bridges the instrument and consequence-based approaches. In keeping with the Article 2(4) instrument based standard, his model consists of seven factors that represent the major distinctions between permissible (that is, economic and political) and impermissible (armed) instruments of coercion.¹⁵

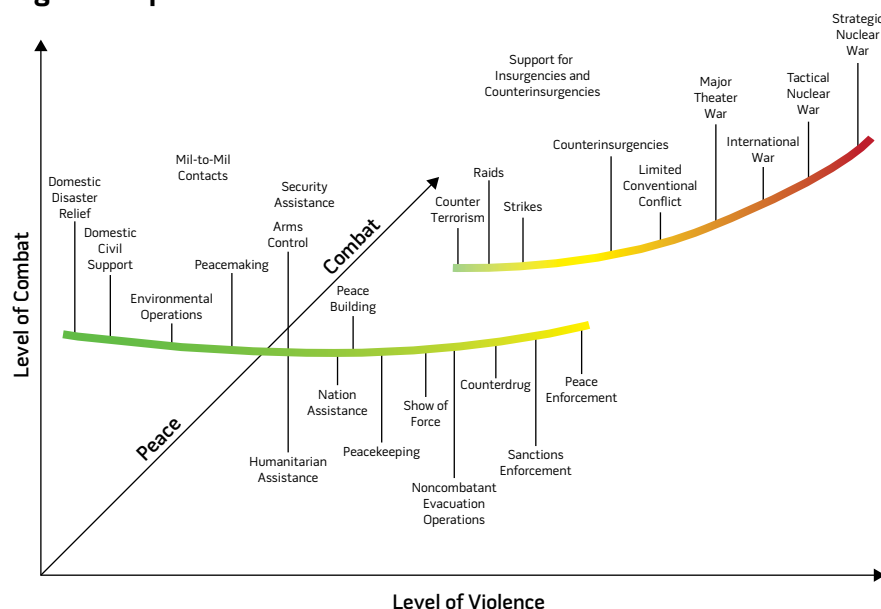
Schmitt’s framework takes the view that the more closely an action in

cyberspace approximates economic or political coercion, the less likely it will be viewed by a nation as an armed attack. Conversely, the more likely an action in cyberspace approximates armed force, the more likely it will be perceived as an armed attack, and hence an illegitimate use of force.¹⁶ Schmitt’s seven factors seek to differentiate between what makes armed force inappropriate and what makes economic and political coercion appropriate. Consider, for example, the differences in characteristics of an oil embargo and a blockade.

Schmitt’s seven factors are as follows:

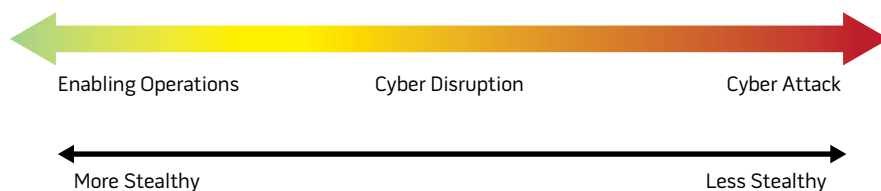
- **Severity:** Armed attacks threaten physical injury or destruction of property, while economic and political coercion do not. Cyber operations that threaten physical harm are more likely to be viewed as a use of force. This includes such characteristics as scope of the action, duration, and intensity.
- **Immediacy:** The damage due to an armed attack usually occurs immediately, while damage due to other forms of coercion develops more slowly. This gives the target nation time to respond to the pressure before damage can take place. Cyber actions whose consequences are immediate, leaving no time for a target nation to respond to pressure or mitigate the consequences, are more likely to be viewed as a use of force.
- **Directness:** Armed attacks can be linked directly to the damage they cause, and other forms of coercion less so. The more directly a cyber action can be linked to its consequences, the more likely the action will be viewed as a use of force.
- **Invasiveness:** In an armed attack, the action usually crosses into a target nation’s territory; other forms of coercion generally stay beyond the target’s borders. So even though armed attacks and economic/political acts may have roughly similar consequences, the armed actions usually are, in the words of Schmitt, “a greater intrusion on the rights of the target state and, therefore, [are]

Figure 1. Spectrum of Conflict



Note: Figure adapted from *Army Vision 2010* (Washington, DC: Headquarters Department of the Army, n.d.), 5, available at <https://rdl.train.army.mil/catalog-ws/view/100.ATSC/CE5F5937-49EC-44EF-83F3-FC25CBOCB942-1274110898250/aledc_ref/army_vision_2010.pdf>.

Figure 2. Spectrum of Cyber Conflict



Source: Gary D. Brown and Owen W. Tullos, "On the Spectrum of Cyberspace Operations," *Small Wars Journal*, December 11, 2012, available at <<http://smallwarsjournal.com/jrnl/art/on-the-spectrum-of-cyberspace-operations>>.

Table 1. Potential Actions in Cyberspace

Ping map	Change or delete data
Probe	Distributed denial-of-service attack (DDoS)
Implant malware	Email bomb
Erase logs	Influence operations in social media
Email fishing	Disable critical infrastructure
Access networks	Damage critical infrastructure
Access email	Attack financial industry
Steal data	Attack military command and control (C2)

more likely to disrupt international stability." The more a cyber operation violates or impairs the territorial integrity or sovereignty of a state, the more likely it will be viewed as a use of force.

- **Measurability:** While the consequences of armed attack are usually easy to determine, the actual negative consequences of other forms of coercion are harder to measure. States are more likely to view a cyber operation as a use of force if the consequences are easily identifiable and objectively quantifiable.
- **Presumptive legitimacy:** In almost every nation, violence is an inappropriate response unless done in self-defense. However, all other forms of coercion are considered lawful unless specifically prohibited by law or treaty. Even actions prohibited by national law, such as espionage, are still considered a legitimate international practice to a certain extent. Cyber actions such as espionage, influence operations, psychological operations, and propaganda, which are legitimately accepted between states, are generally not considered a prohibited use of force.
- **Responsibility:** The more closely a cyber operation can be tied to a state, the more likely it will be viewed as a use of force.

These factors are not an exhaustive list; they are a starting point for further analysis. Nor should they be treated as anything but a holistic approach to characterizing the use of force in cyberspace. Using the Schmitt framework helps set a metric from which to start characterizing potentially hostile actions in cyberspace.

Spectrums of Physical and Cyber Conflict

Armed conflict is not a bi-stable; it does not exist in a state where a potential adversary's action is either a use of force or it is not. In reality, conflict occurs across a spectrum where it is not always clear if an action should be considered hostile or just plain resistant. Figure 1 illustrates this complexity. In the figure,

Table 2. Example of Completed Schmitt Analysis

Cyber action	Severity	Immediacy	Directness	Invasiveness	Measurability	Presumptive Legitimacy	Responsibility
Ping map	1	1	5	7	7	1	3
Probe	2	1	5	7	7	2	3
Implant malware	3	4	5	7	7	3	3
Erase logs	5	5	5	8	7	6	4
Email fishing	4	4	5	5	5	5	5
Access networks	4	5	6	8	5	6	5
Access email	4	5	6	8	5	6	5
Steal data	6	6	6	9	8	6	6
Change or delete data	7	6	6	9	8	8	6
Distributed denial-of-service attack (DDoS)	7	7	7	9	8	8	7
Email bomb	7	5	6	7	7	6	5
Influence operations in social media	6	7	6	6	7	5	7
Disable critical infrastructure	9	8	8	9	8	8	8
Damage critical infrastructure	9	9	8	9	8	8	8
Attack financial industry	8	9	8	9	8	8	8
Military command and control attack	9	9	9	9	9	9	9

there are two shapes: one to the left that represents the spectrum of peace, the other to the right that represents the spectrum of combat. Both use the same sliding scale with level of effort on the left and level of violence across the bottom. Note the overlap near the center. Actions that occur in that overlap region may have different connotations depending on the strategic situation. Does the commander, for instance, desire de-escalation to maintain the peace, or escalation to maintain pressure in accordance with a UN Security Council directive? Any determination of hostile intent in cyberspace must include an understanding of the strategic situation, especially as it pertains to the spectrum of conflict.

Gary Brown and Owen Tullos suggest a spectrum for cyber activity that is based on the *effects* of actions in cyberspace (see figure 2).¹⁷ They postulate that cyber actions fall into three basic categories: enabling actions, which have little impact on the operations of a nation's information infrastructure but can set the stage for future operations and

attacks; cyber disruptions, which may interrupt the flow of information or disrupt the operation of information systems but not cause physical damage or injury; and cyber attack, which may cause physical damage to property or injury to people. Enabling operations tend to be stealthy, and cyber attacks tend to be easily attributable, at least to the point of origin if not the nation responsible.

The Brown and Tullos spectrum is meant to be used in concert with Schmitt's framework. Schmitt's framework provides a detailed metric that is excellent for operational-/strategic-level forensic analysis of an attack but may be too complex for use at the tactical level. Brown and Tullos completely abandon the instruments-based metric for determining if use of force is warranted, but the spectrum is helpful, especially when combined with the overall strategic picture, in establishing what immediate actions are appropriate when a cyber action is detected. Taken together—Schmitt for the strategic analysis and understanding the operational landscape, and Brown and Tullos for deploying

appropriate countermeasures—we create a solid framework for determining hostile intent in cyberspace.

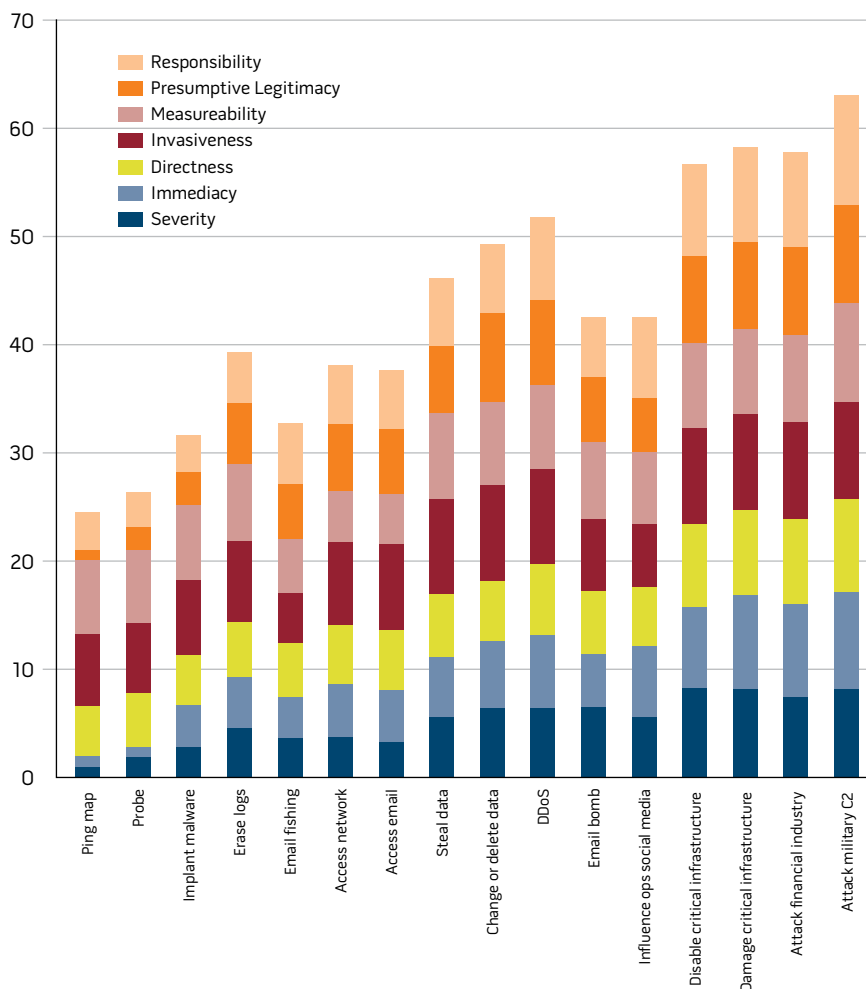
Determining Hostile Intent in Cyberspace

Establishing that framework starts with understanding the strategic situation. Where is the Nation or joint force operating with regard to the spectrum of conflict (figure 2)? How do partner nations and potential adversaries view the strategic situation? Understanding this landscape helps establish priorities and appropriately weighs factors during the Schmitt analysis.

Conducting the Schmitt Analysis.

The analysis begins with a list of potential actions in cyberspace (see table 1). This list of actions is not meant to be specific or exhaustive but strategic and general, similar in manner to how the Standing Rules of Engagement issued by the Chairman of the Joint Chiefs of Staff start out as strategic and general but are modified with more specificity by commanders closer to the conflict. The list should generally and broadly cover the body of

Figure 3. Example of Schmitt Analysis Stack



actions that may occur in cyberspace that have impacts in the theater or area of operations.

Schmitt did not intend for his model to be a quantitative tool but rather to be used as a heuristic. Keeping that in mind, an analyst would use the seven factors to perform a *qualitative* analysis of each action on the list; each action would be evaluated for each Schmitt factor on how close the effects of that action would be to the kinetic effects of an armed attack. For simplicity's sake, analysis would use a scale of 1 to 10—where a 1 means that characteristic is far away from a kinetic effect and a 10 is exactly like a kinetic effect. Once each action is evaluated for each factor (see table 2), the results could then be stacked to give a reasonable comparison of which cyber action is more hostile compared to another.

Determining Response with the Brown-Tullos Spectrum. The Schmitt Analysis Stack (figure 3) gives a good indication of what a commander can consider a hostile act in cyberspace. Figure 4 takes the stack of actions, from least hostile to most hostile, and lays them on the Brown-Tullos Cyber Action Response Spectrum. Using the three general categories in Brown-Tullos (enabling operations, cyber disruption, cyber attack), a commander can develop general responses appropriate to the level of hostility indicated by the action. More importantly, the commander can add or subtract responses, or even move responses up and down the spectrum based on the strategic environment in the theater. For instance, an adversary's access to an unclassified network may be considered enabling operations in a theater at

peace, so the response may be to simply monitor and report the covert access. As tensions rise in the area of responsibility, the response may be adjusted to block and report, or even to conduct a counter cyber action against the adversary.

When used in conjunction with one another, the Schmitt Analysis and Brown-Tullos Cyber Action Response Spectrum provide a commander with a flexible tool to determine an appropriate range of responses to a range of cyber actions. Additionally, both can be useful in coordinating cyber responses from different agencies with differing legal authorities. Figure 5 gives an example of how such authorities may be specified. Note that this matrix shows responsibility for action. The Defense Information Systems Agency or the National Security Agency may respond to a ping map or probe on a Department of Defense (DOD) network, but has no legal authority to pursue the perpetrator who resides in the United States; law enforcement would be responsible for that action, and DOD entities would have to coordinate with law enforcement to take action.

Conclusion

Use of force is not simply in the eye of the beholder; there is a rugged, tested framework that is reflected in the United Nations Charter that governs what is acceptable coercion and what is prohibited use of force. Staying as close to that framework as possible when determining hostile intent in cyberspace means we stay close to the use-of-force lessons and applications of the past six decades. An evolutionary development of the legal basis is more appropriate than a revolutionary development.

Some issues of concern remain: even though it is useful for evaluating the strategic/operational cyber landscape, the Schmitt framework was never meant for real-time battlefield analysis. The analytical framework presented is meant to give the commander a *feel* for how hostile a cyber action is and help plan appropriate responses ahead of time. The analysis is also not meant to be static but dynamic, based on continuous analysis of the cyber landscape. New tools, techniques,

vulnerabilities, and mitigations must be continuously taken into account with the strategic situation to accurately stack all the factors and give a commander the right situational awareness. Additionally, the Brown-Tullos spectrum starts out as an effects-based spectrum and only takes into account the instruments of force after Schmitt has been applied. Both must be used together, therefore, one for the strategic/operational analysis, the other to communicate immediate actions at the tactical level.

The real test for any method of determining hostile intent is how it works operationally—that is, how easily it can be employed on the battlefield. The cyber battlefield is not physical; it is abstract, but its effects have real consequences in the physical world. The results of tests can be quickly seen and applied, and the method improved in a short period of time. JFQ

Figure 4. Example of Brown-Tullos Cyber Action Response Spectrum

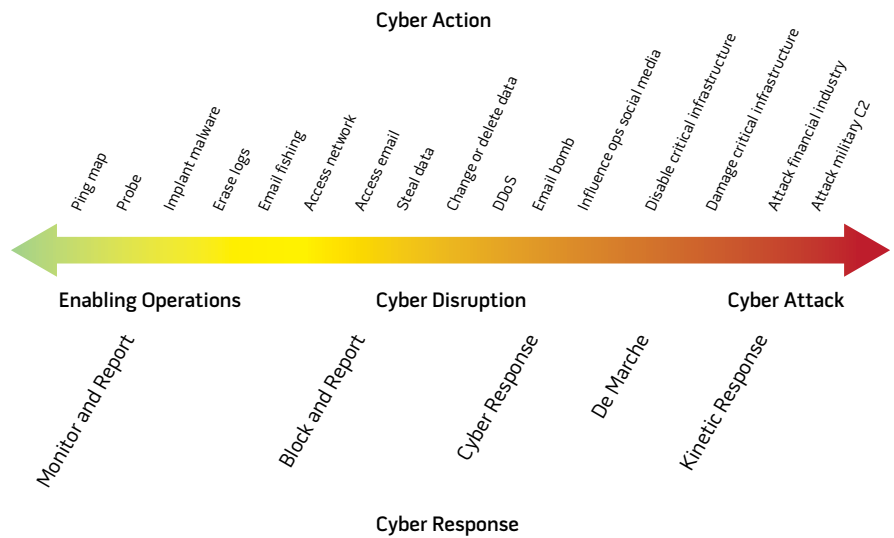
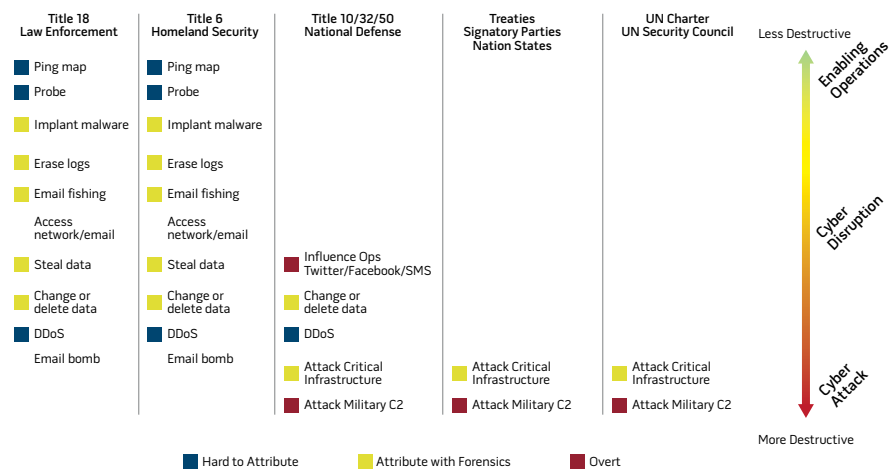


Figure 5. Responsibility for Threats in Cyberspace



Notes

¹ “Splash Two MiGs,” *Fly.Historicwings.Com*, January 4, 2013, available at <<http://fly.historicwings.com/2013/01/splash-two-migs>>.

² Chairman of the Joint Chiefs of Staff Instruction 3121.01B, “Standing Rules of Engagement/Standing Rules for the Use of Force for U.S. Forces,” Washington, DC, June 13, 2005.

³ International and Operational Law Department, *Operational Law Handbook* (Charlottesville, VA: U.S. Army Judge Advocate General’s Legal Center and School, 2012).

⁴ Jude E. Franklin, “CCRTS C2 Plenary Panel,” June 30, 2006, available at <www.dodccrp.org/events/2006_CCRTS/html/presentations/1_Panel.pdf>.

⁵ Sun Tzu, *The Art of War*, ed. James Clavell, trans. Samuel B. Griffin (New York: Delacorte Press, 1989).

⁶ “The Hot Air Balloon,” *Century-of-flight.net*, available at <www.century-of-flight.net/new%20site/frames/balloons_frame.htm>.

⁷ Andrew C. Folz, “Stuxnet, Schmitt Analysis, and the Cyber ‘Use-of-Force’ Debate,” *Joint Force Quarterly* 67 (4th Quarter 2012), 40–48.

⁸ Matthew C. Waxman, “Cyber Attacks and the Use of Force: Back to the Future of Article 2(4),” *The Yale Journal of International Law* 36, no. 42 (2011), 421–459.

⁹ Ibid.

¹⁰ Folz, 40–48.

¹¹ Duncan B. Hollis, “Why States Need an International Law for Information Operations,” *Lewis and Clark Law Review* 11, no. 4 (2007), 1023–1061.

¹² Folz, 40–48.

¹³ Ibid.

¹⁴ Hollis, 1023–1061.

¹⁵ Folz, 40–48.

¹⁶ Ibid.

¹⁷ Gary D. Brown and Owen W. Tullos, “On the Spectrum of Cyberspace Operations,” *Small Wars Journal*, December 11, 2012, available at <<http://smallwarsjournal.com/jrnl/art/on-the-spectrum-of-cyberspace-operations>>.

Asymmetric Warfare Group Advisor takes cover with Soldiers while man-portable line charge system is detonated during training exercise near Forward Operating Base Zangabad, Afghanistan (U.S. Army/Alex Flynn)



Understanding the Enemy

The Enduring Value of Technical and Forensic Exploitation

By Thomas B. Smith and Marc Tranchemontagne

The escalation of improvised explosive device (IED) incidents and related casualties during Operations *Iraqi Freedom* and *Enduring Freedom* led to a new intelligence

Captain Thomas B. Smith, USN, is Commanding Officer of the Naval Surface Warfare Center Indian Head, Explosive Ordnance Disposal Technology Division. Commander Marc Tranchemontagne, USN (Ret.), was an Explosive Ordnance Disposal Officer. He is currently an Associate with R3 Strategic Support Group.

field related to technical intelligence (TECHINT) called *weapons technical intelligence* (WTI), which combined technical and forensic IED exploitation techniques to link persons, places, things, and events. WTI operationalizes technical and forensic activities by fusing the technical, forensic, and biometric disciplines to produce actionable intelligence for countering threat networks. It is an especially powerful tool against terrorist organizations that rely on IEDs as a primary weapon

in their arsenals. Given the enduring nature of the IED problem, careful consideration is required to ensure that we have the necessary counter-IED capability and capacity to meet future threats across the range of military operations. Across this range and at each level of war from tactical to strategic, TECHINT and WTI make critical contributions to joint warfare and military decisionmaking.

WTI development has been incremental and idiosyncratic and has led

to the fielding of a number of new capabilities including Counter-IED Task Forces, Counter-IED Operations/Intelligence Centers, Combined Explosives Exploitation Cells (CEXCs), Expeditionary Forensic Labs (EFLs—formerly Joint Expeditionary Forensic Facilities), and Weapons Intelligence Teams, all of which contribute to WTI. A few capabilities have been written into doctrine or have become programs of record, such as the CEXC platoons, which deploy small footprint expeditionary laboratories for the technical exploitation of IEDs and other ordnance, and the Army EFLs, which perform expeditionary forensic exploitation of IEDs as their name implies.¹ The relationships among these organizations, however, remain largely ad hoc; in the maritime domain, they are untested. These exploitation capabilities—technical and forensic, with the related discipline of biometrics—should be tested with multi-Service concepts of operation, exercised jointly, integrated into joint operational planning, and codified in joint doctrine that addresses the exploitation enterprise holistically.

The need for improved planning and interagency cooperation in counter-IED operations is well documented. A recent Government Accountability Office report found that Department of Defense (DOD) strategic planning does not adequately document the milestones and metrics required to achieve desired goals.² Additionally, Presidential policy directs interagency efforts toward effectively exploiting IED materials, advancing our information analysis, and maintaining our deployable counter-IED resources, among other activities.³ For the foreseeable future, terrorist use of IEDs is expected to “pose a fundamental, significant and enduring threat.”⁴

Discussion

Across the range of military operations, traditional TECHINT takes primacy in conventional conflict, and WTI takes primacy in irregular warfare.⁵ Traditional TECHINT products are used to “prevent technological surprise, neutralize an adversary’s technological advantages, enhance force protection . . . [and]

support the development and employment of effective countermeasures,” as well as inform acquisition priorities and shape strategic decisionmaking.⁶ The Army, for example, maintains antiarmor and antiair task forces that analyze battle damage to identify enemy capabilities, friendly technological gaps, countervailing tactics, techniques, and procedures (TTPs), and areas for product improvement. Although a single weapons system is seldom decisive on its own, new or enhanced technologies can be disruptive. U.S. military superiority serves as a strategic deterrent to war, and U.S. technological superiority underpins that military advantage.⁷

WTI allows operational commanders to interrupt an enemy’s decision cycle and interdict IED tactical employment in real time. Simply put, it can mitigate the costs of technical surprise in terms of personnel, equipment, and dollars by placing better information in the hands of warfighters when prioritizing and planning operations. Its five outcomes—force protection, targeting, component and material sourcing, support to prosecution, and signal characterization—contribute to operational success in irregular warfare. WTI supports counterinsurgency and counterterrorism in current contingencies, but could also contribute to peace enforcement, counterpiracy, maritime security, promoting the rule of law, and countering other irregular challenges. At the operational and tactical levels of war, WTI contributes directly to the doctrinal counter-IED lines of operation: attack the network, defeat the device, and train the force.⁸ In some cases, due to lack of either international agreement or deployed capacity, valuable information is lost when captured material is disposed of where it is found rather than being routed to a forward WTI facility for analysis.

Terrorist and insurgent groups have used IEDs so effectively in Iraq and Afghanistan that they have been called “weapons of strategic influence.”⁹ Terrorists have been proficient at synchronizing IED attacks with information operations to weaken public confidence in the government, demonstrate terrorist

effectiveness, and damage coalition morale. On March 11, 2004, for example, terrorists simultaneously detonated bombs on four trains near Madrid 3 days before Spain’s general election. The incumbent president had a small lead in opinion polls going into the election and was favored to win in spite of his unpopular decision to contribute Spanish troops to the U.S.-led coalition in Iraq. The attacks killed 191 people, wounded 1,800, and changed the outcome of the election, which led to Spain withdrawing its forces from Iraq. Strategically, terrorists have also used IED attacks to influence U.S. public opinion and undermine the Nation’s political resolve.

In October 2011, the Department of Justice unsealed an indictment describing the illegal export of electronic devices to Iran. Four men from Singapore purchased 6,000 radio frequency (RF) modules through a Singapore front company, which were forwarded to Iran through third countries and ended up in IEDs in Iraq. Between 2008 and 2010, the U.S. military recovered 16 of the RF modules from IEDs in Iraq. By locally exploiting the recovered IEDs, the U.S. Government was able to trace the RF modules by serial number from the United States to Iran and then to the IEDs in Iraq.¹⁰ This success is an example of the strategic implications of technical exploitation—in this case, exposing third country support to an insurgency—and the importance of a continuum from collection through out-of-theater exploitation with connections to the broader Intelligence Community.

At the operational level of war, TECHINT and WTI inform military decisionmaking by supporting intelligence preparation of the operational environment and helping to protect friendly critical requirements, identify enemy critical vulnerabilities, and attack the enemy center of gravity. Insurgent reliance on IEDs in Iraq created an opportunity for coalition forces. For the insurgents, IEDs were a critical requirement—the most lethal, effective, and fearsome weapons they possessed—that also proved to be a critical vulnerability. Initially regarded primarily as a force protection issue, the

IED came to be viewed more properly as an intelligence opportunity that could yield key information about the network of bomb designers, builders, emplacers, triggermen, financiers, component suppliers, trainers, planners, and operational leaders who made up the web of actors who execute IED attacks.¹¹

WTI contributes to defeating the enemy center of gravity because it provides insight into the network—how it is led and sustained and how it operates—that is critical to defeating it. Attack-the-network operations fit neatly within the find, fix, finish, exploit, analyze, disseminate (F3EAD) architecture developed by the special operations community during counterterrorism operations in Iraq and Afghanistan. When synchronized with biometric enrollment and detention operations, WTI creates synergy that deepens the operational commander's knowledge of the adversary. Forensic information correlated to biometric databases allows coalition forces to associate a specific IED to a discrete individual, link clusters of devices to a specific bombmaker or IED cell, recognize patterns of insurgent operations, and identify named areas of interest against which commanders can plan operations. Technical exploitation of IED components can indicate where a bombmaker learned his technique and whether IED components were obtained locally or imported.

For democracies such as the United States, political will and public support tend to be critical vulnerabilities—possibly even the friendly center of gravity at the strategic level. IEDs are used by the enemy in part to sow fear, create a perception of host nation weakness, undermine troop morale, split coalitions, provoke overreaction by security forces, alienate local populations, and erode political will. WTI has been used extensively to support rule of law initiatives that demonstrate the effectiveness of the host nation's judicial system and reinforce public confidence in the legitimacy of the government. Identifying the perpetrators of attacks on civilians can help to isolate insurgents from the populace and undermine their propaganda.

In terms of joint functions, TECHINT and WTI support command and control (now replaced by *mission orders* in Army doctrine), fires, movement and maneuver, intelligence, sustainment, and protection.¹² In counterinsurgency, understanding the enemy network allows commanders to develop actionable intelligence and exercise “disciplined initiative” consistent with commander's intent.¹³ Understanding how the enemy perceives the operational environment can inform a commander's decisions on such matters as arranging forces, designating operational areas, achieving effective span of control, and synchronizing operations. The fusing of technical, forensic, and biometric information into actionable intelligence permits precise fires to shape the operational environment, including supply chain interdiction, counterthreat finance operations, information operations, cache destruction, and the capture of high-value individuals. Landmines, IEDs, and naval mines are antiaccess and area-denial weapons that serve as impediments to both movement (for example, the reception, staging, and onward integration of coalition forces) and maneuver. Moreover, mines and IEDs are often used to prevent sustainment and resupply of friendly forces. At the strategic level of war, naval mines can be used to blockade critical ports and target commercial shipping in a strangulation strategy. Technical exploitation of these weapons informs strategic and operational planning and facilitates the development of countermeasures and countervailing TTPs.

Operational analysis demonstrates that WTI yields measurable effects on the battlefield and can be used by commanders to set operational priorities. Recent analysis in Afghanistan, for example, showed that removing bombmakers from the battlefield led to statistically significant reductions in IED attacks in a given area for a quantifiable period of time. Other generally accepted metrics such as cache destruction and route clearance showed no statistically significant effect.¹⁴ Compelling statistical evidence that defeating even relatively low-level insurgent

bombmakers produces measurable effects won over skeptical commanders and resulted in a marked increase in evidence-based targeting.¹⁵ Bombmaking requires special skills and training that are not easily replaced.

Technical exploitation is critical to ensuring that the U.S. Armed Forces maintain a technological advantage against any adversary. Across all phases of operations from peacetime-shaping through stability operations and enabling civil authority, technical exploitation and foreign material acquisition functions provide critical TECHINT on an enemy's ordnance order of battle. An understanding of adversary strengths and weaknesses gained from exploitation of enemy ordnance may influence operational planning and force protection.¹⁶ During World War II, for instance, Germany developed bomb fuzes with antihandling mechanisms to target British bomb disposal personnel during the blitz. Exploitation of recovered fuzes led to countermeasures that allowed clearance operations to continue. It also led to tighter operational security regarding bomb disposal procedures. Recovering captured enemy equipment—including enemy ordnance—is both a combatant command and national requirement and is doctrinally performed at the operational level by a Joint Captured Material Exploitation Center with reachback and collaboration across the interagency.¹⁷

The forensic aspect of exploitation, which links persons, places, things, and events, supports theater strategic goals of reestablishing the rule of law by supporting criminal prosecutions. While getting bombers off the street or battlefield is a positive end in itself, demonstrating the effectiveness of the host nation's judicial system reinforces public confidence in the legitimacy of the host nation government. Identifying the perpetrators of attacks on civilians helps cut insurgents off from the populace and undermines their propaganda. The public's faith in its government and civic institutions' ability to deliver positive social goods is essential to winning in counterinsurgency, where the goal is less to defeat the insurgent than to make him irrelevant.

Exploitation can also provide a powerful metric for evaluating policy. In Iraq, fingerprint matches from recovered IEDs have demonstrated that the recidivism rate among released detainees was higher than believed and that Iraq's amnesty program had returned many bad actors to the street. In Afghanistan, evaluation of recovered homemade explosives (HME) provides insight into the effectiveness of programs to ban the importation of certain fertilizers used in HME production. While the in-country exploitation of IEDs is considered operational, it provides the crucial linkage to strategic, national, and special exploitation capabilities, such as the Federal Bureau of Investigation's (FBI's) Terrorist Device Analytical Center, National Ground Intelligence Center, U.S. Army Criminal Investigation Laboratory, and other national resources.

One way exploitation can influence strategic decisionmaking is by providing early indication of third-country participation in a conflict or state sponsorship of a terrorist organization. For example, the technical exploitation of explosively formed penetrators (EFPs) during Operation *Iraqi Freedom*, corroborated by other intelligence, provided an early indication that EFPs were not being manufactured in Iraq but were imported from a third country. Metallurgy helped confirm that the high-purity copper EFP liners were not produced in Iraq. Differences in the liners indicated the kind of press that was required to fabricate them—a heavy press not commonly seen in Iraq—as well as an indication of the number of different presses that were being used.¹⁸ Similarly, identifying third-country conventional ordnance in a war zone might belie that country's claims of neutrality. In an insurgency, foreign ordnance might indicate external support, arms smuggling, or the presence of foreign fighters. Such evidence can shape strategic decisionmaking.

Technical exploitation can provide evidence of violations of international law and treaties. In countering the proliferation of chemical, biological, radiological, nuclear, and high-yield explosive weapons of mass destruction (WMD), identifying

the country of origin of recovered, seized, or contraband weapons would be a necessary precursor to diplomatic or other action under the Proliferation Security Initiative. Moreover, characterizing the extent of the threat posed by WMD requires an understanding of the level of sophistication of such weapons. In peace enforcement operations, the recovery and exploitation of banned weapons might provide evidence of cease-fire violations. Likewise, the exploitation of recovered drifting mines can provide evidence of violations of international norms and treaties—in this example, the Hague Convention of 1907.

The presence of naval mines in the northern Arabian Gulf was one factor that prevented an amphibious landing at Ash Shuaybah, Kuwait, during Operation *Desert Storm*. Later technical exploitation of these mines showed that many were neither active nor laid effectively. In fact, many lacked batteries and sensors.¹⁹ Had this technical information been available earlier, it might have influenced operational and, perhaps, theater-strategic planning.

At the tactical level of war, WTI outcomes help to predict, prevent, detect, neutralize, and mitigate IED attacks. They have been essential in the development of electronic countermeasures for radio-controlled IEDs and have created new opportunities for commanders to gain tactical advantages in novel ways. WTI outcomes are used to target insurgents, develop force protection measures, formulate counter-IED TTP, design countermeasures, provide indications and warnings of IED attacks, interdict supplies and precursors, and support prosecution by the host nation. The exploitation of an IED incident also yields important information about incident geometry that can help friendly forces understand where an insurgent is likely to emplace an IED or how he might trigger it.²⁰ Not only do WTI products help friendly forces develop TTP to avoid IED ambushes, but they also enable commanders to target the insurgents who employ the devices. WTI allows tactical forces to seize the initiative and become the hunter rather than the hunted.

The Way Ahead

Lessons learned from technical and forensic exploitation in Iraq and Afghanistan have created new capabilities, interdisciplinary methodologies, and operational units for the technical and forensic exploitation of explosives, explosive hazards, and foreign ordnance. The institutionalization of these capabilities—directed by the Joint Requirements Oversight Council—has been incremental, and no joint operating concept for their employment exists. Nor is there an operating concept or doctrine for organizing and employing the various technical and forensic organizations, disciplines, functions, and processes resident in DOD and the Interagency.

Many stakeholders exist across DOD and the other Federal agencies. The Defense Intelligence Agency has primary responsibility for intelligence activities and programs related to forensics.²¹ The Navy is the DOD Single Manager for explosive ordnance disposal (EOD) technology, which includes technical exploitation of recovered explosives, explosive devices, and other explosive hazards. The Navy executes this responsibility through the Indian Head EOD Technology Division.²² The Army is the DOD Executive Agent (EA) for forensic disciplines relating to DNA, serology, firearms and tool marks, latent prints, questioned documents, drug chemistry, and trace materials, as well as forensic medicine disciplines.²³ It is also the EA for biometrics, a separate but related and complementary field that uses measurable biological and behavioral characteristics to uniquely identify people.²⁴ The Air Force is the EA for Digital and Multimedia Forensics relating to computer and electronic device forensics, audio forensics, image analysis, and video analysis.²⁵ Counter-IED operations in Operations *Iraqi Freedom* and *Enduring Freedom* have also relied on coalition partners, particularly the British, who have a lot of experience with WTI.

The Services have developed a variety of modular, scalable, deployable laboratories for overseas contingencies, including those used by the Navy CEXC



Afghan and coalition security force uncovers Taliban weapons cache containing materials for constructing IEDs, including ammonium nitrate, homemade explosives, and detonation triggers, during operation in Helmand Province (DOD/Justin Young)

platoons and Army EFLs. The Army also maintains heavy and light mobile laboratories to conduct field confirmatory chemical, biological, and explosive analysis and near-real-time chemical air monitoring. Experience in Operations *Iraqi Freedom* and *Enduring Freedom* demonstrates that an in-country exploitation capability provides a degree of responsiveness due to physical and psychological proximity to the warfighter that a U.S.-based capability cannot match while providing a comparable level of exploitation. Laboratory exploitation in recent operations has taken place in large bases as well as austere forward operating bases. Extension of these operations continues in U.S. Naval Forces Central in support of Combined Task Force 56, for example, moving a comprehensive capability outside Iraq and Afghanistan for the first time to assist in partnering efforts. Moving a scaled-down laboratory

element forward for a major operation could improve timely intelligence delivery to the warfighter even further. Scaling these laboratories for ground transport on heavy vehicles, intertheater lift, and seabasing has recently been exercised and is already supporting combatant command exercise and engagement plans.

Technical and forensic exploitation operations have not been exercised in a maritime context. Maritime operations might include operating from a seabase, supporting maritime security operations, supporting a Marine Air-Ground Task Force ashore, and conducting WTI operations for underwater threats. The Navy has only a minimal capability to collect forensic evidence in the aftermath of an underwater explosive incident such as the terrorist IED attack against the destroyer USS *Cole* or the sinking of the South Korean corvette ROKS *Cheonan* by a North Korean submarine.

It lacks appropriate doctrine, procedures, training, and equipment to conduct site exploitation and postblast investigation underwater to support WTI—a task that only Navy EOD technicians can execute due to the diving requirement. The FBI runs an underwater postblast investigation course, but it does not provide unit-level training.

The 2010 Quadrennial Defense Review (QDR) identified several key initiatives to ensure that DOD is prepared to provide appropriate support to civil authorities. Regarding counter-IED operations, it states, “to better prepare the Department to support civil authorities seeking to counter potential threats from domestic IEDs, DOD will assist civil authorities with counter-IED TTPs and capabilities developed in recent operations.”²⁶ This contingency has not been exercised and the authorities have not been worked out, but it would seem that

DOD's expertise in counter-IED technical and forensic exploitation operations would be an important asset for defense support of civil authorities. Immediate military support to civilian authorities by EOD forces is allowed by U.S. law but is also ad hoc. As recently demonstrated, the Army's 387th Ordnance Company responded to 64 "call outs" during the Boston Marathon bombing.²⁷ Mindful of the Posse Comitatus Act, we should provide a seamless system that credentials and integrates military EOD operations in support of civil authorities nationally.²⁸

The proliferation of IED knowledge suggests that these devices will continue to be used by terrorists, insurgents, and criminal elements at home and abroad. The Army's EFLs and the Navy's Technical Support Detachment with its subordinate CEXC platoons would be well suited to fulfill the QDR priority of enhancing domestic counter-IED capabilities. The Armed Forces have a large body of combat-tested military EOD technicians experienced in the IED fight who could quickly mobilize to support civilian efforts in the aftermath of an event similar to the Boston and Oklahoma City detonations, or worse, a sustained terrorist bombing campaign. Formal training and credentialing to facilitate their employment in support of civilian authorities in the event of a significant disaster are among the easier options.

Summary

The exploitation of enemy ordnance has important strategic implications for preventing technological surprise and informing strategic decisionmaking. At the strategic level of war, scientific and technical intelligence and WTI can help to:

- ensure U.S. technological advantage and its implicit deterrent effect
- prevent a future enemy from benefiting from disruptive new technologies or counter those technologies once fielded
- support operational and theater-strategic planning
- indicate third-country involvement in hostilities

- indicate state sponsorship of terrorist organizations
- provide evidence of violation of international norms and treaties
- provide metrics for evaluating theater-strategic and national policies
- support development of formal international partnerships
- enable combatant command theater security cooperation plans.

At the operational level of war, TECHINT and WTI contribute to:

- the three counter-IED lines of operation and F3EAD: attack the network, defeat the device, and train the force
- operational planning (Joint Operation Planning Process, Military Decision Making Process, network planning process)
- intelligence preparation of the operational environment
- host nation rule of law
- enabling formal data and information exchanges.

At the tactical level of war, TECHINT and WTI provide information used to:

- target insurgents
- develop force protection measures
- develop friendly TTPs
- develop countermeasures
- provide indications and warnings of IED activity
- interdict supplies and precursors
- support prosecution by the host nation.

Conclusion

An operating concept for conducting expeditionary technical and forensic exploitation would provide commanders with a framework for organizing and employing joint force technical and forensic exploitation capabilities. It would provide a holistic, synchronized approach to integrate multiple organizations, disciplines, functions, and processes that support technical and forensic exploitation. It would provide a joint task force commander a framework for planning, organizing, and executing technical and forensic exploitation

operations including those in a maritime environment. Using lessons learned from Iraq and Afghanistan, a concept of operations would identify best scientific, technical, and operational practices for experimentation and future Service and Joint doctrine. While a number of new organizations and capabilities have emerged to confront IEDs, no complete doctrine, organization, training, materiel, leadership and education, personnel, and facilities solution exists for planning and executing technical and forensic exploitation operations across the range of military operations. Given the proven value of technical and forensic exploitation operations across this range and at every level of war, with the related discipline of biometrics, these exploitation capabilities should be tested with multi-Service concepts of operation, exercised jointly, and codified in joint doctrine that addresses the entire exploitation enterprise. JFQ

Notes

¹ In 2008, the Joint Requirements Oversight Council (JROC) directed the institutionalization of CEXC and the Joint Expeditionary Forensic Facilities (now EFL) through a doctrine, organization, training, materiel, leadership and education, personnel, and facilities (DOTMLPF) Change Request, JROCM 128-08. Joint Staff Memorandum, JROCM 128-08, *Joint Improvised Explosive Device (IED) Defeat DOTMLPF Change Recommendation*, June 20, 2008.

² U.S. Government Accountability Office (GAO), *Defense Forensics: Additional Planning and Oversight Needed to Establish an Enduring Expeditionary Forensic Capability: Report to Congressional Requesters* (Washington, DC: GAO, June 2013), 9, available at <www.gao.gov/assets/660/655546.pdf>.

³ The White House, "Countering Improvised Explosive Devices," Policy Statement, February 26, 2013, 3, available at <www.whitehouse.gov/sites/default/files/docs/cied_1.pdf>.

⁴ Presidential Policy Directive 17, *Countering Improvised Explosive Devices* (Washington, DC: The White House, June 15, 2012), 2.

⁵ Defense Intelligence Agency (DIA) and Joint Improvised Explosive Device Defeat Organization, *Weapons Technical Intelligence Handbook*, Version 1.1 (Washington, DC: DIA, October 2010), 9.

New from NDU Press

for the Center for Strategic Research

Strategic Perspectives 17
*The Indian Jihadist Movement:
Evolution and Dynamics*
by Stephen Tankel



India has been confronting a jihadist threat from Pakistan for decades. Expeditionary terrorism typically receives the

most focus, but indigenous actors benefiting from external support are responsible for the majority of jihadist attacks in India. The Indian mujahideen network, which announced its presence to the public via media in 2007, is the latest and most well known manifestation of the indigenous Islamist militant threat. As Stephen Tankel details in this paper, however, its members were active before then. Moreover, a small number of Indian Muslims have been launching terrorist strikes—with and without Pakistani support—for more than two decades. The dynamics of Indian jihadism and the nature of India's evolving counterterrorism response are not easy to comprehend. This is understandable given that, even among Indian security officials and analysts, a knowledge gap exists.



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

⁶ Joint Publication (JP) 2-0, *Joint Intelligence* (Washington, DC: The Joint Staff, June 22, 2007), B-6.

⁷ At the strategic level, TECHINT is called scientific and technical intelligence (S&TI); JP 2-0, B-6.

⁸ The term *attack the network* is gradually being replaced by *countering threat networks*. For additional information on counter-IED lines of operations, see JP 3-15.1, *Counter-Improvised Explosive Device Operations* (Washington, DC: The Joint Staff, January 9, 2012), III-5.

⁹ Joint Improvised Explosive Device Defeat Organization (JIEDDO), "Official Website of the Joint IED Defeat Organization," available at www.jieddo.dod.mil/index.aspx. According to the mission statement, "JIEDDO leads DOD [Department of Defense] actions to rapidly provide Counter Improvised Explosive Device (C-IED) capabilities in support of the Combatant Commanders and to enable the defeat of the IED as a weapon of strategic influence."

¹⁰ Peter Finn, "U.S. Parts Illegally Used for Iraq Bombs: Trigger Modules Were Smuggled to Iran, Indictment Charges," *The Washington Post*, October 26, 2011, A9, available at http://articles.washingtonpost.com/2011-10-25/world/35277242_1_hossein-larijani-hia-soo-gan-benson-iranian-procurement-networks.

¹¹ For a discussion of critical factors (capabilities, requirements, and vulnerabilities) and center of gravity, see JP 5-0, *Joint Operation Planning*, and Naval Warfare Publication 5-01, *Naval Planning*. JP 5-0 defines *critical vulnerability* as "an aspect of a critical requirement which is deficient or vulnerable to direct or indirect attack that will create decisive or significant effects." JP 5-0, *Joint Operation Planning* (Washington, DC: The Joint Staff, August 11, 2011), III-23-25.

¹² "Joint functions are related capabilities and activities grouped together to help JFCs integrate, synchronize, and direct joint operations. Functions that are common to joint operations at all levels of war fall into six basic groups—C2, intelligence, fires, movement and maneuver, protection, and sustainment." JP 3-0, *Joint Operations* (Washington, DC: The Joint Staff, August 11, 2011), chapter III.

¹³ Field Manual (FM) 3-0, *Operations*, Change 1 (Washington, DC: Headquarters Department of the Army, February 22, 2011), 5-2.

¹⁴ Colonel Leo Bradley, USA, commander, Combined Joint Task Force Paladin, "Personal Observations," lecture, Defense Strategies Institute, EOD/IED and Countermines Symposium, July 24, 2013.

¹⁵ Lieutenant Sarah Turse, USN (former officer-in-charge, CEXC Afghanistan), interview by Marc Tranchemontagne, August 27, 2012.

¹⁶ JP 2-01, *Joint and National Intelligence Support to Military Operations* (Washington, DC: The Joint Staff, October 7, 2004), III-32.

¹⁷ Ibid. The Joint Captured Material Exploitation Center is one of three doctrinal Joint Exploitation Centers, along with the Joint Document Exploitation Center and Joint Interrogation and Debriefing Center.

¹⁸ Commander Scott Kraft, USN (former officer-in-charge, CEXC Iraq, Baghdad), interview by Marc Tranchemontagne, October 18, 2011.

¹⁹ DOD, *Conduct of the Persian Gulf War: Final Report to Congress*, April 1992, 286, available at www.dod.mil/pubs/foi/operation_and_plans/PersianGulfWar/404.pdf. "Many deployed mines lacked sensors or batteries which prevented their proper operation. During MCM operations, 95 percent of the UDM-type acoustic influence mines were evaluated as inoperable. Several moored contact mines were recovered on the bottom and apparently 13 percent of the moored mines broke away from their moorings. However, even the poorly planned and improperly deployed minefields caused damage to two combatants and were one of several reasons the amphibious invasion was not conducted."

²⁰ DIA, 23-29.

²¹ DOD, *DOD Forensic Enterprise (DFE)*, DOD Directive 5205.15E (Washington, DC: DOD, April 26, 2011), 2, available at www.dtic.mil/whs/directives/corres/pdf/520515e.pdf.

²² In 1947, the Bureau of Naval Weapons established the first unit for research, development, test, and evaluation (RDT&E) of explosive ordnance disposal EOD equipment at the U.S. Naval Powder Factory within the EOD School. It eventually became the EOD Technology Center and, presently as NSWC Indian Head EOD Technology Division, has had joint service responsibility for EOD RTD&E since 1951, as directed in DODD 5160.62, *Single Manager Responsibility for Explosive Ordnance Disposal Technology and Training (EODT&T)*.

²³ DOD, *DOD Forensic Enterprise*, 1, available at www.dtic.mil/whs/directives/corres/pdf/520515e.pdf.

²⁴ DOD, *DOD Biometrics*, DOD Directive 8521.01E (Washington, DC: DOD, February 21, 2008), 1, available at www.dtic.mil/whs/directives/corres/pdf/852101p.pdf.

²⁵ DOD, *DOD Forensic Enterprise*.

²⁶ DOD, *Quadrennial Defense Review Report* (Washington, DC: DOD, February 2010), 20, available at www.defense.gov/qdr/qdr%20as%20of%2029jan10%201600.PDF.

²⁷ Rick Crawford, "Testimony," House Armed Services Committee, EOD Priorities for FY2012 NDAA, 112th Cong., 1st sess., 2012, available at <http://docs.house.gov/meetings/AS/AS00/20130508/100806/HHRG-113-AS00-Wstate-C001087-20130508.pdf>.

²⁸ The Posse Comitatus Act of 1878, 18 U.S.C. §1385, as amended, limits the power of the Federal Government to enforce laws using Federal military personnel.



Marshal Josip Tito (right) stands with his Cabinet Ministers and Supreme Staff at his mountain headquarters in Yugoslavia on May 14, 1944 (Imperial War Museum)

Challenges in Coalition Unconventional Warfare

The Allied Campaign in Yugoslavia, 1941–1945

By J. Darren Duke, Rex L. Phillips, and Christopher J. Conover

Lieutenant Colonel J. Darren Duke, USMC, is G2 for U.S. Marine Corps Forces Special Operations Command, Camp Lejeune. Major Rex L. Phillips, USA, is en route to a tour with Special Operations Command Central, MacDill Air Force Base. Major Christopher J. Conover, USAF, is en route to the Air Staff at the Pentagon and is currently serving as a Joint Branch Chief for the Joint Improvised Explosive Device Defeat Organization.

During World War II, operatives and military advisors of the British Special Operations Executive (SOE) and the American Office of Strategic Services (OSS), which was a precursor to both the current Central Intelligence Agency and U.S. Special Forces, conducted a challenging unconventional

warfare (UW) campaign against the Axis forces with and through guerrilla resistance elements in Yugoslavia. The resistance movement effectively fixed in place 35 German and Italian divisions, consisting of roughly 660,000 soldiers in the western Balkan region during 1941–1945.¹ This campaign rendered

them strategically irrelevant by preventing their use in other theaters. The combined United Kingdom (UK)–United States (U.S.) contingent achieved this effect with never more than 100 Allied personnel on the ground in the denied area. The number of Axis personnel killed in the Balkans is estimated at 450,000.² This extremely favorable force ratio and its associated effects commend UW as a low-cost, high-reward method of warfare.

Although ultimately successful, the campaign experienced difficulties. British and American policymakers, primarily President Franklin D. Roosevelt and Prime Minister Winston Churchill, chose with great risk near-term military goals over long-term postwar political strategic interests. Failures in operations security, differences in policy goals, difficulties in command relationships, and disparities in talent and skill among Allied personnel often strained the British-American relationship at multiple levels. Clandestine operatives on the ground inside Yugoslavia dealt with an increasingly vicious civil war among factions within the resistance movements that was rooted in longstanding political and ethnic differences. Contemporary policymakers and UW planners considering unconventional options can benefit from an examination of these challenges, experiences, and lessons learned from the Balkans Campaign of World War II.

Unconventional warfare is activities conducted to enable a resistance movement or insurgency to coerce, disrupt, or overthrow a government or occupying power by operating through or with an underground, auxiliary, or guerrilla force in a denied area.³ Special operations forces (SOF) conduct and support unconventional warfare. U.S. Army Special Forces, Green Berets, are the lead SOF Service component for its doctrine and conduct, while other Service components of U.S. Special Operations Command are tasked with conducting operations in support of UW efforts. Currently, no doctrine for joint or combined UW operations exists. However, history shows us that combined UW not only is possible, but also can be highly successful, even if fraught with

challenges. The combined UK-U.S. UW campaign in the former Yugoslavia offers several important lessons that should inform and help shape continued efforts to improve UW doctrine.

The Balkan Campaign

Formed out of the upheavals of the Balkan wars of the early 1900s and the fallout from World War I, Yugoslavia was a patchwork state cobbled together by treaty and riven by political and ethnic strife. In the spring of 1941, when Adolf Hitler realized that Yugoslavia's weak cohesion as a state would not allow him to keep it in the Tripartite Pact and to protect his southern flank in preparation for his invasion of Soviet Russia,⁴ he ordered the German-led blitzkrieg attack by Axis forces on April 6, 1941, which brought Yugoslavia into the war. Organized Yugoslavian military resistance rapidly evaporated, and the government capitulated after only 11 days. Armed guerrilla attacks on German and Italian units began in earnest by early July.⁵ These attacks—eventually recognized as the most successful guerrilla movement in occupied Europe—created sufficient concern within the German government that counter guerrilla operations were conducted to address the threat. These resulted in severe reprisals against Yugoslavian civilians as early as October 1941.⁶

Early in the war, Churchill expressed a desire to “set Europe ablaze.” When he learned of the resistance operations, he directed the SOE to assess the possibility of providing support to these groups to open up an additional front against the Axis regimes across Europe. The SOE and British secret service had access to an array of regional experts with language abilities and operational skills to provide this assessment. As early as 1939, the British government developed a well-established clandestine presence in Yugoslavia that remained active until the Axis invasion in April 1941.⁷ One of these former operatives, and an excellent example of the British talent, was Captain D.T. “Bill” Hudson.

Bill Hudson arrived in Yugoslavia in 1935 to manage an antimony mine. By

1938, he was fluent in Serbo-Croatian, joined the British secret service, and recruited a network of saboteurs in Croatia for operations against Axis shipping along the Dalmatian coast. Inserted into Yugoslavia by submarine on September 20, 1941, his mission was to determine whom the British government could trust and how it could help disrupt the Axis occupation forces.⁸

His initial findings were not encouraging; old ethnic animosities and new political differences deeply divided the two primary Yugoslavian resistance groups. A Serbian military officer named Dragoljub “Draža” Mihailovic led disparate elements of varying loyalty to the Yugoslavian monarchy-in-exile called Chetniks. Josip Broz Tito led a second group of communist resistance units known as the Partisans. These two groups fought each other in a fierce civil war. British intelligence and the SOE took 2 years to determine which side to back against the Axis powers.

By the summer of 1943, SOE field reports and signals intelligence⁹ convinced Churchill to suspend support to the Chetniks and to expand cooperation with and support of Tito and his Partisans. This decision was highly controversial and taken with a clear realization of the impact on the postwar political order in Europe. The suspension of support for the Chetniks meant the abandonment of a government previously recognized by the UK and a monarch related to British King George VI. Moreover, it meant the tacit recognition of a movement with unambiguous intentions of establishing a communist state in postwar Yugoslavia. No other country where the SOE and OSS facilitated resistance and guerrilla operations presented as severe a challenge in negotiating the deep divide between resistance factions or in weighing the risks of postwar interests in favor of near-term strategic ends.

In the United States, OSS Director Brigadier General William J. Donovan began to consider strategies in the Balkans designed to fracture the Tripartite Pact. Nevertheless, none of these efforts proved successful. With British facilitation, Donovan had visited

Belgrade in January of 1941 and communicated to both the Yugoslavian government and its armed forces that the United States was ready to support resistance to German aggression.¹⁰ This offer was rebuffed. In fact, during that very visit, a Yugoslavian delegation was putting the ink on an agreement to join the Axis Powers. In the end, all of these efforts came to naught in the wake of the Axis invasion later in April 1941.

The separate streams of Allied interest came together again during summer and fall of 1943 after the fall of Benito Mussolini. With Italy falling away from the Axis, the Allies now had an opportunity to exploit the Balkan situation to their advantage by convincing Hitler that the Allied push into Europe might come via the central Mediterranean coast. Donovan received approval from the Combined Chiefs of Staff to initiate unconventional warfare operations in Yugoslavia in September 1943. Simultaneously, Churchill authorized SOE to expand contacts with Tito and his Partisans and to assess their capabilities and requirements. The OSS provided operatives to this UK-led effort as well as attempting, albeit unsuccessfully, to conduct its own operations.

Command of the UW effort in the Balkans was given to Brigadier Fitzroy MacLean. MacLean had no previous military training prior to World War II but had served the British Foreign Office during the 1930s as a diplomat in the British embassy in Moscow. Through his experiences in the Soviet Union, which included reporting on the purges and show trials under Joseph Stalin and extended solo travel into the Caucasus and Central Asia, MacLean developed a keen understanding of the communist movement, Eastern European culture, and political-military affairs in general. Upon the outbreak of the war, he resigned his diplomatic position and eventually found his way into the newly organized British Special Air Service, conducting raids and long-range reconnaissance against German and Italian forces in North Africa and then establishing a UW network in Tehran as a hedge against possible Nazi domination of Iran. This



Sigfried Uiberreither, Martin Bormann, Adolf Hitler, and Otto Dietrich in Maribor, April 26, 1941 (Deutsches Bundesarchiv)

rare combination of experiences made MacLean the perfect man for the job.

Throughout 1944 and into mid-1945, the Allies established and operated numerous clandestine and expeditionary airfields, drop zones, and beach landing sites. Through these facilities, the SOE and OSS teams brought in tons of weapons, explosives, and ammunition directly to the subordinate Partisan formations. They provided training to Partisan units in demolitions, marksmanship, and tactics. Allied advisors accompanied Partisan forces on raids and sabotage missions against Axis lines of communication.¹¹ During all of these activities, they provided detailed intelligence reports of the situation in Yugoslavia and conducted combined planning with the Yugoslavians for future operations and—with less success—unilateral efforts to establish agent networks in Austria for future UW missions within the Third Reich's territory.¹²

National Tensions

The success in the Yugoslavian campaign was achieved in spite of forces and factors working against the Allied efforts. Allied pilots from America and Great Britain, Royal Navy ships, and submarines transported personnel and materiel with no regard for national origin or flag. OSS officers served as

advisors to Partisan formations under orders from MacLean with loyalty and focus even to the point of ignoring operational proposals from OSS headquarters that threatened to distract them from the goal of helping the Partisans defeat the Axis.¹³ It is a testament to the leadership of the U.S. and Allied governments, the SOE and OSS, and the professionalism of the majority of field operatives and officers that none of these elements rose above the level of irritant against the goal of Axis defeat. One of the most obvious sources of tension was the overwhelming disparity in the level of expertise in Balkan regional affairs, culture, and language possessed by the operatives on the ground. As noted above, the British possessed talented men such as Hudson and MacLean with deep regional and professional knowledge. To the contrary, the Americans lacked regional expertise and were almost solely dependent upon Yugoslavian or British translators to facilitate communications. This gap led to tensions between Allied personnel as British officers marginalized Americans by holding meetings in Serbo-Croatian—which the Americans could not speak—or forbidding uncorted American access to senior Yugoslavian leaders.¹⁴ The situation worsened



William J. Donovan, director of the Office of Strategic Services, 1942–1945 (U.S. Army)

over the course of time, particularly as UK and U.S. policy goals diverged toward the end of the war. The result was the eventual establishment of separate American and British missions just prior to the end of the war.¹⁵

A second source of national tension was the difference in organization and operational authorities adopted by the United States and UK. Fitzroy MacLean served not only as a military advisor and coordinator of Allied military support, but also as the direct emissary of the British government to Tito. He enjoyed direct access to Churchill and was personally consulted by the prime minister at major junctions in the decisionmaking

process. American OSS operatives were limited in authorities to military technical advice and assistance only. William Donovan may have enjoyed frequent access to President Roosevelt, but he was still required to submit his plans for approval by General George Marshall as well as the State Department for all of his global operations.

A third and final source of tension for considerations of combined UW was the inevitable competition between waxing and waning global powers. By 1943, with the U.S. war effort in full swing, America's rise to the status of global power was clearly under way. British prospects of preserving their empire, however,

were less assured. Yet it was the British who, by virtue of at least two centuries of colonialism and imperialism, amassed the experience and human capital for influencing global affairs. America was the new kid on the block and was learning many of the hard lessons in the laboratory of global war, to include how to play the games of politics, espionage, and coalition warfare.

Donovan realized that the OSS was dependent on the British secret service to provide training in tradecraft and expertise for clandestine operations. He also knew that national self-interest would necessitate the United States striking out on its own. He did this on several occasions, drawing sharp criticisms from his former British mentors for the unskilled way the OSS attempted operations. To be fair, while the British evinced an attitude of imperial superiority and possible ethnic and religious bias against the OSS and Donovan personally,¹⁶ the Americans gave them plenty of reason to complain. The OSS headquarters that oversaw the early stages of the Balkan Campaign in Istanbul was penetrated by the German intelligence agency, the Abwehr, making the British unwilling to share sensitive information on their operations. Donovan also invested more hope in the advertised abilities of the Chetniks because he lacked talented officers such as Hudson and MacLean to give him solid assessments of their intentions and capacity. The return on this investment by the end of the war was poor, and the United States wasted time in the erroneous belief that the ancient internecine hatreds of the Balkans could be healed by Allied efforts. Had the Americans possessed a MacLean-like figure, they might have saved themselves the effort.

The British-American competition manifested itself in disputes over communications as Americans had to send their OSS traffic over SOE nets using SOE codes, limiting their ability to communicate in OSS channels only.¹⁷ Donovan himself was also rejected by Churchill as a potential commander of the Yugoslavian effort, was refused entry into the Yugoslav theater on occasion,¹⁸ and lacked access to Yugoslavian leaders, as previously noted. By the end of the

war this competition developed to the point where, unbeknownst to British authorities, the OSS placed an agent in London who reported information on British government intentions toward Yugoslavia after the armistice.¹⁹ The special British-American relationship survived the war and far beyond, but it was clear that where the clandestine arts were concerned, “the cousins”—as Donovan liked to call them—had become an alliance of equals.

Strategic Choices and Risks

The thorniest of all the challenges facing the Allies in the conduct of the Yugoslavian campaign was the decision to support the Partisans. Tito was clearly a committed communist intent on establishing a postwar political order consistent with those beliefs. At the same time, he was a highly effective and tenacious guerrilla leader who attacked the Germans and their allies without hesitation. Whatever the decision, there would be second- and third-order consequences for Allied (particularly British) interests and for the future of the Yugoslavian peoples in the face of a communist revolutionary threat clearly intent on exploiting the political turmoil in liberated areas of Eastern Europe to its advantage.

Churchill’s final choice to suspend all support to Mihailovic and his Chetniks in favor of Tito and the Partisans was a conscious acceptance of risk to long-term interests of the democratic West in order to achieve a more rapid defeat of Nazi Germany. Although it is clear in historical hindsight that other factors may have mitigated this risk, such as MacLean’s excellent handling of relations with Tito, it must be remembered that at the time, there was at least one other course of action. An effort was proposed that sought to heal or at least ameliorate the Chetnik-Partisan rift by bringing the two groups under the Combined Allied Command. This course of action offered the possibility of avoiding any ceding of Yugoslavia to the Soviets after the war. Both of these options had their adherents among British and Americans alike and at multiple levels of command. The correctness

of the decision can be measured by the result: The Partisans effectively used the support provided by the Allies to achieve the most critical campaign objectives. Additionally, Churchill’s recognition and assistance of Tito’s government contributed to the moderation exhibited by Tito toward the West during the Cold War.

Lessons for Future Efforts

The challenges associated with combined UW operations during World War II in the former Yugoslavia present today’s UW policymakers, planners, and practitioners with several relevant lessons for consideration. The first is the importance of precrisis intelligence and intelligence-sharing. Intelligence is critical to the success of any endeavor, but the breadth and specificity of intelligence required to support UW operations are unique challenges because the disciplines used to collect intelligence for UW require a long time to bear fruit. Unlike general military intelligence related to conventional operations, the admixture of political and cultural factors creates the need for detailed intelligence long before the crisis erupts. When considering coalition partners, an imbalance in each side’s ability either to participate in or conduct independent intelligence operations can create tension similar to that seen between the United States and UK throughout the campaign. The British superiority in intelligence operations, both in their pool of talent and the way they put their talent far forward into the denied area, gave them an advantage that bred envy and distrust, however well it may have been suppressed by Donovan and others in the OSS. The Americans, on the other hand, had little understanding of the areas required to conduct UW and had limited means to collect the intelligence to educate them. The OSS analysts were also kept in the United States, severely hampering their ability to bring their expertise and understanding to bear on day-to-day operations or to effectively support policymakers.

Fortunately, the United States and UK were committed to sharing intelligence with each other so that both

governments were aware of developments achieved by the other. This sharing included sensitive sources and methods. The lesson here is that coalition members must develop ways to share the important information required for operational success promptly and in a way that builds confidence in the relationship. This level of sharing is built through commitment over time. The United States must develop mid- to long-term operational and intelligence assessments of likely areas of future operations long before crises arise and create intelligence networks and partnerships for effective intelligence-sharing in those potential areas of operation.

The second lesson for the future is the criticality of unity of command and the coordination of policy and plans. As the American subordination of OSS operatives to the SOE shows, the Allies were able to maintain an essentially unified command structure throughout the campaign until the very last stages of the war. The key to this success was the ability of both British and American leaders to suppress national and personal ambitions and to maintain the priority on the defeat of the Axis. All of this occurred under the steady and calm leadership of President Roosevelt, who recognized and ably measured the risks of pursuing unilateral American goals until the appropriate time. Consequently, he deferred to Churchill and the British as senior partners in the endeavor. Differing views were allowed and debate was encouraged, but serious threats to smooth operations were dealt with quickly by American leaders. Additionally, American leaders at the tactical level demonstrated the ability to avoid national agendas and diversions of time and effort on nonessential tasks. An excellent example of this focus is American Franklin Lindsay’s resistance to OSS proposals for propaganda operations in favor of supporting MacLean’s plan for facilitating Partisan lethal operations against the Nazis. The unity of command demonstrated by the Allies allowed for collegial planning that consequently allowed resources to flow efficiently to the decisive places on the battlefield.

The third lesson is the criticality of talent at the operational level for the

art of balancing strategic choices and risk. Churchill's decision to support the Partisans was confirmed by signal intercepts, but intelligence on Chetnik failures to act was only half the story. Without the reporting from men such as Hudson and MacLean, Churchill would not have known if there was any other resistance group worthy of support. Furthermore, the ability of those British SOE officers to provide useful insights on the military and security affairs within Yugoslavia was not developed at the Royal Military Academy at Sandhurst. In fact, none of these SOE officers had formal military training. On the American side, none of the operatives showed any indication of prior assessment and selection for this particular mission other than meeting the general OSS requirements. Many were sent because of their personal prewar ties to Donovan. OSS officers lacked education in strategy, and although a few possessed native language proficiency, they brought ethnic bias along with it,²⁰ thus limiting their usefulness in some aspects. In UW campaigns, the political, strategic, and tactical considerations of warfare all converge at a single focal point. Those serving in the denied area at that point in time and space not only require technical military knowledge but also must possess the understanding of cultural, political, and social dynamics driving the conflict. Whether by personal acquaintance, reputation, or professional development in a vetted process, these UW operatives must have the confidence of senior policymakers who rely on their reporting to inform good strategic decisions. The British SOE clearly possessed all of these traits, and the success of the campaign rested on the personal qualifications of these extraordinary individuals. This demonstrates the veracity of the "SOF truths" that people are more important than hardware and that competent special operations forces cannot be created after an emergency occurs.

Closely related to this principle is the final lesson: the strategic benefit of tactical karma. While the controversy over Churchill's decision to back the Partisans still lingers today and while many of Tito's postwar actions in establishing

and ruling communist Yugoslavia were inconsistent with previous promises, the rapport that SOE and OSS operatives established with their Partisan counterparts explains well Yugoslavia's relative openness to the West during the Cold War. Shared privation and danger with the Partisans cemented ties already developed through national commitments. MacLean demonstrated many of the same strengths in his dealings with Tito and maintained this rapport when the relationship suffered due to political differences. These SOE and OSS men persuaded the Allies to expand aid and support Partisan operations. Their efforts paid off not only in defeating the German forces in the Balkans but also in engendering goodwill toward the West that endured well into the Cold War era.

Conclusion

If the United States is sincere in its expressed desire for increasing the burden-sharing among our international partners in military and security operations around the globe, every operating domain and method of warfare must come to grips with the complexities and caveats of operating across national boundaries. Because of the unique way that national policy, strategy, and tactical concerns come together in UW operations, this method of warfare, perhaps more than any other, requires the development of new ways of sharing intelligence, defining operational authorities, forging effective command structures, and building rapport within the coalition and with the indigenous guerrilla forces, undergrounds, and auxiliaries. The means to this end will be people: men and women with the right combination of skills, experiences, and courage in the spirit of MacLean, Hudson, Donovan, and many others.

Finally, if the United States is successful in increasing the burden borne by our allies and friends in future conflicts, then it is reasonable to conclude that America will conduct UW operations within coalitions. Furthermore, in spite of modern Americans being more globally aware than the World War II generation, pervasive media and information technologies

will require the United States to partner with nations who can operate clandestinely in denied and politically sensitive areas. Under these conditions, the lessons from the past remain relevant. The record of these OSS and SOE allies presents a useful, accessible, and detailed case study for how combined UW operations can be done successfully and how to manage relationships among partner nations and mitigate strategic risks. The United States would be wise to invest more thought and study in order to successfully apply history's lessons. JFQ

Notes

¹ Nikola Kapetanovic, *Tito and the Partisans: What Really Happened in Yugoslavia from 1941 to 1945* (Belgrade: Jugoslovenska Knjiga, 1952), 45–46.

² Ibid.

³ Mark Grdovic, "Developing a Common Understanding of Unconventional Warfare," *Joint Force Quarterly* 57 (2nd Quarter 2010), 136–138.

⁴ Anthony Cave Brown, *The Last Hero* (New York: Times Books, 1982), 156.

⁵ Ilija Jukic, *The Fall of Yugoslavia* (New York: Harcourt, Brace, Jovanovich, 1974), 99.

⁶ Ibid., 99–100.

⁷ Walter R. Roberts, *Tito, Mihailovic and the Allies, 1941–1945* (Rahway, NJ: Rutgers University Press, 1973), 28.

⁸ M.R.D. Foot, "Obituary: Colonel D.T. Hudson," *The Independent*, November 14, 1995, available at <www.independent.co.uk/news/people/obituary-colonel-d-t-hudson-1581911.html>.

⁹ "Off the Page—Fitzroy Maclean," *STV*, December 16, 2010, accessed at <www.youtube.com/watch?v=j2bR6T2kIE>.

¹⁰ Brown, 156–157; Jukic, 45–46; and Jozo Tomasevich, *War and Revolution in Yugoslavia, 1941–1945: Occupation and Collaboration* (Stanford: Stanford University Press, 2001), 35–36.

¹¹ Franklin Lindsay, *Beacons in the Night* (Stanford: Stanford University Press, 1993), 76–87.

¹² Ibid., 149–165.

¹³ Ibid., 27.

¹⁴ Roberts, 142–143.

¹⁵ Brown, 453.

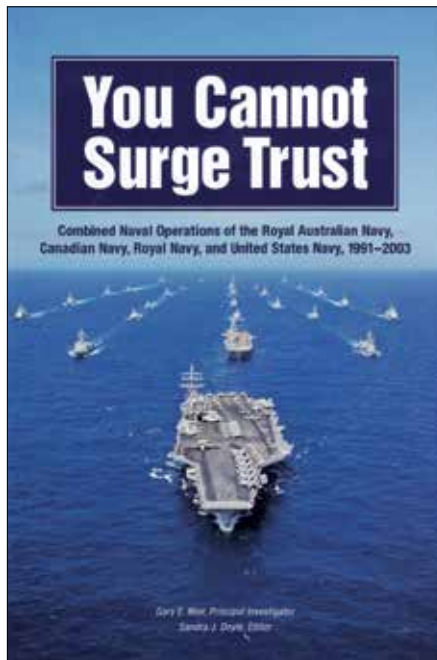
¹⁶ Ibid., 457.

¹⁷ Roberts, 142–143.

¹⁸ Brown, 456–457.

¹⁹ Ibid., 663.

²⁰ Lindsay, 12, 25.



**You Cannot Surge Trust:
Combined Naval Operations
of the Royal Australian Navy,
Canadian Navy, Royal Navy, and
United States Navy, 1991–2003**

Principal Investigator: Gary E. Wei
Editor: Sandra J. Doyle
Naval History and Heritage Command,
2013
345 pp. \$38
ISBN: 978-0945274704

Reviewed by Dov S. Zakheim

You *Cannot Surge Trust* is a valuable review of the unique relationships that bind the U.S. Navy and its British, Canadian, and Australian counterparts. Edited by Sandra Doyle of the Naval History and Heritage Command, the book is a collection of essays by naval historians from the United States, Australia, Canada, and United Kingdom (UK) that provide insights drawn from common experiences derived from combined peace support operations between 1991 and 2003. These insights offer useful pointers for the U.S. Navy leadership as it seeks to establish close cooperative arrangements with other navies around the world.

As all the essays make abundantly clear, two key factors lie at the heart of the U.S.-UK-Canada-Australia cooperative relationship. The first, so obvious it rarely is mentioned in the essays, is common language and heritage. Communication is far easier when the communicants speak the same language, share the same values, and, to a great extent, draw upon a common heritage. As an example of the latter, this author recalls that at a Pentagon meeting of British and American planners during the 1982 Falklands War, the senior U.S. Navy representative was a direct descendant of Captain John Strong, who claimed the islands for the British.

The second factor is a history of cooperation. The Anglo-American “special relationship” generally is dated from World War II, but it had its informal start in the previous world war. Thus, by the time the U.S. and Royal navies worked as a combined team to enforce sanctions against Iraq by conducting maritime interdiction operations in the aftermath of the 1991 Gulf War, they had nearly a century’s experience of cooperating with each other.

The U.S. Navy’s relationship with its Canadian and Australian counterparts dates to World War II as well. The U.S. and Canadian navies fought side by side in the Atlantic; the American and Australian navies did the same in the Pacific. In the case of American combined operations with both Canada and Australia, as indeed with their mother country, Britain, formal arrangements were supplemented by close personal and professional ties among the sailors in all four fleets.

Nevertheless, despite these ties, effective and successful combined operations among them have never been a foregone conclusion. Each of the case studies—the aforementioned maritime interdiction operations and those that followed during Operation *Iraqi Freedom*; Operation *Sharp Guard* off the coast of Yugoslavia during the Balkan Wars; Operation *Stabilise* in East Timor; and maritime operations in support of Operation *Enduring Freedom*—highlights the complications caused by politically driven

variations in national rules of engagement and by a lack of clarity regarding command relationships in ad hoc coalition operations. Either, and certainly both, of these factors could have prevented the four operations from achieving their goals.

What was remarkable, however, was the degree to which those constraints were overcome in operations that were joint as well as combined, involving air and/or land forces. As Sarandis Papadopoulos, author of four of the book’s chapters, writes in his introduction, “coalitions always have seams, especially in politically complex situations, but the trust built on common doctrine, shared training, and technically interoperable systems minimized any fraying of relations” (p. 14). Indeed, as all the authors point out to a greater or lesser extent, sailors from the four fleets often had to overcome shortfalls in interoperability as well, rendering their success that much more remarkable.

Papadopoulos’s observations are borne out throughout the volume, one of whose most valuable features is its presentation of the same operations from both American and allied vantage points. Thus, Stephen Prince and Kate Brett, of the UK Naval Staff, offer their perspectives on *Sharp Guard* alongside that of Papadopoulos’s recounting of the U.S. Navy’s role in that operation. David Stevens, of Australia’s Sea Power Centre, and Papadopoulos do the same in evaluating the performance of their respective maritime forces, notably including amphibious forces (pp. 130–131), in supporting land-based operations that ensured Indonesia’s withdrawal from East Timor. Two essays by Jeffrey Barlow, of the Naval History and Heritage Command, on the U.S. Navy’s role in coalition maritime operations in the Arabian Gulf from 1991–2001, and on its support for maritime interdiction operations in the first 2 years of Operation *Enduring Freedom*, complement that of Robert Caldwell, of the Directorate of History and Heritage at Canada’s National Defence Headquarters, who carries the story up to 2008.

Unlike the twinned chapters relating to the other operations, which follow

immediately upon each other, Barlow's review of Arabian Gulf operations, the first such essay in the book, is not collocated with his other chapter and that of Caldwell. Instead, it is followed by intervening chapters that address the other operations. As a consequence, the reader will not obtain as clear a sense of comparative Canadian and American perspectives as would have been the case if the three chapters appeared in succession. But this is a minor quibble.

All the essays provide the historical context for each operation and recount the challenges that had to be overcome in every case, not least of which was the fact that other allies also were involved in these efforts, and, like the four English speaking navies, were subject to their own national rules of engagement. In addition, every chapter bears out the critical and central role of the U.S. Navy, whose resources have long outstripped those of its allies. Even in those cases, like Operation *Stabilise*, where the Navy did not lead the operation, its role was crucial as a unique provider of intelligence and logistics support without which success could not have been achieved.

Summarizing the volume's main findings, Edward Marolda, formerly of the Naval History and Heritage Command, reprises and underscores its central thesis. His observation deserves to be quoted at length:

The key to the success of several post-Cold War multinational naval operations involving Australian, Canadian, British, and American navies was the trust, understanding, and mutual respect of leaders and commanders for one another in often challenging situations. Years of experience with combined . . . operations, at-sea exercises, shore-based education and training, and professional and social interaction had created a corps of allied naval officers confident in the abilities of their foreign counterparts. The human element was and is the key factor that binds the operations of [the four navies] (p. 279).

With the ongoing shrinkage of its force levels, which now comprise about half that of its order of battle in the

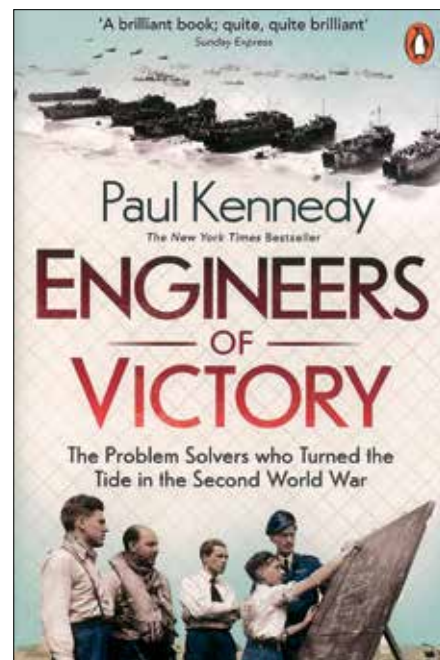
1980s, the U.S. Navy must work even more closely than before with allied and partner navies worldwide. It would do well to draw upon the lessons of its successful combined operations with its sister navies from Britain, Canada, and Australia, and apply them to others with whose countries America shares common interests. The fact that English is the international lingua franca for most partner navies creates opportunities for ever tighter and more fruitful operational relationships between them and the U.S. Navy.

The Navy already conducts numerous exercises with its partners across the globe. But exercises are not enough. The Navy should redouble its efforts to make its communications technology in particular available to more allies and partners. Even the three close partners highlighted in this volume have difficulty accessing technologies that would significantly enhance their ability to pursue combined naval operations with the United States.

In addition, and in line with the principle that "you cannot surge trust," the Navy should sponsor more professional and educational exchanges between its officers and their many counterparts. In a budget-constrained environment, such exchanges are tremendously cost-effective. Relatively speaking, they are low cost items. Yet they provide the foundation for creating the kinds of relationships that have enabled the navies of the United States, Britain, Canada, and Australia to work so closely and well together.

With the Navy likely to play an increasingly important role in a variety of operational contexts for the foreseeable future, its ability to work with a host of different partners will be critical to its success. *You Cannot Surge Trust* demonstrates how that success can be achieved. It should be required reading for all officers who aspire to lead combined maritime operations some time in their careers. JFQ

Dov S. Zakheim, Ph.D., is a Senior Fellow at the Center for Naval Analyses. He served as Under Secretary of Defense (Comptroller) from 2001 to 2004.



Engineers of Victory: The Problem Solvers Who Turned the Tide in the Second World War

By Paul Kennedy
Random House, 2013
436 pp. \$30.00
ISBN: 978-1846141126

Reviewed by Bryon Greenwald

Best-selling author and historian Paul Kennedy, the Dilworth Professor of History and Director of International Security Studies at Yale University, has written a stimulating book about the *middle*—the middle years of World War II, the middle or operational level of war, and the mid-dlemen, problem-solvers, and midlevel commanders that made victory possible. In doing so, he focuses attention on a largely unexplored portion of the war's history and provides professional historians and general readers a deeper understanding of how and why the Allies won World War II.

Much of the English-language history of World War II obscures or bypasses Kennedy's "middle." The war's numerous general histories gloss over how the Allies solved their thorny operational problems,

and the volumes recounting the war's great strategic decisions or detailing its tactical maneuvering far outnumber studies of organizational, technological, or operational innovation in the middle. Moreover, few such studies delve as extensively into this critical middle world filled with a multitude of organizations, weapons and technology, Service and joint doctrines, and theater planning efforts that connect the lofty endstates and big ideas of statesmen to the vital combat action on the ground, in the air, and on and under the sea.

Paul Kennedy examines that middle ground in an easy yet erudite manner and explains in five information-filled and engaging chapters how the Allies solved the five operational tasks essential to victory: crossing the Atlantic, winning command of the air, stopping the Blitzkrieg, seizing an enemy-held shore, and defeating the "tyranny of distance." Building on the excellent work of other historians, particularly the *Military Effectiveness* series by Allan R. Millett and Williamson Murray, Kennedy highlights who, what, where, when, why, and how the United States, United Kingdom, and Soviet Union achieved these tasks and defeated the Germans, Italians, and Japanese in a war fought on six of seven continents and most of the world's oceans.

The majority of the book focuses on the middle years of the war, approximately the 18 months from the Casablanca Conference in January 1943 to the launching of the first B-29 bombing mission from Tinian on the day after Thanksgiving (November 24) 1944. As such, Kennedy analyzes the Allied transition from losing to winning in every domain of warfare (land, sea, and air) and every major theater of war—the Atlantic, North Africa, Russia, Northwest Europe, and the Pacific. His emphasis on the operational level of war as well as the organizational and technological innovations required to tip the balance is refreshing and long overdue.

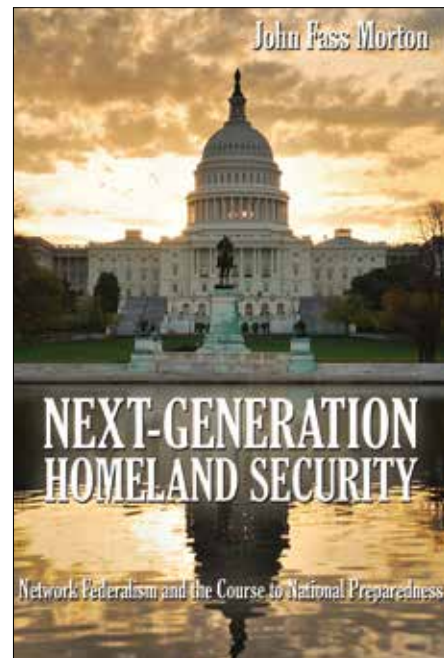
Kennedy is a master of deconstructing problems into their discrete elements and discussing in detail the decisions and actions that solved them. For such an easy read, the book is intellectually dense. (Indeed, his footnotes, commentary, and

bibliography are equally valuable.) One example should suffice to prove the norm.

Getting adequate quantities of fuel, weapons, munitions, troops, and food-stuffs to England was the first essential step toward the defeat of Germany. Appropriately, the book opens with a thorough discussion of how synergistic innovations in doctrine, technology, materiel, training, and leadership significantly reduced U-boat attacks on merchant shipping and won the Battle of the Atlantic. To put this struggle in perspective, U-boats sank 6.3 million of the 7.8 million tons of Allied merchant shipping lost in 1942, a total that virtually nullified the 7 million tons of shipping mass-produced in America that year. Left uncorrected, this strangulation meant that the Allies would never marshal sufficient supplies, weapons, and men in England to attack Germany and that the British people would most likely starve or freeze to death. Kennedy dissects this dilemma and deftly describes each problematic strand of this knotty challenge. He then adroitly details how the use of drop tanks, additional escort craft, and the development of miniaturized microwave radar and the deployment of Hedgehog antisubmarine munitions allowed the Allies to "find, fix, and finish" U-boats before most launched their deadly torpedoes. The rest of the book is equally compelling and illuminating.

Engineers of Victory is an important book that should encourage further study of World War II by all readers. Seventy-seven years after the war began (if one includes the 1937 Japanese attack into Manchuria), the *middle* remains a vast untapped area of historical inquiry. By necessity, Paul Kennedy only scratches the surface in explaining the key Allied operational-level questions of the war. In a fluid, well-researched, and insightful volume, he inspires us to ask and answer more questions about the problem-solvers, the "tweakers," and the "culture of innovation" that enabled the Allied victory. JFQ

Dr. Bryon Greenwald is a Professor in the Joint Advanced Warfighting School, Joint Forces Staff College, at the National Defense University.



Next-Generation Homeland Security: Network Federalism and the Course to National Preparedness

By John Fass Morton
 Naval Institute Press, 2012
 416 pp. \$36.95
 ISBN: 978-1612510880

Reviewed by Katie Kuhn

The threats to U.S. national security have evolved, but the means to respond to them lag far behind. After 9/11, Hurricane Katrina, and countless other natural and unnatural disasters, now is the time to rethink U.S. security strategy. John Fass Morton's *Next-Generation Homeland Security* could not be timelier in proposing an overhaul of the Cold War-era system. Policy change, he argues, will not be enough; we must change the structure of national security governance because the Cold War structures reflect only the strategic conditions that were relevant at that time. The United States can no longer rely on the forces that made it powerful in the second half of the 20th century, as the international system has changed, so too must our national security system. As

globalization has reshaped the meaning of sovereignty, nations are no longer the only important actors. In today's strategic environment, states play a co-equal role in policy development and strategy formation, and so they must also play a co-equal role in national security governance.

Morton's recommendations follow extensive, impressively thorough research on the evolution of emergency management and national preparedness. His inside perspective on the struggles to reform homeland security in the wake of 9/11 and Hurricane Katrina shows us the difficulties in making effective policy changes and the need for a change to the whole structure of our security system.

"This federal-centric homeland security system we have right now is a single point of failure," Morton tells Pennsylvania Governor Tom Ridge. We need a self-reliant citizenry to get away from this single point of failure. Currently, the Federal Government is responsible for national security yet owns neither the problem of homeland security threats nor the solution to them because the private sector owns critical security infrastructure. The structure and process of homeland security therefore needs buy-in from the Federal Government's "mission partners": nongovernmental organizations, the private sector, and state and local authorities. For local authorities to be effective, Federal authorities must respect what Morton calls a fundamental truth—that is, local government is the level most responsive to the will of American citizens. We have seen what happens when this truth is ignored: In the aftermath of the BP oil spill, for instance, crisis management efforts at the local level were undermined by Federal authorities, leading to frustrated efforts by the Okaloosa County Board of County Commissioners to contain the crisis. Morton suggests improving coordination through the application of network theory—taking insights on decentralization from the information technology world and applying them to management and organization.

The network that Morton proposes revolves around 10 regional nodes.

Regional, private-sector organizations on national security are not new; since the early 1990s, multicity and multistate associations have collaborated in large-scale disaster relief efforts. Such regional collaborations, though, must form the basis of the U.S. homeland security system rather than supplementing a national government-dominated system. Intergovernmental relationships should be not only vertical (Federal, state, and local) but also horizontal (interstate, interlocality). This setup means that top-down command models are not appropriate; the Incident Command System (ICS) is far more suitable for the management of incidents involving multiple jurisdictions and levels of government. The ICS blends hierarchical and network organizational models by serving as a temporary hierarchical authority that establishes a clear chain of command in a disaster to coordinate responses at each level of government. The ICS assigns section chiefs to five major functional areas: command, operations, planning, logistics, and finance/administration, with intelligence/investigation as the sixth functional area in the case of a terrorist event. Incidents are managed by a single Incident Commander (IC) if only one jurisdiction is involved, or by a Unified Command (UC) if multiple jurisdictions are affected. The IC or UC assumes the top position in a temporary hierarchy and determines strategies and resource allocations to respond to the incident, and the authority of the ICS recedes after the incident's resolution.

Morton recommends that a regionally based national preparedness system form through a "maturing-by-doing" process whereby homeland security professionals at each level work to resolve three problem areas: risk assessment; operational planning and exercise validation; and use of homeland security preparedness grants to target, develop, and sustain state and local capabilities. Though these three goals must be met at the local, state, and Federal levels, it is Federal regions that should play a central role in coordinating collaboration among states and localities. The Federal Government also has a central role in financing the national

preparedness system; that is, it holds the financial burden for providing states and localities adequate resources for national catastrophic planning and assessments.

Morton's plan is ambitious but sound. He does not claim that he or his book are the final authority on the design of a regionally based national preparedness system, but *Next-Generation Homeland Security* launches a debate that is long overdue: how to reform outdated Cold War-era structures into a security system that can meet the strategic challenges of today's world. The security of the American people and the political and economic stability of the international system are at stake, so this book is a must-read for anyone interested in homeland security. JFQ

Katie Kuhn recently completed her Ph.D. in Political Science from The George Washington University. She specializes in International Politics with a focus on Latin American Politics.

Sailors inspect catapult before launching F/A-18F Super Hornet from *Nimitz*-class aircraft carrier *USS Carl Vinson*, deployed supporting maritime security operations and theater security cooperation efforts in U.S. 5th Fleet area of responsibility (U.S. Navy/Travis K. Mendoza)



Implementing Joint Operational Access

From Concept to Joint Force Development

By Jon T. Thomas

Strategic guidance issued to the U.S. military over the past 5 years explicitly cites the emerging challenge to what has been a significant advantage for American and partner forces for decades: the unfettered ability to project military force into an operational area with sufficient freedom of action to accomplish a designated mission.¹ In some instances this ability includes access to sovereign territory,

but in all cases it requires access to the global commons.² Potential enemies are developing antiaccess/area-denial (A2/AD) capabilities³ that could threaten access and jeopardize missions. Concept development, as the bridging mechanism from strategic guidance to operational capabilities, has played a key role in the past few years to guide joint and Service force development activities in this area. The Joint Operational Access Concept (JOAC) and the recently signed Joint Concept for Entry Operations⁴ are examples of where strategic guidance to overcome A2/AD challenges is translated into operational

concepts intended to guide how the U.S. military is organized, trained, equipped, and employed.

Less visible perhaps but equally important are the processes whereby the ideas embodied in these concepts are transitioned into specific force development activities arrayed across the entire spectrum of doctrine, organization, training, materiel, leadership and education, personnel, facilities, and policy (DOTMLPE-P). These activities, actioned by Service, Joint Staff, and Defense agency sponsors and accomplished in a timeframe that accounts for the complexity of the task and the

Brigadier General Jon T. Thomas, USAF, is Deputy Director of the Joint Staff J7 Future Joint Force Development.

scope of the work required, are what institutionalize the change demanded by strategic guidance documents. In other words, concepts without accompanying implementation plans typically end up as nothing more than “books on a shelf.” Moreover, these force development activities always occur within a resource-constrained environment, which implies a need to prioritize efforts necessary to implement the concept.

Over the past year, the Joint Staff in conjunction with the Services, combatant commands (CCMDs), and key stakeholders in the Office of the Secretary of Defense (OSD) developed an implementation plan for Joint Operational Access (JOA) that prioritizes efforts and identifies specific actions to institutionalize the ideas in the JOAC. The Chairman of the Joint Chiefs of Staff signed the plan on August 29, 2014.

Why a JOA Implementation Plan?

The JOAC is the principal concept guiding U.S. military efforts to counter opponent A2/AD strategies. It describes how joint forces will achieve operational access in the face of armed opposition by potential enemies and under a variety of conditions as part of a broader national approach. Chairman of the Joint Chiefs of Staff General Martin Dempsey signed the JOAC on January 17, 2012. Less than 2 weeks prior in the Defense Strategic Guidance (DSG) issued by then-Secretary of Defense Leon Panetta, specific direction was provided to “implement the Joint Operational Access Concept.”⁵ Thus, development of a plan to implement the JOAC is simply following orders.

The need for a JOA Implementation Plan (JIP), however, runs deeper than simply the direction provided in the DSG. As mentioned, multiple strategic guidance documents explicitly identify the need to prepare for and overcome opponent A2/AD strategies, and the joint force started taking action immediately. In some cases, these actions are part of a large-scale effort (the multi-Service Air-Sea Battle [ASB] Concept and its associated implementation activities are

a good example), while in other cases Services, CCMDs, and agencies are focusing efforts on specific aspects of the A2/AD challenge. Missing from the overall effort is a mechanism to bring all of these actions together to foster coherence among all the ongoing activities across the joint force. First and foremost, enhancing coherence among operational access efforts is the practical outcome of developing an overarching JIP.

Notably, some valuable second-order effects are derived from conducting an effort to produce coherence. First, the visibility generated by documenting all operational access efforts within one overarching plan generates opportunities for synergy among ongoing (or planned) actions across the joint force. Interrelated activities can be accelerated or decelerated, or content added or subtracted, based on this added visibility. Second, having an overarching plan provides an opportunity to prioritize efforts and maximize the return on resources committed to the effort. Such a prioritization must be carefully supported with analysis and vetted with key stakeholders, but once produced can be a powerful tool to inform multiple DOTMLPF-P governance processes across the Department of Defense (DOD). Finally, pulling all of the various activities together related to JOA may result in new discovery that informs the way ahead.

Such new discovery could take three forms. First, in an organization as large as DOD, it is possible for *all* actors to assume that an activity, already recognized as necessary, is being accomplished by someone else, when in reality these assumptions have led to no single organization actually initiating the activity. Collectively, a key activity has somehow been overlooked and a new effort must be initiated to accomplish the necessary action. Second, after reviewing the volume of efforts within a given required capability area, a conclusion may be reached that the collective effort has missed something and a new effort should be initiated to address the newly discovered need. Third, documenting all activities related to a JOAC required capability may reveal that one or more stakeholders is performing similar actions

that could potentially be combined, or one activity curtailed, so as to facilitate economy of effort. In the development of the 2014 JIP, the first two examples of new discovery (recognized but overlooked necessary activities or specific missed actions) manifested themselves, but the third example (duplication) is likely to manifest in future updates to the plan.

What the 2014 JIP Does

At this point, it is worth explaining why the term *Joint Operational Access* is used rather than *Joint Operational Access Concept* implementation plan. While the 2014 plan focuses on the required capabilities in the JOAC⁶ as the organizing construct, future updates in 2015 and beyond are intended to incorporate additional required capabilities from supporting approved joint concepts.⁷ By orienting the implementation plan to the broader subject of JOA, there is room left for inclusion of other capabilities as joint concepts further mature.

The central elements of the 2014 JIP are a prioritization of the 30 required capabilities described in the JOAC and then a matrix of specific force development actions that, if completed, would significantly contribute to achieving the associated required capability. Because this prioritization is intended to inform multiple DOTMLPF-P governance processes across DOD, the 2014 JIP carefully describes the analytic process used to derive the prioritization of the JOAC required capabilities. This process leveraged multiple existing mechanisms such as the Comprehensive Joint Assessment (CJA); Chairman of the Joint Chiefs of Staff, Service chief, and combatant commander posture statements and congressional testimony; combatant command Integrated Priority Lists (IPLs); and the Capability Gap Assessment (CGA). Due to its central role in the overall DOD requirements process, the Joint Capabilities Board reviewed this portion of the 2014 JIP, and the prioritization of required capabilities was endorsed via a JROC memorandum.

With respect to specific force development actions, the 2014 JIP includes activities related only to the 10 highest



USS *Abraham Lincoln*, *Ticonderoga*-class guided-missile cruiser USS *Cape St. George*, and Military Sealift Command fleet replenishment oiler USNS *Guadalupe* conduct replenishment at sea (U.S. Navy/Travis K. Mendoza)

priority JOAC required capabilities due to the scope and magnitude of the task at hand in relation to the time available to develop the first iteration of the plan. The decision to address only those actions associated with these top 10 priorities should not be construed to mean that no efforts are currently under way or planned to address the remaining 20 JOAC required capabilities. Future updates in 2015 and beyond are planned to include a broader set of force development actions as additional required capabilities are addressed.

The 2014 JIP identifies 165 discrete DOTMLPF-P force development actions⁸ to be accomplished by specific sponsors within the Services, CCMDs, Joint Staff, combat support agencies, or OSD. This execution matrix describes the action to be taken, the output of that action, the sponsor (referred to as the office of primary responsibility [OPR]), other stakeholders with which the action must be coordinated, and the timeframe in which the action is to be completed

(an estimated completion date [ECD]). While some actions are to be completed within 1 year, many of these force development actions will not be completed for several years due to the magnitude of the effort. This level of detail within the execution matrix permits a key additional step—assessment of progress.

The assessment plan included in the 2014 JIP simply seeks to determine what progress was made in completing the actions described in the plan. Primarily consisting of self-reporting of progress by OPRs, the individual results of this annual assessment will be compiled and then used to inform the subsequent update to the JIP. In most cases, actions will be completed on schedule or remain on track when the ECD extends beyond the current year. In some cases, circumstances during execution may delay completion by the ECD. The assessment process will seek to determine the cause of the delay and how to respond to it. In either case, the 2014 assessment will inform adjustments to priorities and actions in the 2015 JIP.

Finally, the 2014 JIP includes a description of the process for communicating to audiences both internal and external to DOD as to why and how the plan was developed, how actions will be implemented, and how progress will be assessed. The purpose of this communication is to encourage collaboration among all stakeholders through improved understanding of joint force development activities related to operational access. While the JOAC itself is an unclassified and publicly available document, the 2014 JIP is classified due to the detailed manner in which it addresses capability shortfalls. As a result, distribution of the 2014 JIP will be limited consistent with established classification procedures.

Some unclassified metrics, however, can shed light on the content in the 2014 JIP execution matrix. First, of the 165 actions in the matrix, a majority (64 percent) consist of ongoing activities within DOD. This is understandable given that strategic guidance related to A2/AD challenges has been in place

for years, and the joint force has already begun many efforts to address the issue. Second, 84 percent of the 165 actions listed in the execution matrix are related to non-materiel activities. That is, the vast majority of actions in the 2014 JIP are not focused on building new things, but instead are focused on finding ways to better employ the materiel capabilities currently planned for the joint force, an approach consistent with the ideas in General Dempsey's assessment of the 2014 Quadrennial Defense Review.⁹ Third, the force development actions identified in the 2014 JIP are spread across the entire range of possible OPRs: approximately 50 percent across the military Services, about 25 percent for the Joint Staff, and the remaining 25 percent allocated across the CCMDs, OSD, and support agencies. So in addition to the volume of actions (165) associated with just 10 of the 30 JOAC required capabilities, this spread of OPRs is a clear indication of the significant scope of the force development effort required to address the A2/AD challenge to operational access. Together, these metrics highlight the broad, inclusive nature of the 2014 JIP, a pattern that can be expected to remain as the plan is updated in future annual cycles.

Relationship to Air-Sea Battle

While the JOAC is the principal concept guiding U.S. military efforts to counter opponent A2/AD strategies, the ASB Concept developed in May 2012 contributes to this effort as a multi-Service concept. ASB focuses on ensuring freedom of action in the global commons in order to enable concurrent or follow-on power projection operations.¹⁰ A complementary and supporting relationship exists between the ideas in ASB and those articulated in the JOAC. Because ASB represents a subset of the overall joint approach to ensuring operational access, the 2014 JIP includes many of the ongoing activities associated with implementation of ASB. As JOA implementation and ASB implementation processes mature, it is reasonable to expect further convergence of these efforts.

Way Ahead

The force development effort described in the 2014 JIP will take years to fully execute. This duration is a direct function of the scope and complexity of the overall joint force development effort. During 2014, execution of ongoing actions will continue and new activities will begin through the processes that govern DOTMLPF-P portfolios. Assessment of progress made on the actions documented in the 2014 JIP will occur and, combined with analysis derived from the fiscal year 2015 CJA, IPL, and CGA processes, will inform the development of the 2015 update. This method for annual updates to the JIP is intended to be responsive both to the amount of progress made in prior plans as well as to changes that inevitably occur in the evolving strategic environment. While the joint force may achieve a significant advance in operational access capability within a given year, it is more likely that major progress over the coming years will accrue as a result of sustained, focused effort guided by the JIP.

Summary

General Dempsey's approval of the 2014 Joint Operational Access Implementation Plan was a significant milestone in joint force development of required capabilities to maintain operational access in defense of the Nation and its partners. Developing a formal process to move the concept off the shelf and into formal action was new to the Joint Staff, Services, combatant commands, and the Office of the Secretary of Defense. With the 2014 JIP, there now exists a documented process and an initial set of actions to generate coherence and synergy of prioritized efforts across the joint force. Annual updates to this plan will broaden the effort and are likely to result in new discovery that uncovers additional opportunities to overcome A2/AD challenges. With key stakeholder commitment to this process, progress will be made to the endstate of a joint force capable of achieving operational access in the face of armed opposition

by potential enemies under a variety of conditions as part of a broader national approach. JFQ

Notes

¹ *National Security Strategy* (Washington, DC: The White House, May 2010); *The National Military Strategy of the United States 2011: Redefining America's Military Leadership* (Washington, DC: The Joint Chiefs of Staff, February 2011); *Sustaining U.S. Global Leadership: Priorities for 21st Century Defense* (Washington, DC: Department of Defense, January 2012).

² The term *global commons* is defined as "areas of air, sea, space and cyberspace that belong to no one state. Access to the global commons is vital to U.S. national interests, both as an end in itself and as a means of projecting military force into hostile territory." See Joint Operational Access Concept (JOAC), annex A (Glossary), 42.

³ *Antiaccess* (A2) refers to those capabilities, usually long range, designed to prevent an advancing enemy from entering an operational area. *Area denial* (AD) refers to those capabilities, usually of shorter range, designed not to keep the enemy out but to limit his freedom of action within the operational area. See JOAC, annex A (Glossary), 40.

⁴ Chairman of the Joint Chiefs of Staff General Martin E. Dempsey signed the Joint Concept for Entry Operations (JCEO) on April 7, 2014.

⁵ *Sustaining U.S. Global Leadership*, 5.

⁶ JOAC, 33–36.

⁷ JCEO is a prime example of where required capabilities from a subordinate concept will be addressed in the 2015 update.

⁸ In several instances, the 2014 Joint Operational Access Implementation Plan also identifies necessary "precursor actions" that are necessary to further refine and test ideas and approaches to force development before moving forward with actual adjustments in DOTMLPF-P elements. Examples of these precursor actions include additional concept development, wargaming, and technology demonstrations.

⁹ *Quadrennial Defense Review*, March 2014, 58–64.

¹⁰ "ASB [Air-Sea Battle] is a limited objective concept that describes what is necessary for the joint force to sufficiently shape A2/AD environments to enable concurrent or follow-on power projection operations. The ASB Concept seeks to ensure freedom of action in the global commons and is intended to assure allies and deter potential adversaries. ASB is a supporting concept to the Joint Operational Access Concept (JOAC), and provides a detailed view of specific technological and operational aspects of the overall A2/AD challenge in the global commons." See *Air-Sea Battle: Service Collaboration to Address Anti-Access & Area Denial Challenges* (Washington, DC: Air-Sea Battle Office, May 2013), 4.



Khas Kunar chief of police was charged with misuse of his position (1 year in prison) and logistics officer was charged with corruption (61 months and fine) during rare public trial at Kunar provincial courthouse (U.S. Air Force/Christopher Marasky)

Dealing with Corruption

Hard Lessons Learned in Afghanistan

By Richard J. Holdren, Stephen F. Nowak, and Fred J. Klinkenberger, Jr.

Corruption is the existential, strategic threat to Afghanistan.

—GENERAL JOHN R. ALLEN, USMC

Operation *Enduring Freedom* has exacted a tremendous cost on the United States in terms of both blood and treasure. By the end of fiscal year 2013, the financial toll

had reached \$645 billion. While we have made a significant investment in rebuilding Afghanistan, certain actors have seen our sacrifice as an opportunity to enrich themselves by stealing

money and materiel intended to aid in the rebuilding of the country.

A recent study has indicated that these corrupt actions threaten the future of Afghanistan. According to the Joint and Coalition Operational Analysis (JCOA) report titled *Operationalizing Counter/Anti-Corruption Study*, “Corruption alienates key elements of the population, discredits the government and security

Colonel Richard J. Holdren, USA, is Senior Analyst and Study Team Lead in the Joint and Coalition Operational Analysis (JCOA) Division of the Joint Staff J7 Future Joint Force Development. Stephen F. Nowak is an Analyst and Writer in JCOA. Fred J. Klinkenberger, Jr., is a Writer-Editor in JCOA.

forces, undermines international support, subverts state functions and rule of law, robs the state of revenue, and creates barriers to economic growth.”⁷¹ Corruption, in other words, undermines the very essence of those attributes required to establish and maintain a legitimate government.

There is no universal definition or criterion as to what encompasses corruption, with many describing it as, “You know it when you see it.”⁷² After years of struggling with the corruption problem in Afghanistan, the term has yet to be defined in joint doctrine. Part of the difficulty is that each culture defines behaviors and attitudes that it considers “normal,” and these vary greatly from one group to another. Acceptable behavior in one culture may be anathema to another, while merely boorish to another. In some cultures, paying a gratuity may be frowned upon, while in others it is seen as appropriate in certain situations. In the United States, for example, the wait staff in restaurants depends on tips for a majority of their wages. Taxi drivers expect to be tipped and are not afraid to explain tipping etiquette to passengers who fail to grasp the concept. On the other hand, attempting to offer a gratuity to a police officer or a judge is considered a corrupt practice.

Afghans, on the other hand, have become accustomed to paying additional fees, which they call *baksheesh*, for goods and services as a matter of routine. It is important to note that *baksheesh* is not a token of gratitude for a job well done, but a payment that is required before a service is rendered, even if the provider is already being paid to perform that service. According to the United Nations, Afghans pay \$3.9 billion per year in bribes and similar “gratuities.” Given that Afghanistan has a total gross national product of only \$14 billion per year, corruption consumes 28 percent of the Afghan economy; roughly half of Afghan citizens reported paying a bribe for a public service. Among the most outrageous examples of *baksheesh* are documented cases of wounded Afghan soldiers starving to death because military hospital staff refused to feed (or even

treat) patients until the appropriate gratuity was paid.³

Afghanistan is not unique in suffering from corruption. In its report published in 2013, Transparency International assessed 177 nation states, and 122 (69 percent) were identified as having a serious corruption problem. Of these, Afghanistan, North Korea, and Somalia were tied for last place as the three most corrupt.⁴

Why is corruption such an important issue? It is reasonable to expect that in future military engagements, we will continue to face the problem of corruption. Corrupt governments are often ineffective and unstable, making them likely candidates to fail and require intervention. We need to heed the costly lessons learned in Afghanistan to be better prepared to deal with corruption in the future.

A Brief History of Corruption during *Enduring Freedom*

To understand corruption in Afghanistan, we must understand the execution of Operation *Enduring Freedom* and the prosecution of the war. This contextual understanding may be helpful in making the lessons of the operation more readily adaptable to future situations.

In October 2001, the United States initiated *Enduring Freedom* after the Taliban government refused to hand over al Qaeda leaders implicated in the 9/11 attacks against the United States. U.S. Special Forces and Central Intelligence Agency (CIA) operatives allied with warlords from the Northern Alliance—a well-organized Afghan resistance group already fighting the Taliban—to engage the group as a proxy force. This phase of the strategy was successful, and the Taliban and al Qaeda were driven out of Afghanistan’s population centers.

Unfortunately, with the intense focus on defeating al Qaeda, little attention was paid to the pervasiveness and potential consequences of corruption in Afghanistan. The U.S. military’s support of and patronage to the Northern Alliance enabled the warlords to operate without constraint. With the void left by the absence of the Taliban, there was

no organized rule of law in the country. Unfettered by legal or other challenges, the warlords leveraged goods they had received legitimately from the United States as well as those acquired through criminal acts in order to amass political power.

When Afghanistan’s new constitution was signed in 2004, Hamid Karzai—through a series of political deals—was named the country’s interim president. The 25 ministries of the Government of the Islamic Republic of Afghanistan offered him a perfect opportunity to dispense patronage, and Karzai appointed various warlords to fill key government positions. Karzai also had the authority to appoint all governors and the mayors of key cities. While patronage allowed Karzai to consolidate his powerbase, his continued political security was dependent on the continued support of warlords. As one advisor explained, “He and his family started making deals with the various warlords in order to keep themselves in power, and [they have] certainly done so.”⁷⁵

Once established within ministries and other government posts, the warlords who had become government officials used their positions to divert resources to their constituencies to strengthen the reach and power of their networks. This convergence of power and money under the warlords’ control created what became known as criminal patronage networks, which offered a conduit through which both legal and illegal gains were blended so that the warlords now had the ability to conduct illegal activities under their own protection.

As the U.S. military presence grew, it faced a logistical challenge: “Afghanistan . . . is a landlocked country whose neighbors range from uneasy U.S. allies, such as Pakistan and Uzbekistan, to supposed adversaries, such as Iran. Thirty years of war have devastated what little infrastructure the country had.”⁷⁶ To ensure a steady flow of the materiel required to sustain its forces, the United States contracted with Afghan companies to provide secure long-haul trucking services. The result was that the “responsibility for the supply chain was almost

entirely outsourced to local truckers and Afghan private security providers.”⁷

These transportation and security contracts represented a significant investment—in 2010, the Department of Defense contracted \$2.16 billion for truck transportation. The contract went to eight companies as prime contractors, none of which were known for expertise in logistics (and in fact were suspect). In fact, “several of the prime contractors . . . [did] not own trucks and subcontract out all of their trucking needs. In other words, they essentially [served] as brokers to the local Afghan trucking companies.”⁸ Also, “one of the prime contractors . . . was founded by the son of the Afghan Defense Minister and had no direct experience with managing trucking before this contract.”⁹

The trucking companies were required to provide their own security, for which they relied on private militias that were largely controlled by the warlords. According to the JCOA report, the “private security companies . . . are typically warlords, strongmen, commanders, and militia leaders who compete with the [Afghan government] for power and authority. . . . The contractors have little choice but to use [the security companies] in what amounts to a vast protection racket.”¹⁰ Transportation and construction companies, as well as security escorts, pay the Taliban not to be attacked. In December 2009, then-Secretary of State Hillary Clinton acknowledged before the Senate Foreign Relations Committee that “one of the major sources of funding for the Taliban is the protection money.”¹¹

Funding to Afghanistan was provided primarily to support the Afghan Security Forces, but money was obligated for other purposes as well. One example was for the repair or construction of badly needed infrastructure. Local U.S. military commanders initiated projects, but were not able to see them to completion due to normal deployment cycles. As a result, many projects were planned and maybe even begun, but few were finished.

Meaningful measurement of progress during wartime is difficult because it is dependent upon objective, quantifiable data. One metric that was quantifiable

was the distribution of Commander’s Emergency Response Program (CERP) funds. One officer noted, “When [senior commanders] believed that putting cash in people’s hands was the way to win hearts and minds, they graded [lower-level] commanders on the number of CERP projects they could get obligated.”¹² As a former member of the Commission on Wartime Contracting explained, “They got a whole bunch of CERP projects; none of which were completed and most were barely under way when that commander rotated and the new commander came in. What’s [the new commander’s] incentive? To go fix all of the old CERP projects or do a bunch of his own.”¹³

The sheer amount of money for direct aid and contracted services flowing into Afghanistan overwhelmed its economy; there was so much American cash that it could not all be spent. According to the JCOA report, “An economy can only absorb a certain amount of inputs until it becomes saturated. Additional input goes somewhere else, usually capital flight, usually illicit. In Afghanistan, absorptive capacity [was] reached in the first year of operations. That led to the corruption eruption.”¹⁴

When the United States realized the severity of the situation, it sought to correct it but faced an insurmountable hurdle. It could not impose sanctions on the trucking companies or the security forces; the warlords had become so well entrenched that any imposed sanctions would have impeded U.S. logistics.¹⁵ To ensure U.S. forces continued to be supplied, the criminal activities of the warlords were largely ignored.

The problem, however, was not limited to activities controlled by the warlords. Financial aid from the United States and other coalition members was deposited directly into the Afghan treasury, and materiel, such as medical equipment and supplies, was turned over to the various Afghan ministries.¹⁶ At that point, the United States transferred all legal rights of the cash or materiel to the sovereign state of Afghanistan. It was the government’s to use or dispose of as it saw fit.¹⁷

There were no treaties or other enforceable agreements in place to control the money or materiel after transfer. When U.S. officials observed materiel being misused or stolen, they referred it to the Afghan government to resolve, but the usual response was that there was no problem to correct. When the Americans pressed Afghan officials to conduct an investigation, their response was that the United States was interfering with Afghan sovereignty.¹⁸

The Lessons

Over time it became obvious that even with massive U.S. financial investment, the expected results were not being achieved. The military hospital was not performing as planned. Fuel was being diverted before reaching its intended destination. Afghan officers were reportedly using military helicopters for questionable purposes. Ultimately, this led to various investigations and analyses, the results of which may prove as important for future operations as they did for resolving the problems experienced in Afghanistan.

In retrospect, it may seem that correcting corruption in Afghanistan was not a high priority. However, the priority for finding answers during armed conflict is to solve combat problems; defeating improvised explosive devices will win out over auditing funds given to a construction company every time. If there was limited capacity to address problems, protecting American troops always took precedence.

By 2010, Afghanistan’s corruption problem was being examined by the Special Inspector General for Afghanistan Reconstruction, whose report was critical of the U.S. provision of reconstruction assistance to Afghanistan “without the benefit of a comprehensive anticorruption strategy, and that U.S. anticorruption efforts had provided relatively little assistance to some key Afghan institutions.”¹⁹ To solve a problem, one must understand it, so in March 2013 General Joseph F. Dunford, Jr., USMC, commander of U.S. Forces, Afghanistan, requested, through the U.S. Central Command chain of command, “a study



Anti-corruption interview team from 101st Sustainment Brigade talk with local trucker about conditions on road (U.S. Army/Peter Mayes)

examining counter/anti-corruption (CAC) operational challenges and provide recommendations to inform planning, operations, and decision-making for the final stages of Operation [Enduring Freedom], the follow-on mission, and to capture best practices for future doctrine.”²⁰

The Joint Staff J7’s JCOA Division, in cooperation with the Joint Center for International Security Assistance Force Assistance, executed the task. After interviewing 66 key individuals and reviewing relevant material from over 500 literature sources, the study was completed and signed on February 28, 2014.

Among the report’s key findings are the following four points.

Allying with the Warlords and Overwhelming the Afghan Economy with Cash Fostered Corruption. The decision to ally with the Northern Alliance was driven by the military objective of defeating al Qaeda and the Taliban. Such

short-term alliances of convenience can lead to long-term problems. (In 2002, there was little expectation that military operations in Afghanistan would continue for so many years.) In the future, it would be prudent to anticipate that short-term operations are going to take far longer than initially expected.

Commanders must also be aware that there will be second- and third-order consequences of their decisions. Initially the Northern Alliance’s role as a proxy force was beneficial, but ultimately it became a powerful obstruction to U.S. interests. It is important to realize that military issues and goals do not exist in a vacuum. To analyze the composite of the conditions, circumstances, and influences that affect a commander’s decisions, we need to include political, military, economic, social, information, and infrastructure factors.

The civil war that followed the withdrawal of Soviet forces in 1989 left Afghanistan and its economy in shambles.

What little remained was absent a central government and central bank to support an economic system. Most of the modest infrastructure that had once existed had been destroyed. Outside of agriculture, there was little potential for legitimate development or employment. It would have been wise to consider these economic factors in the analysis of the operational environment. In Afghanistan, if we had been more aware of these issues, we may have had an earlier understanding of the overall influence of the warlords and the impact of corruption.

Corruption is a cultural, economic, and legal issue. To the joint force commander, however, the key consideration is how corruption will affect the desired endstate. In Afghanistan, a successful endstate was dependent upon the successful transfer of responsibility to a legitimate Afghan government—something that has not been the norm in the past century.

Actions performed in a foreign country need to be considered in the context of that country and not purely from the U.S. perspective. In 2002, the United States pumped \$20 billion into an economy that normally operates with less than \$15 billion dollars per year, which totally overwhelmed the Afghan economy. Nevertheless, the next year, we continued to pump in more. What were the consequences? How has it impacted Afghan businesses that need to transport their products by truck now that U.S. contracts have driven up the price? What has this done to the price of fuel or building materials? What will happen as coalition military forces (and the money spent to support them) leave? The CIA estimates that Afghanistan's economy grew 6.1 percent in 2011 and 12.5 percent in 2012, but the growth rate fell to 3.1 percent in 2013.

There Must Be Rule of Law to Combat Corruption, and There Must Be Processes and Mechanisms That Monitor Where Money Has Gone and What It Is Being Used For. There was no effective rule of law at the beginning of Operation *Enduring Freedom*. After the Soviet military left, the Taliban had enforced order through local courts, but after the Taliban's defeat, there was no national legal system until the Afghan constitution was ratified in January 2004. Without the rule of law, behaviors and actions may be influenced, but they cannot be directed. In addition, property rights are not defined and there is no prosecutorial power or punishment for infractions, no matter how outrageous they may seem.

How could the United States have better managed the money and materiel it supplied for the reconstruction of Afghanistan? Declaring martial law (to secure the disbursement) would have come at a tremendous political cost that could have encouraged a more unified insurgency. A more pragmatic approach would have been to disburse money and materiel with a clear understanding of expected outcomes, with future payments dependent upon prior performance.

Tracking money and materiel and measuring performance, however, require an appropriate monitoring and reporting

system, which was woefully lacking in Afghanistan. A simple paper-based system that host-nation personnel could understand and use would be far more effective than a sophisticated computerized system they do not understand. We should also leverage the expertise of Servicemembers experienced in law, supply management, finance, and contracting—granting them the commensurate authority to monitor and measure the effectiveness of our supporting funds and materiel.

Until There Was an Understanding of Afghan Corruption, There Was Little We Could Do to Correct It. Afghanistan's corruption is a complex issue. The unexpected consequences of early decisions—such as the empowered warlords being appointed to senior government positions—are caused by the failure to adequately understand the problem.

Every military officer who is expected to deploy has the potential to be operating in an environment that includes corruption. To effectively deal with corruption, an understanding of its causes and effects should become part of every officer's skill set. Professional military education should introduce the topic of corruption and other economic factors early and reinforce them throughout every officer's career. Including the significance of economic factors into exercises and wargames would be beneficial. While economics is not a traditional focus of military operations, like cyber, it may soon be a critical component of the battlespace.

All Parties Must Work Together toward a Common Goal. Economics is recognized as one of the elements of national power and is dependent on a whole-of-government approach. Unity of effort would benefit if the highest levels of government provided clear guidance as to the need to address corruption. As seen in Afghanistan, the potential damage caused by corruption is significant and demands effective action. Legislation to sanction corrupt nation-states would provide a powerful tool. The Leahy Law, which restricts support for nations that violate human rights, would be an appropriate model.

Working toward a common goal with government partners is a frequent theme

for the military. *The Capstone Concept for Joint Operations: Joint Force 2020* places the responsibility on the military to “identify those agencies with whom Joint Forces will work most often and develop common coordinating procedures.”²¹ Guidance such as this may provide a way to operationalize combined efforts toward a common goal.

Conclusion

Every generation of military leaders builds on the lessons of those who came before, and future leaders expect that their views of operating environments will be even more comprehensive. To the map and binoculars, we have added computers and reconnaissance aircraft. Now we need to add social and economic factors such as corruption. Operation *Enduring Freedom* taught us that corruption can have devastating effects. To effectively deal with it, we must incorporate a thorough understanding of corruption into our education, training, and exercises. We need to be open to other factors that we will identify in the future as having an impact on our effectiveness; however, we must remember that our decisions and actions have unintended consequences. The better we understand the operating environment, the faster we will identify problems that are more easily solved in their early stages.

Corruption is a problem that does not require a costly technological solution. Instead, it is one that requires an open mind with which to observe, analyze, adapt, and address the problem in a timely manner. JFQ

Notes

¹ Joint and Coalition Operational Analysis (JCOA), *Operationalizing Counter/Anti-Corruption Study (CAC)* (Suffolk, VA: JCOA, February 28, 2014), 1, available at <http://nust.edu.pk/INSTITUTIONS/Schools/NIPCONS/nipcons-institutions/CIPS/Download%20Section/JCOA%20CAC%20Final%20Report_U.pdf>.

² Ibid., 53.

³ Maria Abi Habib, “At Afghan Military Hospital, Graft and Deadly Neglect,” *The Wall Street Journal*, September 3, 2011.

⁴Transparency International, “Corruption Perceptions Index 2013,” *Transparency.org*, available at <www.transparency.org/cpi2013/results>.

⁵ CAC, 9.

⁶Sydney J. Freedberg, Jr., “Supplying the Surge in Afghanistan,” *National Journal*, February 20, 2010, available at <www.national-journal.com/magazine/supplying-the-surge-in-afghanistan-20100220>.

⁷ CAC, 10.

⁸“Warlord, Inc.: Extortion and Corruption Along the U.S. Supply Chain in Afghanistan,” Report of the Majority Staff, Rep. John F. Tierney, Chair, Subcommittee on National Security and Foreign Affairs, Committee on Oversight and Government Reform, U.S. House of Representatives, June 2010, 13, available at <www.cbsnews.com/htdocs/pdf/HNT_Report.pdf>.

⁹ Ibid., 12.

¹⁰ CAC, 11.

¹¹ “Warlord, Inc.,” 37.

¹² CAC, 13.

¹³ Ibid.

¹⁴ Ibid., 12.

¹⁵ Ibid., 11, 12.

¹⁶ “Dawood National Military Hospital, Afghanistan: What Happened and What Went Wrong?” Subcommittee on National Security, Homeland Defense and Foreign Operations, Committee on Oversight and Government Reform, U.S. House of Representatives, 112th Cong., 2nd Sess., Serial 112-164, September 12, 2012, 65, available at <www.gpo.gov/fdsys/pkg/CHRG-112hhrg76249/html/CHRG-112hhrg76249.htm>.

¹⁷ Ibid., 56.

¹⁸ Ibid.

¹⁹ Special Inspector General for Afghanistan Reconstruction (SIGAR), *Quarterly Report to the United States Congress* (Washington, DC: SIGAR, October 30, 2013), 43, available at <www.sigar.mil/pdf/quarterlyreports/2012-10-30qr.pdf>.

²⁰ CAC, v.

²¹ *The Capstone Concept for Joint Operations—Joint Force 2020* (Washington, DC: The Joint Staff, September 10, 2012), 9, available at <www.defenseinnovationmarketplace.mil/resources/JV2020_Capstone.pdf>.

Joint Publications (JPs) Under Revision (to be signed within 6 months)

JP 3-02, *Amphibious Operations*

JP 3-02.1, *Amphibious Embarkation and Debarkation*

JP 3-09.3, *Close Air Support*

JP 3-10, *Joint Security Operations in Theater*

JP 3-13.2, *Military Information Support Operations*

JP 3-26, *Counterterrorism*

JP 3-40, *Countering Weapons of Mass Destruction*

JP 3-52, *Joint Airspace Control*

JP 3-63, *Detainee Operations*

JPs Revised (signed within last 6 months)

JP 2-01.3, *Joint Intelligence Preparation of the Operational Environment* (May 21, 2014)

JP 3-07.2, *Antiterrorism* (March 14, 2014)

JP 3-29, *Foreign Humanitarian Assistance* (January 3, 2014)

JP 3-30, *Command and Control for Joint Air Operations* (February 10, 2014)

JP 3-31, *Command and Control for Joint Land Operations* (February 24, 2014)

JP 4-05, *Joint Mobilization Planning* (February 21, 2014)

JP 4-10, *Operational Contract Support* (July 16, 2014)

JP 3-05, *Special Operations* (July 16, 2014)



The Noncommissioned Officer and Petty Officer: Backbone of the Armed Forces

NDU Press, 2013 • 176 pp.

A first of its kind, this book—of, by, and for noncommissioned officers and petty officers—is a comprehensive explanation of enlisted leaders across the United States Armed Forces. It balances with the Services’ NCO/PO leadership manuals and complements *The Armed Forces Officer*, the latest edition of which was published by NDU Press in 2007. Written by a team of Active, Reserve, and retired enlisted leaders from the five Service branches, this book describes how NCOs/POs fit into an organization, centers them in the Profession of Arms, defines their dual roles of complementing the officer and enabling the force, and exposes their international engagement. As Chairman of the Joint Chiefs of Staff General Martin E. Dempsey writes in his foreword to the book, “We know noncommissioned officers and petty officers to have exceptional competence, professional character, and soldierly grit—they are exemplars of our Profession of Arms.”

Aspirational and fulfilling, this book helps prepare young men and women who strive to become NCOs/POs, re-inspires currently serving enlisted leaders, and stimulates reflection by those who no longer wear the uniform. It also gives those who have never served a comprehensive understanding of who these exceptional men and women are, and why they are known as the “Backbone of the Armed Forces.”

Have you checked out NDU Press online lately?



With 20,000 unique visitors each month, the NDU Press Web site is a great place to find information on new and upcoming articles, occasional papers, books, and other publications.

You can also find us on:



Facebook



Flickr



Twitter



Pinterest

Visit us online at: <http://ndupress.ndu.edu>

JFQ is available online at the Joint Electronic Library:
www.dtic.mil/doctrine/jfq/jfq.htm



JFQ

JOINT FORCE QUARTERLY

Published for the Chairman of the Joint Chiefs of Staff by National Defense University Press
National Defense University, Washington, DC

