

# JFQ

# Joint Force Quarterly

Issue 85, 2<sup>nd</sup> Quarter 2017



## New Technologies, New Strategies

An Interview with  
David L. Goldfein

Operational Graphics  
for Cyberspace



# Joint Force Quarterly

Founded in 1993 • Vol. 85, 2<sup>nd</sup> Quarter 2017  
<http://ndupress.ndu.edu>

**Gen Joseph F. Dunford, Jr., USMC, Publisher**  
**MajGen Frederick M. Padilla, USMC, 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

## Book Review Editor

Frank G. Hoffman, Ph.D.

## Associate Editor

Patricia Strait, Ph.D.

## Art Director

Marco Marchegiani, U.S. Government Printing Office

## Advisory Committee

COL Michael S. Bell, USA (Ret.), Ph.D./College of International Security Affairs; LTG Robert B. Brown, USA/U.S. Army Command and General Staff College; Brig Gen Christopher A. Coffelt, USAF/Air War College; Col Keil Gentry, USMC/Marine Corps War College; BGen 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; Brig Gen Darren E. Hartford, USAF/National War College; Col Brian E. Hastings, USAF/Air Command and Staff College; RADM P. Gardner Howe III/U.S. Naval War College; LTG William C. Mayville, Jr., USA/The Joint Staff; MG William E. Rapp, USA/U.S. Army War College; LtGen Thomas D. Waldhauser, USMC/The Joint Staff; RDML Brad Williamson/Joint Forces Staff College

## Editorial Board

Richard K. Betts/Columbia University; Stephen D. Chiabotti/School of Advanced Air and Space Studies; Eliot A. Cohen/The Johns Hopkins University; COL Joseph J. Collins, USA (Ret.)/National War College; Mark J. Conversino/Air War College; Thomas P. Ehrhard/Office of the Secretary of Defense; Aaron L. Friedberg/Princeton University; Bryon Greenwald/Joint Forces Staff College; 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. McNaughter/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): Member of Team USA during archery competition of 2016 Air Force Wounded Warrior Trials at Nellis Air Force Base, Nevada (U.S. Air Force/Kevin Tanenbaum); Bill Murray with Soldier from Presidio's 229<sup>th</sup> Military Intelligence Battalion during 3-M Celebrity Challenge charity event at Pebble Beach Golf Links, February 8, 2017 (U.S. Army/Steven Shepard); Squadron Sergeant Major of Marine Wing Communications Squadron 28 speaks with Marine during semi-annual Spartan Cup, at Marine Corps Air Station Cherry Point, North Carolina, January 20, 2017 (U.S. Marine Corps)



# In this Issue

## Dialogue

- 2 In Memoriam: General John W. Vessey, Jr., USA  
*By John Wagner*

## Forum

- 4 Executive Summary
- 6 An Interview with David L. Goldfein
- 16 Toward a Unified Metric of Kinetic and Nonkinetic Actions: Meaning Fields and the Arc of Effects  
*By Bradley DeWees, Terry C. Pierce, Ervin J. Rokke, and Anthony Tingle*
- 22 Information Warfare in an Information Age  
*By William R. Gery, SeYoung Lee, and Jacob Ninas*
- 30 The Rise of the Commercial Threat: Countering the Small Unmanned Aircraft System  
*By Anthony Tingle and David Tyree*

## Commentary

- 36 Forensic Vulnerability Analysis: Putting the "Art" into the Art of War  
*By Darryl Williams*
- 42 Operational Graphics for Cyberspace  
*By Erick D. McCroskey and Charles A. Mock*

## Features

- 50 The Need for a Joint Support Element in Noncombatant Evacuation Operations  
*By George K. Dixon*
- 58 Policing in America: How DOD Helped Undermine Posse Comitatus  
*By Steven C. Dowell, Jr.*
- 66 The U.S. Government's Approach to Health Security: Focus on Medical Campaign Activities  
*By George E. Katsos*



## About the Cover

Navy explosive ordnance disposal technicians assigned to Task Group 56.1 perform tactical personnel insertion rope suspension training, June 30, 2011, Manama, Bahrain (U.S. Navy/Peter D. Lawlor)

## Recall

- 76 The Advent of Jointness During the Gulf War: A 25-Year Retrospective  
*By Christopher G. Marquis, Denton Dye, and Ross S. Kinkead*

## Book Reviews

- 84 Mission Failure  
*Reviewed by Bruno Carvalho*
- 85 Margin of Victory  
*Reviewed by John Dethlefs*
- 87 The New Grand Strategy  
*Reviewed by Micheal D. Russ*

## Joint Doctrine

- 88 Improving Joint Doctrine for Security in Theater: Lessons from the Bastion-Leatherneck-Shorabak Attack  
*By Nicholas J. Petren*
- 94 Joint Publication 3-20, Security Cooperation: Adapting Enduring Lessons  
*By Keith D. Smith, Mark H. Lauber, and Matthew B. Robbins*
- 100 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.

### Copyright Notice

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

### 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 to ScholarOne, available at <https://mc04.manuscriptcentral.com/ndupress>, 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](mailto:JFQ1@ndu.edu)  
JFQ online: [www.dtic.mil/doctrine/jfq/jfq.htm](http://www.dtic.mil/doctrine/jfq/jfq.htm)

2<sup>nd</sup> Quarter, April 2017  
ISSN 1070-0692



Chief of the National Guard General Frank Grass meets with Retired General Jack Vessey, former Chairman of the Joint Chiefs of Staff, during visit to Camp Ripley, August 10, 2015 (DOD)

# In Memoriam

## General John W. Vessey, Jr., USA

By John Wagner

*Our strategy is one of preventing war by making it self-evident to our enemies  
that they're going to get their clocks cleaned if they start one.*

—GENERAL VESSEY

We mourn the passing and celebrate the life and service of General John W. Vessey, Jr., the longest serving U.S. Soldier, who died on August 18, 2016, at the age of 94. He began his 46-year service by enlisting in the Minnesota Army

National Guard when he was just 16. General Vessey rose to the rank of first sergeant in World War II and received a battlefield commission as a second lieutenant in 1944 during the Battle of Anzio while serving as an artillery forward observer.

A combat veteran of World War II and Vietnam, General Vessey eventually became the 10<sup>th</sup> Chairman of the Joint Chiefs of Staff, the Nation's most senior military officer, from 1982 until his retirement in 1985. He was a recipient of the Distinguished Service Cross, Defense Distinguished Service Medal, along with Army, Navy, and Air Force Distinguished Service medals, Legion of Merit, Bronze Star, and Purple Heart, among numerous other decorations.

---

Colonel John Wagner, USAF, is the U.S. Air Force Chair and Assistant Professor in the Dwight D. Eisenhower School for National Security and Resource Strategy at the National Defense University.

At General Vessey's retirement ceremony, President Ronald Reagan exclaimed:

*General Vessey will be remembered for many things: as a battlefield hero—you've heard today about North Africa, Monte Cassino, Anzio, and that grim night with the 2<sup>nd</sup> Battalion in Vietnam; he'll be remembered as a man of patriotism and deep religious belief, an officer who brought character and credit to every billet he ever held; as a military leader who always spoke his mind to civilian authority, respectfully but candidly; as the Chairman of the Joint Chiefs of Staff who presided over the restoration of America's military strength and power at a moment critical to the fate of freedom and his country's security. In all these things, he bore the marks of greatness.<sup>1</sup>*

The President then highlighted why General Vessey was such an inspirational leader throughout his career, and why he will remain a role model for any future leader in or out of the military: "There's one accomplishment that is not there in Jack Vessey's personnel file, yet it's an accomplishment that made the difference in the lives of so many GIs over so many years in so many places around the globe. Jack Vessey always remembered the soldiers in the ranks; he understood those soldiers are the backbone of any army. He noticed them, spoke to them, looked out for them. Jack Vessey never forgot what it was like to be an enlisted man, to be just a GI."<sup>2</sup>

General Vessey was the last Chairman who served before the Goldwater-Nichols Department of Defense Reorganization Act of 1986 transformed America's military organization and designated the Chairman as the principal military adviser to the President and Secretary of Defense. Thus, he was the last Chairman to have operational control of forces in the 1983 *Urgent Fury* operation that "rescued nearly 600 Americans and 120 foreigners, restored popular government to Grenada, and eliminated the potential strategic threat to U.S. lines of communication in the area."<sup>3</sup>

General Vessey also looked to the future—innovating, advocating, and activating two unified commands that would transform the American way of war and

be essential to the success of Operation *Desert Storm* less than a decade later. At the U.S. Central Command activation ceremony, he noted, "The Command is a signal to everyone concerned, friends and possible foes, that the United States has great interests in the region, that we stand ready to defend those interests and to help promote peace and stability in cooperation with our friends in the region."<sup>4</sup> Just over 2 years later, at the U.S. Space Command activation ceremony, he remarked, "The United States Armed Forces use space systems to preserve national security by performing such functions as communications, weather forecasting, navigation, and warning. This new command will improve the use of current systems and will enhance planning for future use of these systems in these areas."<sup>5</sup> The groundbreaking work begun in these two commands continues to improve our ability to fight and win the Nation's wars.

While he did not receive a college (bachelor's) degree until 1963 as a lieutenant colonel, General Vessey remained a continuous proponent of professional military education. He graduated from the Industrial College of the Armed Forces, predecessor to the Eisenhower School for National Security and Resource Strategy, in 1965. Eighteen years later, General Vessey urged, "I say to you that this new National Defense University must play a major role in keeping this a just nation justly armed. It must play its part in the preservation of peace. The quality of the education that the officers and civilian leaders get here will have a great deal to do with the defense decision-making in the years ahead."<sup>6</sup>

After retiring from the Army, President Reagan asked General Vessey to lead the efforts to account for military personnel listed as missing in action from the Vietnam War. As special emissary to Presidents Reagan, George H.W. Bush, and Bill Clinton, he made six trips to Vietnam to negotiate a number of issues with the Vietnamese government. General Vessey's efforts directly led to American search teams continuously on the ground in Vietnam and Cambodia since 1988 and Laos since 1991, along with occasional targeted investigations in China. To date,

these teams have identified and repatriated over a thousand Americans who were previously listed as prisoners of war or missing in action, returning them home for final closure with families and loved ones. For these efforts, President Bush awarded him the Presidential Medal of Freedom in 1992 as a "Soldier-Statesman who would not leave anyone behind."

As we reflect on the life and service of this national hero, I believe General Vessey would side with President Reagan if there was just one thing that he would want us to remember about him: His concern for the American soldier, the "GI," was legendary in combat during two wars and throughout the entire Cold War. In his final words as Chairman, General Vessey remarked, "It occurred to me that probably the best thing to do here this morning was to give my fellow citizens the same charge that Saint Paul gave to the Hebrew Christians when he said, 'Let us run with perseverance the race that has been set before us.' And then just simply say, 'Thanks. Thanks, troops.'"

Thank you, General Vessey. JFQ

---

## Notes

<sup>1</sup> Ronald Reagan, "Remarks at a Farewell Ceremony for General John W. Vessey, Jr., Chairman of the Joint Chiefs of Staff," September 30, 1985, available at <[www.presidency.ucsb.edu/ws/?pid=37816](http://www.presidency.ucsb.edu/ws/?pid=37816)>.

<sup>2</sup> Ibid.

<sup>3</sup> Ronald H. Cole, *Operation Urgent Fury: The Planning and Execution of Joint Operations in Grenada, 12 October–2 November 1983* (Washington, DC: Joint History Office, 1997), available at <[www.dtic.mil/doctrine/doctrine/history/urgfury.pdf](http://www.dtic.mil/doctrine/doctrine/history/urgfury.pdf)>.

<sup>4</sup> John W. Vessey, Jr., "Remarks at the U.S. Central Command Activation Ceremony," in *Selected Works of General John W. Vessey, Jr., USA, Tenth Chairman of the Joint Chiefs of Staff, 22 June 1982–30 September 1985* (Washington, DC: Joint History Office, 2008), available at <[www.dtic.mil/doctrine/doctrine/history/vessey\\_speeches.pdf](http://www.dtic.mil/doctrine/doctrine/history/vessey_speeches.pdf)>.

<sup>5</sup> John W. Vessey, Jr., "Remarks at the Activation of U.S. Space Command, Peterson Air Force Base, Colorado Springs, CO," in *Selected Works of General John W. Vessey, Jr.*

<sup>6</sup> John W. Vessey, Jr., "Address to the National Defense University Foundation, Fort McNair, Washington, DC," in *Selected Works of General John W. Vessey, Jr.*



General Norman H. Schwarzkopf, Commander, U.S. Central Command, consults with Chairman of the Joint Chiefs of Staff General Colin Powell regarding allied military coalition during Operation *Desert Shield*, July 18, 1990 (DOD/H.H. Deffner)

## Executive Summary

The old saying that history is written by the victors does not hold in all cases, but it still has a certain truth to it. Being able to know, with any certainty, what happened in the past is always a challenge, especially for the warrior scholars among us. As Editor in Chief, I have relied on the oral histories of those who have been involved over the years in producing *JFQ*. As you might expect, we have been fortunate to have many talented people at NDU Press with a common purpose of making General Colin Powell's vision for the journal a reality.

In a world filled with tweets, Facebook posts, and e-mail, receiving a handwritten letter has become a rare event. Even rarer for me would be to receive a letter from someone who was at

the beginning of *JFQ*'s history. Colonel Frederick "Fred" J. Kiley, USAF, Ph.D., was in my seat at the formation of the journal and worked with General Powell directly to launch it, primarily as a means of fostering jointness among the Services. While I knew this fact, I had never had contact with Fred until he wrote me to discuss the most recent *JFQ* he had read. After reading his letter, I can say that having one of the founding folks speak so well of the current effort was a great moment in my professional career.

Fred Kiley took General Powell's vision, found talented people who could make it happen, and then led them to a successful start some 85 issues (plus special editions) ago in 1993. Not bad for someone who was also responsible for hundreds if not thousands of Air Force

Academy cadets learning how to write well. (Fred holds a Ph.D. in English and served for over four decades "up on the Terrazzo.") In a follow-up phone call between us, he helped fill in many of the gaps in my understanding of how and why *JFQ* came to be. Most important was how he identified his leadership style in just a few minutes of conversation by immediately giving credit to the team he built. Fred began with Robert A. Silano, longtime managing editor, who took Powell's vision and drove it to execution with great success; he also credited Hans Binnendijk, then in his first tour as director of the Institute for National Strategic Studies here at the National Defense University, for "top cover" in keeping the resources in place in order to make the journal happen. Fred also credited the

skills of his staff, including two editors who were here when I arrived in 2010, Calvin Kelley and Martin “Jimmy” Peters, Jr. Just like the joint team they supported, *JFQ* has remained a unique and successful team effort. In talking about validation of effort from someone who should know what “right” looks like, you could not ask for better.

We continue in the path set down nearly 25 years ago by General Powell, Colonel Kiley, and his NDU-based *JFQ* team, and we look forward to giving joint issues “a thorough airing” for many years to come.

Our Forum section includes my interview with U.S. Air Force Chief of Staff, General David L. Goldfein. With a bit of pride, the general and I were squadron commanders together at the 31<sup>st</sup> Fighter Wing, Aviano Air Base, Italy, during the air war over Kosovo. I think you will be hard-pressed to find many senior officers who really understand the complexities of today’s joint operations in the way he does. Also, I think you can get a pretty good sense of how he is wrestling with a range of factors that must be addressed as he seeks to implement his vision for the Air Force as a part of the joint force. In a groundbreaking article, Bradley DeWees, Terry C. Pierce, Ervin J. Rokke, and Anthony Tingle describe how best to understand the results of kinetic and nonkinetic actions (think bullets and bombs versus cyber attacks) across all the domains that the joint force operates in and then use that understanding to improve the use of the force. The key lies in how we understand how war is fought in the 21<sup>st</sup> century. In another view of part of that key terrain, William R. Gery, SeYoung Lee, and Jacob Ninas add to our understanding of modern information warfare. In addition, the rapid expansion globally of drones or small unmanned aircraft systems available from commercial sources has driven Anthony Tingle and David Tyree to think about what kind of threat they might pose.

Commentary has two think pieces that invite us to consider saving a valuable but rapidly diminishing capability in one case and the need to add capability in the other. The ability to use forensics to



Chairman of the Joint Chiefs of Staff General Colin Powell speaks via satellite to Pentagon while visiting troops during Operation *Desert Shield* (DOD/Jeff Wright)

assess the vulnerabilities of our opponents might seem like an obvious requirement, and Darryl Williams argues this capability is fast becoming a lost art. Erick D. McCroskey and Charles A. Mock have developed an important, and so far, unachieved capability—how to graphically depict cyberspace operations.

In Features, we cover a range of issues associated with the dynamic security environment of the 21<sup>st</sup> century. George K. Dixon describes the requirement for a Joint Support Element as a part of our noncombatant evacuation operations, which seem to be happening with greater frequency. As local policing methods have become more militarized in recent years, Steven C. Dowell, Jr., takes a fresh look at the merging of military capabilities in law enforcement and the potential implications for the Posse Comitatus Act. As many readers will be familiar with our continuing discussion on health security, a frequent contributor to *JFQ* from the Joint Staff, George E. Katsos, discusses the U.S. Government’s focus on medical operations in joint campaigns.

Recall returns us to the first Gulf War, as Christopher G. Marquis, Denton Dye, and Ross S. Kinkead provide a historical review of the evolution of jointness since the victory won in Operation *Desert Storm* in 1991. In the Joint Doctrine

section, we have two important articles with insights from our recent conflicts. Nicholas J. Petren takes us to the attacks in 2012 on Camp Bastion-Leatherneck-Shorabak in Afghanistan, where he suggests improvements in how the joint force provides security for our forward deployed bases. Kevin D. Smith, Mark H. Lauber, and Matthew B. Robbins next give us a rundown on the updated Joint Publication 3-20, *Security Cooperation*. You will also find the Joint Doctrine Update and three valuable book reviews.

What do you see happening in the joint force today? Are we a better fighting force 30 years after Goldwater-Nichols? What do you see as the important issues today and going forward? Our *JFQ* audience wants to hear what you have to say. You have made *JFQ* “one of the most thoroughly read and influential journals” in the military profession, as General Powell had wanted. Only you can continue to let leadership know what you are thinking. *JFQ* is here to help you do just that. *JFQ*

WILLIAM T. ELIASON  
Editor in Chief



General David L. Goldfein is Chief of Staff of the U.S. Air Force (DOD)

that tends to be what is most on the radar for not only leaders in Washington, DC, but also the American people.

Let's first talk about what we do from a deployed-in-place standpoint. It starts with the nuclear enterprise. The Air Force is responsible, with the Navy, for two-thirds of the nuclear triad, and 75 percent of the nuclear command and control, which is the foundation of the nuclear enterprise. You can have great individual pieces and parts, but if it's not connected to the President, then it's not a nuclear enterprise. It's not safe, secure, or reliable.

You have to consider the 35,000 Airmen who are deployed-in-place in the nuclear enterprise, which overrides all military operations that we conduct around the world. You can't talk 4+1 without actually starting a dialogue in the nuclear missile fields and with the bomber force and the NC3 [nuclear command, control, and communications]; there is direct connection throughout. If a contingency begins anywhere on the globe, those forces are unavailable to go forward because they are doing their mission deployed-in-place. That's the first thing.

The second thing you need consider is what we do in space. With the exception of small pockets, the vast majority of the forces that conduct the business of space is deployed-in-place. Just like the nuclear enterprise, these forces are unavailable, with small exceptions, to go forward. They are going to be doing 4+1 at the same time we are doing all the things to defend the homeland and everything else that we do around the globe.

Space has become a contested place. Looking at how we fight in space should a war extend there is job one for the Air Force because we normalize the way we do warfighting, and we do warfighting by organizing, training, equipping, acquiring, and sending forward-ready forces to a combatant commander who then fights the fight.

We need to lead the debate on how we normalize space as a warfighting domain so that I provide those forces to combatant commanders; and whether they are geographic or functional commanders they then fight those forces and rely on

## An Interview with David L. Goldfein

*JFQ: What does today's Air Force bring to the joint fight that deals with what the Chairman of the Joint Chiefs of Staff has described as the "4+1" challenges: Russia, China, Iran, North Korea, and Islamic extremism?*

**General David Goldfein:** To see what the Air Force does for the Nation as part of the joint force, there are several lenses you should look through. I'd begin by looking at what we do from a deployed-in-place outlook and what we do to deploy forward. It's actually easier to describe what we do to deploy forward, and



what we bring from space, whether you want to talk about communications or precision navigation and timing, or all the other things we do to sense the globe as part of the ISR [intelligence, surveillance, and reconnaissance] enterprise.

You have to think about what the Air Force does for the Nation in the business of space operations. Then you have to transition to cyber. Like space and like nukes, the cyber force, with small exceptions, is not required to deploy forward and simultaneously defend the homeland, deter the nuclear threat, and be involved in 4+1.

You have to walk yourself through these mission sets, and I would add ISR to that, because the vast majority of the ISR enterprise actually does not deploy forward. The sensing piece does, but the reachback that it takes to do the analytical work every day and turn it into decision-quality information, that's an enterprise.

That's this whole part of the Air Force that can be viewed as under the waterline. It contributes directly to 4+1 and homeland defense—and it contributes to strategic deterrence. Then we start thinking about what we deploy forward. We'll start with global reach. We are truly a global power because of our global reach. You have to examine what that looks like and the requirement for us to deliver a certain number of million-ton miles per day across the globe as a validated joint requirement. Then we have to take a look at what we are doing in the business of conventional airpower forward. We could consider what we are doing in the Middle East, on the Korean Peninsula, or in Europe. We could also take a look at what we're doing in U.S. Southern Command.

Getting the decision speed faster than your adversaries and then having the operational agility to move forces where required to be able to produce dilemmas for the enemy that they could never match are paramount. If you take a look at that end to end, the reality is you are going to be hard-pressed to find a mission that the joint force performs that doesn't have an Airman present. Whether in space or in cyber or ISR or delivering airpower, we are always there.

*JFQ: On a more domestic front, you stated that one of your main focuses is to look at Air Force squadrons. I know you have written a book about this; I remember the day you talked about it as a fellow. Why is this still important to you?*

**General Goldfein:** My experience has been that the squadron is the level of command and the level of leadership in the structure of the Air Force where we succeed or fail as an organization. It is where the *command team*, which I define as the squadron commander, a senior [noncommissioned officer], is going to have the most influence on the culture of an organization. It is where we build readiness. If you buy that and if you believe that's the heartbeat of the Air Force, then it's worth putting a laser focus on it across the Service to ask how are we doing? How are we doing at first identifying the folks we believe have the potential for squadron command, and, once we have identified those individuals, what do we do about it? What do we do to prepare them? What tools are we arming them with? If in fact it's the most important level of command they will ever have, and that we will ever have as a Service in terms of what we contribute, what are we doing to prepare them for success?

Moreover, once these squadron commanders are in command, are we tossing them in the pool to see if they can swim as a test for the next level, or are we supporting them with everything we can to ensure that we are investing in their success? And are we holding them accountable for success, and the mission we have given them?

There is this code that you and I grew up with. The code is "leadership challenge." What that really means is I'm not going to give you all the money you need and I'm not going to give you all the people you need, but I expect you to get the job done. Some of that has been part of our history, and others have done this before us, so how do we ensure we are fully supporting these squadrons while they are in?

There is also a sizing piece to this. Right now, we have over 2,000 squadrons of different sizes, shapes, and

mission areas across the Air Force, and they go from 40-person organizations to 1,400-person organizations, and everything in between. Now start doing the math. Two thousand squadrons, 2,000 first sergeants, 2,000 superintendents, 2,000 DOs [directors of operations], 2,000 times 2,000 times 2,000—that's a lot of manpower.

But do we have these sized correctly? When we built the unit manning documents for these organizations, we didn't build them based on an expectation that 20 to 30 percent of the squadron would always be gone on continuous deployed operations. We built them based on the force we needed to do the job. If you go to a personnel recovery squadron, I suspect the commander will never have his squadron together, 4 months on, 4 months off, 4 months on, 4 months off.

*JFQ: What is your assessment of how the Air Force is doing?*

**General Goldfein:** I think we are like we have always been. We have squadron commanders out there who are absolutely crushing it. Here's what is interesting. As I travel around, I find there are four things that go into a successful command team. It's family, organizational culture, understanding the mission, and accomplishing the mission.

I can walk you into a missile squadron, and then I'll take you to a contracting squadron at Mountain Home [Air Force Base (AFB)], and then I'll take you to a space squadron at Schriever [AFB], and I can show you every different kind and flavor of squadron. Morale is high. They have taken on the culture of the organization. The common thread between those who are doing well and those not doing as well is the command team.

If a commander has taken on the responsibility for family and culture, then that squadron is going to be cooking. Now we have some institutional issues that we have to work, such as whether we are sized right, giving the needed tools, and supporting the commander.

At the same time, I'm hoping that one of the positive spinoffs will be a fresh



Airman with 1<sup>st</sup> Special Operations Aircraft Maintenance Squadron participates in Emerald Warrior 16 on May 3, 2016, at Hurlburt Field, Florida (U.S. Air Force/Jordan Castelan)

look at where decision authority resides. My gut tells me that as an unintentional consequence of downsizing and consolidating and moving people out of squadrons, decision authority started moving up. Now I've got people who are entrusted with the mission of the Air Force—whether we succeed or fail—but may not have the decision authority they need to accomplish their mission. We're taking a fresh look at that, too.

*JFQ: How have ongoing budget pressures affected how the Air Force operates today and its plans for the future, and what steps have you taken to mitigate these fiscal issues?*

**General Goldfein:** The biggest challenge that we face as Service chiefs is not having a stable budget environment to plan and build the best Service we can. We need a budget that allows us to have money in more than 1-year increments. We have experienced so many years of CRs

[continuing resolutions] followed by a 1-year budget, possibly 2.

What it does to a Service chief is you start building in unintentionally bad behaviors. We are never going to get money in the first quarter of any given year because, historically, we are going to get a CR every year, and then the force starts thinking about how it spends, and working a budget plan that we cram in at the last half of the year. We live on life support, and it becomes grossly inefficient. It's budget instability and the lack of being able to plan that is keeping us from getting into some programs that, quite frankly, would be really good for the Nation—the multiyear kind of programs that allow us to get the price points we need to deliver the best capability for the dollar.

What are we doing about it? I give General [Mark] Welsh [20<sup>th</sup> Chief of Staff of the Air Force] a lot of credit for this. He and his team spent 2 years building a strategic plan with the Air Force future

operating concept, and as part of that, he put in place a developmental planning process that helps us look further out to determine where it is that we need to look, where we need to be in 2030—what we need to think about regarding the global security environment. It's not a crystal ball, but planning. The value of planning is the *planning*.

The first ECCT [Enterprise Capability Collaboration Team] that we did on air superiority is already bearing fruit. In terms of now laying out a path—where we need to head in the business of air superiority as a core mission of the U.S. Air Force—the next step is going to be multidomain command and control.

*JFQ: Regarding the integration across multiple domains and components—and the Air Force's role as the connective tissue to make that happen—how do you view this role for the Air Force? Why is it so important?*

**General Goldfein:** It starts with the fact that it is one of our five core missions, going back to 1947. Command and control is something that we do for the joint force, as a member of the joint team. So, first and foremost, I don't look at this from a competitive lens; I look at this from an *obligation* lens. I think that we have an obligation. I marry that idea with my experience as the CFACC [Combined Forces Air Component Commander] forward, and one of the lessons learned in that experience was this: I went into the job thinking that I'd spend most of my time just making sure I had the right kind of air with the right attributes over the ground force commander, understand the ground force commander's scheme of maneuver and objectives, and just marry up and make sure we always had him covered.

We did that, but to be honest with you, that's not where I spent most of my time as a CFACC. I spent most of my time being the connective tissue for the combatant commander and doing regional command and control because there was no parallel to the CAOC [Combined Air Operations Center]. There was no parallel in any of the other components that brought the size of the various elements that I had on the floor and on the staff.

My BCD [Battlefield Coordination Detachment] was 60 soldiers. My SOF [special operations forces] element was rather robust. I had interagency coordination. Space and the Navy were our connective tissue to the maritime [operations] center. It was the place where it all came together, and where we actually accomplished multidomain, multimission, and regional command and control.

I looked at it through a lens to say that this is an obligation for the Air Force, and as I look toward the future of combat and conflict, I'm one who believes victories in combat—*planned* combat—are going to go to those who successfully can command their forces, make decisions, and move forces, and create dilemmas from all domains simultaneously if required, with resilience, so if I'm taken out in one domain, I can attack you in five others. It's going to be

that individual who can deny the enemy's ability to do that same thing. He is going to win.

Looking through an obligation lens is why I believe that we, from a joint perspective, have to think through what the future of multidomain is going to look like; it's not a place. Anybody who thinks about a "multidomain" as a bigger CAOC with more screens is completely missing the picture. It's CONOP [concept of operations], and that CONOP is about connecting a grid that senses the globe from six domains (I say six because I include the undersea as a domain).

When we think of the cyber domain, we should start thinking about social media because we sense in these domains, and then the question becomes how do we pull together all the sensing and turn it into decision-quality information? How do we take pre-effects from those same domains? It is sensing, effects, decision speed, and operational agility that are going to define the victors in future campaigns.

*JFQ: I sense from what you just said that your future vision is to disperse this as far down the command and control line as you possible. Is that your vision? Similar to mission command?*

**General Goldfein:** Yes. Here's how I look at it. We walk around and look at pictures of airplanes on a wall. The 20<sup>th</sup>-century approach would be to procure a weapon system to replace that weapon system so that I can expand the mission set and get to the next level of capability. By the way, eventually you have to figure out how to connect it to a network. That's the 20<sup>th</sup>-century approach. Here's the 21<sup>st</sup>-century approach: build the network, and then build your apps. Some of your apps fly, some of them drive, some of them walk. Some of them are in low Earth orbit. Some of them are in GEO [geostationary Earth orbit]. If you think about it in that mindset, it totally reverses where you focus.

Actually, it's the network that gives us the ability to have that asymmetric advantage, and then it allows us to start

thinking about procuring all the apps in a way that is different from what we have done in the past, which is focusing all energy on big programs, and lots of dollars.

*JFQ: You're stating that in the past there were more pieces to the puzzle. You are now starting with a view of what the puzzle was to begin with.*

**General Goldfein:** That's right.

*JFQ: To decide whether that fits or not.*

**General Goldfein:** Yes. When I talk about multidomain command and control, keep in mind that I'm looking at it from a network perspective. It's actually cultural. It's easy for an Airman to think about. An example I use when I talk about family of systems is your typical personnel recovery. What happens when someone is injured in enemy territory, a place where there is a contested environment? Think about all the steps that occur. This massive choreography that goes into place that is far beyond the HH-60. It goes from a radio call on a small handheld radio in the Hindu Kush. That call is bounced off an airborne layer amplified into satellites over protected or unprotected [communications] into a command control headquarters, often more than one. Then it is jumping into chatrooms, determining information, pulling up data on the individual, and determining what kind of help is needed.

While all that is happening, we are moving ISR overhead. We are cataloging where the enemy is. We're building the ingress routes, the HH-60, and the pararescuemen are getting their work. We have moved airborne battle manager over the top. We are doing the airborne C2. We have a C-CAT [Critical Care Air Transport Team] that's jumping onto a C-17. They are already launching. Think about that. Air, land, sea, space, cyber, all domains, multidomain, multimission, all coming together to save one life. This is actually natural for us.



B-52 Stratofortress during annual Cope North Exercise, February 22, 2011 (U.S. Air Force/Angelita M. Lawrence)

**JFQ:** *Let's discuss the retirement plans for the A-10 and how that relates to your perspective of how close air support will look in the future. Related to this is the F-35 and how you are trying to leave the A-10, at least to some extent, to be able to have personnel to support the F-35 mission. How do you see this playing out during your term?*

**General Goldfein:** First, I look forward to a time where I'm not having as many discussions about platforms, and I'm actually having far more meaningful discussions about mission, and how we accomplish that mission. We have evolved to the point where there is no silver bullet in any of the domains, so it's not the F-35, it's not the A-10, it's not this or that. It is how these things come together.

Here's the example I would use. As a CFACC, understanding the ground force commander's scheme and maneuver, terrain challenges, battle lines, and what he was trying to accomplish, we divided

Afghanistan into regional commands [RCs]: RC-East, RC-South, RC-West, RC-North. These commands had different terrains, different schemes and maneuver, and somewhat different objectives based on where the battle was at the time. Each ground force commander required coverage that brought different attributes. So, again, my job was to look at the family of systems and make sure that those attributes were overhead and that the ground force commander was covered.

In RC-East, there was mountainous terrain and generally the worst weather. That was a place where I needed to have something that could get into the valleys and provide the precision fires that were required, and when things went bad, they went bad in a hurry. I needed to have something that could get there quickly. So quite frankly, MQ-9s were a great asset to place there. RC-South was generally flat, with a lot of agriculture and a lot of challenges around Kandahar and

other areas. A-10s worked well when we had them at Kandahar. When I needed to get something in RC-North, I needed something that could get there and could stay there for a while. That's where B-1s tended to park. And then in RC-West, it was a different battle line. In the *same* mission, there were four different platforms, each that brought the attributes the ground force commander wanted.

**JFQ:** *Given the expansion of domains to include land, sea, air, space, and cyber, what is the Air Force doing to make sure it provides a total force capability across all these domains?*

**General Goldfein:** We already are engaged in all of them. It goes back to the "always there"—take a look at all the missions, whether deployed-in-place or deployed forward. You would be hard-pressed to find a mission that we're not engaged in. It's always a balancing act

against a finite number of resources. We must balance not only capability and capacity but also force readiness to ensure we are able to contribute to all those mission areas.

You mentioned total force. One of the great gifts of Mark Welsh is the fact that we are truly one Air Force with three components and five core missions. But how do we reinforce that we truly are *one* Air Force with three components? You can't tell us apart. Each component brings unique attributes. Whether we are looking at squadrons, or how we develop joint leaders in the future, or how we look at multidomain command and control and the network approach to warfare, we have to look through the lens of one total force. When we place talent in all mission areas, how do we get the most return on our investment? The story of the Air Force is this: As we have gotten smaller over the years and made a conscious decision to trade capacity and readiness for capability and modernization, there were mission areas that grew, some of them exponentially, such as ISR.

Space has become a more contested place. Cyber. Nukes. All these areas. The budget numbers are coming down and the missions are getting bigger, so how do we pay that bill? We pay through some of our key enabling support, infrastructure, people, and conventional airpower. The problem is that we have gotten to the point where we are far too big of an Air Force for the resources that we have been given, and far too small for what the Nation and the joint force requires. In between those two bookends lives risk on the backs of our Airmen. That's why you're hearing me coming out to talk about the fact that this Air Force needs to grow.

*JFQ: I would like to hear you talk about joint leadership and how that is built.*

*How do we step beyond the three-star level for jointness and leadership? How do we get an Airman to become a joint force commander?*

**General Goldfein:** I started off by telling you I think we do a pretty good job right now. Again, I'm not thinking we



Senior Airman of 932<sup>nd</sup> Aeromedical Evacuation Squadron participates in Exercise Global Medic 2011, a joint field training exercise for theater aeromedical evacuation system and ground medical components (DOD/Carolyn Erfe)

have to go fix things. The words that we chose in each of my focus series is important, strengthening joint leaders and teams. I'll give you four names, and you can use this list to describe how the Air Force is doing just fine: Lori Robinson, Paul Selva, John Hyten, and Darren McDew. I don't think we could find better leaders on the planet than those

four. The Air Force is not building joint leaders; they are evidence that we are building *great* joint leaders.

The question for me is how do we strengthen that? I believe the Airmen of the future are working to provide the voices in building a joint plan, so there ought to be an assumption that they understand the operational integration



Airmen assigned to 23<sup>rd</sup> Special Tactics Squadron at Hurlburt Field, Florida, use MH-47 Chinook to conduct overt and covert infiltration, exfiltration, air assault, resupply and sling-load operations in wide range of environmental conditions (U.S. Air Force/Christopher Callaway)

of air, space, and cyber. We're going to do a complete scrub that goes from entry level, for example, in the [Air Force] Academy, ROTC, or BMT [Basic Military Training], through the life cycles of Airmen to look at where they are and how are we exposing them to the operational art of air, space, and cyber. I'll be honest with you, the first time I truly had to understand space—not be a user of space, but understand space as an Airman—was being the Space Coordinating Authority as the CFACC. That was a little bit late. The first time I truly had to understand the operational art, operations in the cyber domain, was a little bit late. Where I want to focus on strengthening joint leaders in the Air Force is first and foremost that Airmen are exposed to the operational art earlier in their careers, earlier and more often.

The expectation ought to be that when we sit down at the table, we can speak air, space, and cyber with authority

and credibility because we understand it. That goes to career path progression. How long are we staying within stovepipes versus migrating across the air, space, and cyber domains and making sure we understand it? How much time do you have in a career to be able to get that kind of experience? We are going to look at all the curricula at the university, the Academy, and other places.

*JFQ: What have we not talked about that you would like to talk about?*

**General Goldfein:** Perhaps it would be helpful if I give you a little perspective on why I picked the three areas I focused on and how they tie together. There is actually a method behind the madness: When we connect the dots, and they actually equal joint warfighting excellence, that's where I intend to stay focused for my tenure as chief.

I only know one thing with absolute clarity, and I believe I only have one moral obligation as a chief. My moral obligation is that I ought never to allow an Airman to be sent forward to do a mission in harm's way without being properly organized, trained, and equipped. That's a moral obligation. The one area that I want to make sure that we stay focused on is our contribution as an air component as a member of the joint team for the joint force.

Then there are four elements to this. There is an organizational element, a leader development element, a CONOPS element, and a technological element. The three focus areas actually cover those four, so we have the organizational piece and the squadrons, leader development piece, as well as strengthening joint leaders and teams. CONOPS are associated with the ECCT. How do we take the sensing grid and combine it with the effects grid and pull it together in the way

we discussed? The technological aspect is really that whole piece of the network. How do we change the mindset on where we focus with future acquisitions?

*JFQ: How do you feel the Air Force is doing readiness-wise?*

**General Goldfein:** If you want to find high morale, go where we have high readiness. You want to go find low morale? Look where we have low readiness. The two are inextricably linked. We generate high readiness forward—pretty high morale on the Korean Peninsula and pretty high morale in the Middle East, relatively speaking. That’s where we generate and send supervisory capability, parts, readiness.

I will tell you that if pilots don’t fly, air traffic controllers don’t control, air battle managers don’t manage, maintainers don’t maintain—if we can’t affect their quality of service where they feel like they can be the most competitive they can be regarding career path and combat capability—then there is not enough money in the Treasury to keep them in the Air Force. When I look at all the things that build readiness and I look at where we are as an Air Force right now, my number one focus is people. If I’m going to generate the airpower the Nation requires and deserves, I have to have more people.

*JFQ: As we wrap up, one thing that may be useful to discuss is your take on “ready for what?”—not to overgeneralize readiness or lack of readiness across the force.*

**General Goldfein:** There are a lot of reasons readiness is complex. For instance, think about what I just talked about in terms of readiness of the force that deploys in place. How do we accurately describe the readiness of the space force, which is absolutely critical? How do we describe the readiness of the cyber force or the ISR force?

When I’m asked, what do you say to readiness, I think you have to rephrase the question: “ready for what and when?” If you were to ask, can you sustain that

ops [operations] tempo, and if the answer is, that is the steady state and it’s all I have to be ready for, then yes, I can. I will continue to pull from stateside units, and I will continue to have readiness in those units that are not next to deploy, but I can sustain that level of readiness.

But if you ask, are you prepared to simultaneously provide two-thirds of the strategic deterrence and most of the NC-3 [nuclear command, control, and communications], that is, do those things from a deployed-in-place that defend the homeland, contribute to the 4+1, continue the fight against extremism as the lead striking force in that operation, and take on any other contingency, I will tell you that we will be challenged.

*JFQ: You have to start making serious choices.*

**General Goldfein:** That’s right. That is why “ready for what and when” is such an important part of the dialogue, or you end up with a partial answer to a partial question.

*JFQ: Chief, thank you so very much for your time. This has really been a pleasure.*

**General Goldfein:** Thanks, yes, great seeing you. JFQ

## New from NDU Press

for the Center for the Study of Chinese Military Affairs

Strategic Forum 299  
*China’s Future SSBN Command and Control Structure*  
by David C. Logan



China is developing its first credible sea-based nuclear forces. This emergent nuclear ballistic missile submarine

(SSBN) force will pose unique challenges to a country that has favored tightly centralized control over its nuclear deterrent. The choices China makes about SSBN command and control will have important implications for strategic stability. China’s decisions about SSBN command and control will be mediated by operational, bureaucratic, and political considerations. A hybrid approach to command and control, with authority divided between the navy and the Rocket Force, would be most conducive to supporting strategic stability.



Visit the NDU Press Web site for more information on publications at [ndupress.ndu.edu](http://ndupress.ndu.edu)



Survival, evasion, resistance, and escape specialists wait before performing static line jumps as door of C-130 Hercules, assigned to Dobbins Air Reserve Base, Georgia, opens over Nevada Test and Training Range, Nevada, March 11, 2016 (U.S. Air Force/Kevin Tanenbaum)







USS *Toledo*, assigned to Commander, Task Force 54, transits through Arabian Gulf, January 21, 2016 (U.S. Navy/Torrey W. Lee)

# Toward a Unified Metric of Kinetic and Nonkinetic Actions

## Meaning Fields and the Arc of Effects

By Bradley DeWees, Terry C. Pierce, Ervin J. Rokke, and Anthony Tingle

---

Captain Bradley DeWees, USAF, is a Doctoral Student at Harvard University. Captain Terry C. Pierce, USN (Ret.), is the Director of the Center of Innovation at the U.S. Air Force Academy. Lieutenant General Ervin J. Rokke, USAF (Ret.), is Senior Scholar in the Center for Character and Leadership at the U.S. Air Force Academy. Lieutenant Colonel Anthony Tingle, USA, is the Concepts Evaluation Branch Chief at U.S. Army Space and Missile Defense Command.

There is a critical need for new thinking on how the United States can better meet the full spectrum of kinetic and nonkinetic 21<sup>st</sup>-century security challenges. Revolutionary changes in information technologies, communications, and the composition of both nation-state and nonstate actors necessitate a change in our approach toward national security. Though emerging cyber capabilities tend to dominate current defense dialogues, technological advances in the traditional domains of land, sea, air,

and space also demand a concept for holistically assessing the reality of our national security environment and the effects of actions we take toward those ends. In short, we need a unified cognitive approach for assessing and measuring kinetic and nonkinetic actions.

Recent work has suggested an incremental movement from our traditional focus on combined arms warfare toward combined effects power and has explicitly called for the crafting of desired effects by appropriate civil-military authorities at the tactical, operational, and strategic

levels.<sup>1</sup> This incremental shift in focus from traditional instruments of warfare toward desired effects opens the door for a more holistic consideration of the broad spectrum of security instruments, both kinetic and nonkinetic and across all domains. The challenge we face now is how best to assess and measure effects, particularly those of a subjective character such as the adversaries' morale, courage, willingness to fight, and views of their security environment.

In this article, we introduce two constructs: the *arc of effects*, which describes the continuum of national security actions, and *meaning fields*, which describe how our actions create different adversarial effects. Concurrently, we further develop the definition of *effects*. We believe that these concepts are the initial stages to developing a cognitive path for achieving holistic, unified measurements of kinetic and nonkinetic effects in all domains, including the increasingly important cyber domain.

## The Arc of Effects

Traditionally, our military has tended to measure effects in the natural domains (land, sea, air, and space) in terms of physical outcomes, with the focus on linear measurement of destruction caused by kinetic instruments of power. An emphasis on the physical domains has led us to neglect an important characteristic of warfare. Actions during conflict exist on a continuum, ranging from the purely physical to what Carl von Clausewitz termed "moral forces." These moral forces encompass more ephemeral factors such as motivation, will, spirit of sacrifice, patriotism, and courage.<sup>2</sup> We present a construct—the arc of effects—for better understanding and referencing physical and moral effects.

While the physical results of kinetic operations are relatively well understood and can be measured with some precision (even when considering second- and third-order effects),<sup>3</sup> effects toward the moral end of the arc are more difficult to measure because they require a degree of "military empathy," or the ability to consider the enemy's perspective. The

challenge of considering the enemy's perspective becomes exponentially more difficult when the existing environment is altered, for example, through the introduction of a new domain such as cyber, with substantial nonkinetic as well as kinetic potential.

Dissonance, such as that forced by a new domain, is common throughout military history. Just prior to the outbreak of World War I, Sir Arthur Conan Doyle wrote a fictional account of the defeat of Great Britain by unrestricted submarine warfare. At the time, it was farfetched to believe that Germany would use submarines to sink merchant vessels and to logistically isolate Britain. Because Doyle's ideas did not conform to the naval zeitgeist, they were summarily dismissed by the military establishment. Submarines were a radical and complex technology designed to function in a new domain of warfare, and surface navies were slow to understand the domain below the sea, ignoring its potential impact. Almost immediately at the onset of submarine warfare, countries became aware of the physical results (the loss of shipping) but were less timely in appreciating its potential effects on the moral forces end of the spectrum (uncertainty and terror).<sup>4</sup>

The submarine example is analogous to the rising contemporary challenge of nonkinetic effects. We are both reluctant and unable to define or fully understand the extent of these effects because we have traditionally emphasized the physical end of the arc of effects. This deficiency also limits our government's capacity for devising an effective deterrent to the full range of security threats and allows our opponents greater freedom of maneuver. In short, we need a tool for navigating the arc of effects that enables us to identify and assess the full spectrum of physical and moral forces.

## Meaning Fields

Clausewitz insisted that to be victorious, we must convince our enemies that they are defeated.<sup>5</sup> Victory requires that our adversaries perceive the totality of our actions that create an unacceptable environment. This perception, or

"meaning," that emerges on the part of the adversary is what we define as an "effect." When assessing or measuring such effects, a major challenge exists with the more subjective, moral side of the arc of effects. Unlike the physical effects of kinetic actions, which we can usually measure with some precision, moral effects are defined by the adversary and are thus more difficult to assess.

To meet this challenge, we offer a metaphor from the discipline of quantum physics, which we call meaning fields. The idea of "fields" is an elementary component of quantum physics. While early Newtonian physics focused on a body and the forces acting upon it, quantum physics explains the physical world as the result of particles moving through and being connected by fields (for example, electromagnetic fields or gravity), much like a blanket connecting individual patches of cloth. One ubiquitous field, the Higgs Field, is of particular significance because it imparts mass onto particles as they pass through it. The more substantial the particle, the more mass the Higgs Field imparts upon it. Because it imparts mass, the Higgs Field allows particles to join together, forming the foundation on which the rest of the universe is built.

We liken the Higgs Field to meaning fields, which we assert surround all actors in the international security arena, be they individuals, organizations, subnational groups, or nation-states.<sup>6</sup> A major difference, however, between our metaphorical fields and the Higgs Field is that there are many meaning fields, with every actor—from individuals to nation-states—possessing its own. Such meaning fields are a representation of how actors bestow meaning on actions of the external world and are constructed, inter alia, of human nature, culture, education, historical experiences, and circumstance. In the same way that the Higgs Field imparts mass to an object moving through it, meaning fields impart meaning on security-related actions or lack thereof.<sup>7</sup> Actions that do not intersect our adversaries' meaning fields (that is, that go unnoticed by the target actor)



Sailor assigned to USS *Mahan* talks to sonar technicians about attack options during anti-submarine warfare training in Arabian Sea, January 17, 2017 (U.S. Navy/Tim Comerford)

are imparted no meaning and are irrelevant. In short, the result of interaction with a meaning field is what we define as an *effect*.

We believe that the meaning field concept can provide a cognitive pathway to better understand the full spectrum of the arc of effects and is useful for military planners to assess how opponents impart meaning to external actions. The meaning field construct attracts the right kind of questions, including thoughts on which meaning fields are most relevant. Unlike measures of effects that focus primarily on attrition and destruction, the meaning field concept is more likely to accommodate effects on the moral side of the arc because it more explicitly addresses the Clausewitzian emphasis on how the enemy understands our actions. A second advantage of the meaning field construct is that it offers a means

for assessing the effect of inaction. It draws attention to how actors other than ourselves see the world, including the proposition that inaction can have just as much of an effect as action. Third, the construct provides a pathway for measuring follow-on (second-, third-, fourth-order) effects.<sup>8</sup>

Despite these advantages, the meaning field concept is also a humbling tool. It complicates the security picture by exponentially increasing the number of variables military policymakers must consider. It also makes apparent the uncomfortable reality that when we take actions to achieve desired effects, our own meaning fields are often irrelevant to our opponents.<sup>9</sup> Thus, to be effective managers of effects, our focus must be on our *opponent's* meaning fields. Without understanding an adversary's meaning field, the default instinct is to focus on

the less complicated metrics associated with the physical side of the arc of effects. While these kinetic effects can be measured with relative precision and circumvent the challenge of additional analysis, it is perilous for countries to neglect their adversaries' meaning fields.

### **Tactical- and Operational-Level Model Application: The Fall of Singapore**

One of the most devastating defeats in the history of the British military had its roots in the moral region of the arc of effects. On December 7, 1941, as the Japanese surprised the Americans at Pearl Harbor, they simultaneously attacked the British Empire on the islands of Singapore, leading to what would become a painful embarrassment and costly strategic setback for the British.<sup>10</sup> Although outnumbered



Sailor assigned to Blue crew of ballistic missile submarine USS *Maine* receives her submarine warfare officer device at Naval Base Kitsap-Bangor, Washington, December 5, 2012 (U.S. Navy/Ahron Arendes)

almost three-to-one, the Japanese were victorious against what was widely considered a vastly superior force in large measure because of their superior ability to assess and understand the meaning field of their British opponent.

The defenses on the main island of Singapore were considered a crowning achievement of the British Empire in the Far East. At the time, the fortress contained the largest fixed-position cannon in the world. These guns, like most of the defenses on the island, were initially positioned to defend from a southerly sea attack. The British discounted a Japanese attack from the Malaysian Peninsula, as any amphibious landing within proximity of the main island would be slowed by the dense jungle and could be interdicted by overwhelming land forces. The British meaning field assumed that strength was measured in the metric of total forces,

especially heavy forces, and that those forces were most effective in open terrain.

The Japanese upended the British meaning field. Led by General Tomouki Yamashita, the Japanese amphibious assault occurred near the northern border of Malaya, well outside the influence of British forces.<sup>11</sup> Aware of the advantages of blitzkrieg tactics, Yamashita focused on speed of maneuver. His relatively light forces blazed through the jungle, using bicycles, fixing partially destroyed bridges at night, and viciously giving no quarter, as prisoners slowed their advance. With the preponderance of the British air component being destroyed early in the assault, the Japanese were able to press across the peninsula relatively unimpeded, overrunning the British, taking valuable airfields, and reinforcing a cycle of rapid Japanese success.

The final Japanese victory over the main island of Singapore was as remarkable as their initial 600-mile march to capture Malaya in just 54 days. With a recklessly low ratio of attackers to defenders, and with supplies and morale running low on both sides, Yamashita pressed the assault. In a last-ditch effort to force British capitulation, Yamashita ordered a massive artillery shelling of the city (expending the last of his stores) to feign unlimited resources. Additionally, with a view toward the moral forces end of the arc of effects, Yamashita attacked the city's water supplies instead of the British-defended city proper. With dead bodies accumulating in the streets and facing the prospect of dying of thirst, the British surrendered.

Superior Japanese understanding of the British meaning field, as well as audacity and determination, led to the



Sea Hunter is part of DARPA's Anti-Submarine Warfare Continuous Trail Unmanned Vessel program, in conjunction with ONR (U.S. Navy/John F. Williams)

fall of Singapore. The Japanese asked not how to defeat the British forces, but how to sap the British will to fight. We argue that modeling meaning fields in the planning process could prompt our forces to ask the same questions. For the British, their failure could have been prevented by constructing a meaning field of the Japanese view of Malaya, a view that focused on more than the physical side of the arc of effects.

### Strategic-Level Model Application: Russia's Gray-Zone Warfare

While the example of Singapore represents a tactical and operational application of the meaning field construct, the model is also valuable in analyzing both kinetic and nonkinetic strategic-level effects. Russia's actions in Ukraine represent what is often referred to as "gray-zone" warfare, or the aggressive application of asymmetric and conventional techniques (including diplomatic, informational, military, economic, and other political forces) designed to achieve political goals

while maintaining hostilities below the threshold of conventional war. In this section, we examine the problem of Russia's gray-zone warfare in the context of both the arc of effects and meaning fields.

Russia's actions against Ukraine, often referred to as *hybrid* or *new-generation* warfare, encompass both the physical and moral components of the arc of effects. The physical forces component of Russia's strategy includes conventional strikes, train and equip operations, and Spetsnaz incursions, while nonkinetic elements include information warfare with distributed and focused cyberattacks.<sup>12</sup> When considering hybrid warfare strategies, we are forced to consider the entire arc of effects and the resulting synergies of simultaneously employing kinetic and nonkinetic means.

The underpinning concepts behind hybrid warfare are not new. At its core, hybrid warfare is simply a combination of asymmetric and regular warfare—the existence of which has been present throughout history.<sup>13</sup> So what is the basis for our current fervor over the dangers

of hybrid warfare and gray-zone conflict? Clearly the Russia-Ukraine conflict brings a change in the technological character of war. A lack of understanding nonkinetics and cyber operations prevents our senior policymakers from articulating actionable desired effects and deterring gray-zone type incursions.

Successful gray-zone operations rely heavily on ambiguity and the adversary's resulting inaction. In the absence of strict international policies and laws regarding hybrid warfare actions, aggressors operate with relative impunity.<sup>14</sup> While Ukraine is not a member of the North Atlantic Treaty Organization (NATO) and is not privy to protections under Article 5, Russia's invasion clearly violates international norms against annexation. Decisionmakers in gray-zone situations are often unable to articulate and uphold diplomatic "red lines." To counteract gray-zone warfare, the need to understand the adversaries' meaning fields becomes paramount.

So it is that the meaning field construct provides a cognitive path for dealing with security problems such as

hybrid warfare. Throughout this article we have portrayed our adversary's meaning field as at least as important as our own. Regarding Russia, it appears that Vladimir Putin's meaning field was not considered adequately when deciding to expand NATO. And now the West's inaction toward Russia's aggression into Ukraine is presenting itself as a particle through Putin's meaning field. By understanding our behavior in terms of meaning fields, we are better able to articulate our desired effects and produce viable counters to hybrid warfare actions.

In sum, the meaning field construct can focus our efforts to counter gray-zone conflicts. While the U.S. Government has the means to oppose these types of hybrid threats, economy of force and the threat of escalation are underlying concerns. Possible solutions to hybrid warfare include train and equip (proxy) operations, special operations forces, massive nonkinetic retaliation, and conventional strikes. Any combination of these options, including our own hybrid warfare, is a possibility.<sup>15</sup> By predicting our adversary's response to our actions using the meaning field theory, it is possible to achieve our desired effects through the most economical and politically palatable means available.

## Conclusion

The British strategy for the defense of Singapore reflected their own meaning field, which the Japanese correctly perceived was predicated on a traditional force-on-force strategy. However, this is not how the Japanese perceived the operational environment. They viewed the terrain, defenses, and the entire island system in terms of how it would affect the British will to fight. Similarly, the United States and our allies are slow to consider our actions in regard to Russia's meaning field.

We need to apply the meaning field concept across all domains. The growth of cyber is just one example of a technological advance that spans the physical and moral side of the arc of effects. The risk we run with this technological advance is forcing it into the physical side of the arc of effects. We make this

mistake because it is convenient to think in terms of physical forces rather than in terms of how the enemy sees the world.

The meaning field concept provides a cognitive path for moving our focus toward the mind of possible adversaries in the interconnected world of national security. The notion that military leaders should focus on the mind of the enemy is not new; it was the basis of Sun Tzu's *Art of War*. But more than two millennia after Sun Tzu, we still lack a means to effectively incorporate his advice directly to measuring effects. We continue to define effects based largely on our own intuition rather than in terms of how the enemy sees the world. We see the meaning fields concept as a helpful point of reference in the doctrinal process for reorienting military leaders to the mind of the enemy.

If we seek to defeat our adversaries, we must first perceive their meaning fields. Doing so would increase the probability that we will think like the enemy (minimizing the "mirror imaging" problem) and a greater probability of achieving desired effects. Moreover, this concept allows us to consider multiple, increasingly complex and interconnected adversaries who strive to operate beyond the second and third orders of effects. By understanding meaning fields, we access the entire span of the arc of effects, creating a definition of "effects" that unites all possible domains of warfare. JFQ

## Notes

<sup>1</sup> See Ervin J. Rokke, Thomas A. Drohan, and Terry C. Pierce, "Combined Effects Power," *Joint Force Quarterly* 73 (2<sup>nd</sup> Quarter 2014); and James G. Stavridis, Ervin J. Rokke, and Terry C. Pierce, "Crafting and Managing Effects: The Evolution of the Profession of Arms," *Joint Force Quarterly* 81 (2<sup>nd</sup> Quarter 2016).

<sup>2</sup> Carl von Clausewitz, *On War*, ed. and trans. Michael Howard and Peter Paret (Princeton: Princeton University Press, 1989), 97.

<sup>3</sup> When focusing only on physical results, the follow-on effects are relatively simpler to discern than nonkinetic (moral forces) results.

<sup>4</sup> According to Michael L. Hadley in *Count Not the Dead: The Popular Image of the German Submarine* (Montreal: McGill-Queen's University Press, 1995), 14: "The submarines had done so by isolating the vital centre of the Brit-

ish Empire through direct attacks that entirely evaded the might of the British surface fleet."

<sup>5</sup> Clausewitz.

<sup>6</sup> The authors credit Lieutenant Colonel Mario Serna, USAF, for his assistance in translating the Higgs Field metaphor into the meaning field. Also see Sean Carroll, California Institute of Technology, "The Higgs Boson and Beyond," The Great Courses, 2015.

<sup>7</sup> Meaning fields can also impart meaning upon inaction. For inaction to be considered significant vis-à-vis meaning fields, we must consider two factors: expectation of action and time. An adversary must expect some action (which is never taken), and the appropriate amount of time must pass. An example of significant inaction in this context is the relative U.S. inaction in the face of Syria's use of chemical weapons in 2013, and the meaning that the Bashar al-Asad regime imparted to this inaction.

<sup>8</sup> For every action, there are consequent actions and effects. Each initial action passes through all meaning fields, producing effects. Each one of these effects then passes through all meaning fields, producing another effect (a second-order effect). This cycle is repeated, with each order effect being influenced by the relevant meaning fields. If the military planner is cognizant that all actors have unique meaning fields, then once the initial meaning field is considered, it becomes easier to accurately comprehend and possibly predict second-, third-, fourth-, and fifth-order effects. This visualization is the first step in understanding ordered effects of our actions.

<sup>9</sup> When considering the desired effects of our actions, the opponent's perception of our meaning field is often irrelevant. Simply put, our adversaries are often equally negligent when considering meaning fields.

<sup>10</sup> Due to the International Date Line disparity, this was the date of the event in the United States. The actual date in Singapore was December 8, 1941. The Japanese initially attacked the islands by air.

<sup>11</sup> These forces constituted a coalition from across the British Empire, including British, Australian, and Indian troops.

<sup>12</sup> Patrick Duggan, "Strategic Development of Special Warfare in Cyberspace," *Joint Force Quarterly* 79 (4<sup>th</sup> Quarter 2015).

<sup>13</sup> For a historical perspective on the existence of hybrid wars, see Frank G. Hoffman, "Hybrid Warfare and Challenges," *Joint Force Quarterly* 52 (1<sup>st</sup> Quarter 2009).

<sup>14</sup> See U.S. Special Operations Command, "The Gray Zone," September 9, 2015.

<sup>15</sup> Joseph Votel et al. suggest that the most effective counter to hybrid warfare is hybrid warfare. See Joseph Votel et al., "Unconventional Warfare in the Gray Zone," *Joint Force Quarterly* 80 (1<sup>st</sup> Quarter 2016).



As part of Internet of Things display, booth of Deutsche Telekom at CeBit 2015 shows moving arms of robots holding magenta umbrellas, March 16, 2015 (Courtesy Mummelgrummel)

# Information Warfare in an Information Age

By William R. Gery, SeYoung Lee, and Jacob Ninan

In the past week, how many devices have you used that were connected to the Internet or relied on an algorithm to accomplish a task? Likely, the

number is upward of 10 to 15, and most of those devices are used daily, if not hourly. Examples may include a Fit-Bit, cell phone, personal computer,

work computer, home monitoring system, car, Internet television, printer, scanner, maps, and, if you are really tech savvy, maybe your coffee pot or refrigerator.

The Internet of Things (IoT) is bound by a mesh network that is increasingly connected to every part of our lives, and those devices are becoming increasingly reliant on each other to perform their functions.<sup>1</sup> Computing devices, using advanced algorithms, are entering the machine-learning phase, a subset of computer science in which the computer is “learning” about the environment and presenting predictions based on available data and conditions.<sup>2</sup> Trends include machine-autonomy and self-learning. The idea of interconnectivity is not only about the IoT but also the information that

---

Major William R. Gery, USAF, is Program Manager for the U.S. Air Force Weapon System Evaluation Program at Air Combat Command. Major SeYoung Lee, Republic of Korea (ROK) Army, is a Student in the Military History Institution of ROK Army Headquarters. Lieutenant Colonel Jacob Ninan, USA, is a Branch Chief in the 704<sup>th</sup> Military Intelligence Brigade.



transits the Internet, and how it influences our daily decisions. The trend toward a worldwide mesh-network is nearing, and with the creation of an information technology (IT)-based domain comes increased understanding of the environment in which we live. There appears to be no deviation from Moore's law, developed in 1965, and popularized and demonstrated since its inception. If Moore's law continues to be upheld in the future, more apps, algorithms, and daily functions will link together each part of our lives, providing increased processing capability and a limitless stream of information creating maximum efficiency for humans.

The Westphalian design of society and order contributes to the human need to work within a set of logical models, whereas the principle of international law and orderly division of nations enables sovereignty over territory and domestic affairs. It is possible that globalization, which would be nearly impossible without a relatively high transfer rate of information, will play a critical role and may challenge global order. Assuming an information advantage is required to achieve nation-state and military objectives, and information superiority is not guaranteed because of the complex IoT, how does the U.S. Government present effective and integrated information warfare capability (IW) in the information age? Moreover, if wars are fought in the information space, can they be won with information alone? In other words, can information warfare provide the ways and means to fight wars, as well as the ends? Also, does the U.S. Government need to invest in an organization responsible for the coordination and integration of IW capabilities and effects?

To increase the U.S. Government's capability and capacity, a new organization should be created within the U.S. Government to focus on information warfare, with a fundamentally different organizational structure than our current governmental hierarchical structures. Specifically, the U.S. Government subscribes to the diplomatic, information, military, and economic (DIME) model but does not have an organization designed to lead the information functions

of this model. The Department of State coordinates the diplomatic role, Department of Defense the military role, and Department of Treasury the economic role. Twenty-first-century challenges presented by the IoT require a more innovative organization that promotes adaptability and agility in the information space, akin to models used at Google, Facebook, or Apple.

Winn Schwartau, author of *Information Warfare* and recognized IW theorist, describes the information age as "computers everywhere."<sup>3</sup> The ultimate fact of the information age is the proliferation of IT, which "incorporates information systems and resources (hardware, software, and wetware) used by military and civilian decisionmakers to send, receive, control, and manipulate information necessary to enable 21<sup>st</sup>-century decisionmaking."<sup>4</sup> Additionally, the development of IT allows sharing of information in near real time, at an exponential rate, anonymously and securely. These advances can be used as an asset, but also pose a potential vulnerability to the United States, our allies, and our adversaries.<sup>5</sup> It takes seconds to upload pictures or comments on social media networks. At the same time, adversaries can use these systems to gain access to critical information. According to a *New York Times* article, "In July 2015, 21.5 million people were swept up in a colossal breach of government computer systems that was far more damaging than initially thought, resulting in the theft of a vast trove of personal information, including social security numbers and some fingerprints."<sup>6</sup> The following list provides a general summary of the number of times systems have been attacked via cyber.<sup>7</sup> The number of attacks on information systems has increased each year, reinforcing the fact that warfare is currently being conducted in the information space via IT.

- *The Pentagon reports getting 10 million attempts a day.*
- *The National Nuclear Security Administration, an arm of the Energy Department, also records 10 million hacks a day.*

- *The United Kingdom reports 120,000 cyber incidents a day. That is almost as many as the state of Michigan deals with.*
- *Utah says it faces 20 million attempts a day—up from 1 million a day 2 years ago.*<sup>8</sup>

To meet the challenge that exists in the information age, organizational changes are required. Modern ideas and incorporating industry concepts may be one way to traverse the information space and create an advantage in future conflicts.

Within the IoT, actions take place in nanoseconds and occur billions of times daily. Big data concepts attempt to harness massive amounts of information and distill that information into something that a human can use to make a decision. In the near future, the information required to win the advantage over an enemy may be determined by who can extract data, identify key centers of gravity in the information space, and automatically take action through rule sets and computational criteria based on defined "rules of engagement." The ability to harness big data exists now and is only increasing. Consumer product companies are mining Facebook, Google, and other data to understand customer preferences, global trends, and public opinion on matters of interest. From a military standpoint, understanding the information terrain in relation to the potential adversaries is foundational to discerning points for information operations (IO) across the range of military operations. Big data concepts used in business could be advantageous and used in information warfare. It is possible that data-mining and subsequently an information advantage could achieve objectives purely through IW alone.

The United States has used various IW strategies, agencies, and professionals, with varying degrees of success. The U.S. Information Agency (USIA) was created in 1953 and was in service until 1999. USIA was designed to consolidate all information activities:

[USIA] comprised all of the foreign information activities formerly carried out by the Department of State's International Information Administration (IIA) and Technical Cooperation Administration, and by the Mutual Security Agency Overseas, existing United States Information Service posts became the field operations offices of the new agency. The exchange of persons program conducted by IIA remained in the Department of State, but USIA administered the program overseas. The Department of State provided foreign policy guidance.<sup>9</sup>

Historically, information warfare was identified as critical to national security, and USIA was required to erode support for the Soviet Union during the Cold War.<sup>10</sup> Today, we usually consider IW as the means, or sometimes a way, to achieve an objective. But currently we rarely think of IW as an end, even though we live in an information age where we are all affected by the information environment every day. Brian Nichiporuk, the author of "U.S. Military Opportunities," discusses IW concepts and postulates:

*The goals of an offensive information-warfare campaign are to deny, corrupt, degrade, or destroy the enemy's sources of information on the battlefield. Doing so successfully, while maintaining the operational security of your own information sources, is the key to achieving "information superiority"—that is, the ability to see the battlefield while your opponent cannot.*<sup>11</sup>

In current and future warfare, information superiority could be the single most decisive factor. For instance, we could think about the China-Taiwan scenario. China is employing a robust IW strategy targeting the Taiwanese government in order to bring Taiwan under Chinese control, without engaging in kinetic war. They are simultaneously using information operations to delay U.S. involvement to the point where any outside interdiction occurs too late to affect the outcome.<sup>12</sup> This concept is fully realized by a dedicated focus on IW strategy, organization, and capabilities. This could be analyzed best by Sun Tzu's strategy: "To

subdue the enemy without fighting is the acme of skill."<sup>13</sup> In another example, the Russian operations in Crimea provide a modern case study where the outcome of operations was directly attributed to IW principles and capability.

### Information Warfare: The Russian Invasion of Crimea

The Russian incursion into eastern Ukraine, and eventual annexation of Crimea in 2014, serves as the current model of a sustained IW campaign and provides examples of successes and failures in these efforts. Russian IW, known as Reflexive Control, has its origins in Soviet doctrine and serves as a key component in their hybrid warfare operations.<sup>14</sup> Reflexive Control "relies . . . on Russia's ability to take advantage of preexisting dispositions among its enemies to choose its preferred courses of action."<sup>15</sup> During operations in Ukraine, Russia's primary impediments included Western European powers and the United States. Russia took multiple actions to seize the advantage of preexisting dispositions among its enemies in order to conduct successful operations in Ukraine and, at the same time, avoid a large-scale confrontation with the West.

As part of Reflexive Control, Russia utilized a well-coordinated denial-and-deception plan, called *maskirovka*, through the use of "little green men" to establish checkpoints and secure key terrain in Ukraine. These little green men operated with speed and efficiency, and wore no identifying patches or unit insignia. This lack of identification allowed Russia to deny any association with these forces, which were later acknowledged as Russian troops. By controlling information and being able to deny its involvement in the occupation of Ukraine during the early stages of the conflict, Russia was viewed as an interested party by the international community—as opposed to a belligerent. This fed directly into Russia's view that Western Europe and the United States did not desire a direct conflict and would not press the issue of Russian involvement, even if discovered.

The ability to operate in relative secrecy also allowed Russia to successfully mask its true desired endstate. By doing so, it allowed for almost any action to potentially be considered a successful mission to enemies and outside observers, due to a lack of understanding of Russian intentions. This also allowed for unchallenged Russian saber rattling and threats against the North Atlantic Treaty Organization and the West as Russia attempted to paint Western Europe and the United States as weak, especially in the eyes of developing nations. In addition to actions on the ground in Ukraine, Russia integrated and utilized television, print media, and social media to deflect and hide its efforts at occupation and annexation while reducing potential Western involvement.<sup>16</sup> The successful use of IW allowed Russian forces to occupy eastern Ukraine and annex Crimea without a large-scale response from the West.

As the world continues to move into the information age, the ability of nation-state and nonstate actors to employ successful IO tactics into their overall strategy will undoubtedly increase. To successfully deter and respond to these threats, the United States must innovate and develop organizations with expertise in both preventing and conducting such actions.

Russia's IW campaign in Ukraine enabled it to achieve the objective of annexing Crimea, but it was not a flawless strategy. One flaw was the effort that Russian leaders took to deny the existence of troops in Ukraine. Even after undeniable proof, including geotagged photographs on social media and captured Russian troops inside Ukrainian territory, Russian President Vladimir Putin continued to deny involvement. These excessive and continual denials served only to discredit Russian leaders and provide additional reason to believe that Russian forces were in fact operating inside Ukraine.<sup>17</sup> In addition, the lack of an overwhelming campaign of offensive cyber actions brings into question the overarching hybrid warfare campaign. Russia is arguably one of the most capable nation-state cyber actors.<sup>18</sup> The lack of a comprehensive offensive



Deputy Secretary of Defense Robert Work and Vice Chairman of the Joint Chiefs of Staff General Paul Selva meet with Commander of U.S. Pacific Command, Admiral Harry Harris, to discuss Third Offset Strategy and its implications for Indo-Asia-Pacific region, October 18, 2016, Camp H.M. Smith, Hawaii (U.S. Navy/Jay M. Chu)

cyber campaign, such as that observed in Estonia in 2007 and Georgia in 2008, raises questions about Russian IW and Reflexive Control strategy. While this may indicate a desire not to aggravate potential adversaries, it may also indicate Russia's inability to control all aspects of its offensive cyber actions such that it was concerned that actions could produce large-scale unintended consequences.<sup>19</sup> These consequences may have resulted in the Russians' inability to deny their involvement, or brought powerful enemies into the conflict. As discussed, the flaws noted in Reflexive Control doctrine serve as examples of how difficult it is currently, and will be in the future, to control the consequences of offensive actions and conduct information warfare in an information age. In an effort to better understand the capabilities and intentions

of potential adversaries, understand their lessons learned, and use them to our advantage, the U.S. Government must ensure that the current organization of IW capabilities and strategic planning enables an integrated and cohesive National Security Strategy.

### Strategic Planning Guidance to Tactical Execution?

In the joint planning process, IO planning is typically a supporting effort. If we prescribe to the idea that all wars are fought on the cognitive plane, at least at some point, then it is logical to assume that, at one point or another, IW courses of action (COAs) should be the supported effort. Moreover, "information operations support themes" are sometimes developed after military kinetic COAs are.<sup>20</sup> While the

current planning process and traditional planning structure provide the formal links between national strategy and the tactical level, they do not prescribe a way in which to gain the information advantage in future conflicts. Arguably, from a national perspective, an information strategy should drive subsequent actions and be integrated from the President to the individual Servicemember. The information strategy should be integrated with strategic communications efforts of the U.S. Government. However, as noted in the 2008 report from the Defense Science Board, "Strategic Communications is a dynamic process with responsibility held by those at the highest levels of government—the President and senior government leaders. . . . But to do so requires a commitment not yet seen,



Routers and switches inside Google's campus network room at Council Bluffs, Iowa, allow data centers to talk to one another, with fiber-optic networks that run at speeds more than 200,000 times faster than typical home Internet connections (Photo courtesy Google Inc.)

though some steps have been taken.”<sup>21</sup> In fact, the report recommends the creation of a nonprofit, nonpartisan Center for Global Engagement as a focal point for strategic communication activities.

In 2010, Joseph Biden provided the President a report on strategic communications that urged synchronization and defined the overall concept.<sup>22</sup> An interagency policy committee, led by the National Security staff, was a recommended solution; however, a committee is made up of individuals with allegiances to their own organization and likely with other responsibilities, not fully being dedicated to integrated strategic communications. The little IW capability that exists is based on the current and legacy organizational structure, which hinders effective IO planning and execution.

If information space can be considered a way and means to fight and win wars, then a framework is required to assist in prioritization and planning and

to present ends that may be achieved through information warfare. Planners must articulate why a specific action is being taken and when it should occur based on commander's intent, the operational environment, and the operational approach designed to solve the problem. Decades of trial and error in warfare have led to institutional doctrine and rule sets. While there is an argument that these rules should be applied to both kinetic and nonkinetic effects, it is important to realize that there are certain unique factors associated with both. For example, targeting fundamentals are largely agreed upon and accepted for offensive force-on-force operations, but do the theories of targeting need to adjust for information warfare?

Some argue that the center of gravity (COG) for the Islamic State of Iraq and the Levant (ISIL) is the Internet. If we accept this idea, how does the United States target ISIL? Does the U.S.

Government shut down Internet Service Providers (ISPs) (that is, the target) that ISIL is using? Does the government conduct a distributed denial-of-service attack against certain Web sites? Does it put influential messages onto ISIL message boards on the Internet? All options are plausible, but many times are not executed due to lengthy and unsynchronized plans. The lack of leadership and a focal point in the U.S. Government who can articulate the second- and third-order effects of information operations often contributes to a lack of action. The ability to understand how the information space will be influenced by the outcome of a U.S. action is not effective because there is no lead organization.

In addition to the tactical-level information effects, how are strategic communications vetted and targeted? Do the processes differ or are they the same? If the view of this process were to change, and targeting were to become a

process within which information targets are held at risk (for example, the ISP example or building a strategic weapon to deter an enemy), then it is possible that realistic options could be presented to a combatant commander in a crisis action scenario. To execute a concept where the United States holds information targets at risk, it must have access to the target. Access for information-related effects delivered through the information space is no different than for physical effects delivered by airplanes or ships. The delivery method could be news, a cyber capability, a military action, or even a comment by the President. The path to employ information-related capabilities (IRCs) requires access from the sender to the receiver, and that targeting path must be sustainable. Without sustained access, a target cannot be held at risk because gaining access to the receiver could take an extended amount of time, with relation to the operation.

Additionally, the capability must be attainable. Software development can be a potential strategic advantage. Driving education and training for software development down to the tactical level empowers young Servicemembers to create capabilities linked to the target, reduce cost, and create efficiencies. For example, a Soldier is taught how to use a rifle, the foundations are built in training, and he is able to utilize the weapon through the employment of various tactics, techniques, and procedures on the battlefield as the situation dictates. If the situation changes, he adjusts to the enemy in an instant. From an IW perspective, software is but one tool, as is the rifle. Foundations are built, skills are honed, but it is left to the tactical level to ensure the capability is “tuned” to the target because the tactical-level operator should have the most accurate knowledge of that target. Additionally, as accesses change, the tactical and operational level should ensure consistent and reliable access to the target. Indeed, the Soldier does not develop the strategy; the national security staff, President, and combatant commanders do. But what organization is responsible for coordinating the strategic message throughout the national

security apparatus? Furthermore, what organization is responsible for providing information operation COAs for the President, specifically designed as an end?

The contrarian viewpoint to the idea of driving development down to the operator level (that is, the Soldier) is that authorities do not come with capability. This is true. A tactical-level unit should not have authority to execute operations in the information space, just as the Soldier with the rifle would not fire without orders. There should be a strategy with clear and precise guidance for operational and tactical targeting. This does not require “execution authorities,” but it does require guidance from national-level leadership on the issue. In other words, because technical acumen is required, the U.S. Government cannot afford to have a disjointed IW strategy in which progress is slowed due to an overly complicated and bureaucratic hierarchical structure. A lack of unity of effort results, and risk to mission and risk to force increase. Developers, operators, and analysts need flexibility and agility to solve problems quickly with innovative technology and an understanding of the information age, just as a Soldier does when in battle.

### Is the World Organizationally Changing?

Military organizations have generally followed hierarchical models as early as the Greeks in 400 BCE for organizing and equipping. It is possible that global IT trends will require a foundationally different way of thinking and organizing IRCs in the U.S. Government to maintain pace with the speed of information. Largely, from the time of the Greeks to that of the current U.S. Government, militaries have been designed around a hierarchical system. As IW becomes increasingly more important during the conduct of government or military operations, a lattice framework and system may be a logical way to organize information warfare-based capabilities and personnel.

This concept prescribes basic guidance and a certain rule set (that is, authorities) but empowers individual

members to develop solutions unabated by personnel unfamiliar with the technical situation. The concept capitalizes on meritocracy-based principles and focuses on a federated approach as well as crowd-sourcing solutions internally to the military, or even in the public sector, to arrive at solutions. Within the U.S. Government, it is unlikely that a lattice organization would be wholly integrated; however, a hybrid concept that captures the value of a legal and hierarchical framework along with realizing the potential benefit of a lattice organization would be valuable, as globalization and IT increasingly integrate our world. Additionally, a lattice framework would more closely align conceptually with the mass-network IT environment in which we live. Ideas presented in the corporate world are potential solutions that can be used or modified for complicated IW concepts within the U.S. Government. In a thought piece from business, Cathleen Benko and Molly Anderson from *Forbes* magazine highlight a few key benefits of a lattice organizational structure:

*With employees working in geographically dispersed teams, the old ways of communicating [are] no longer served. Lattice ways to participate moved the organization toward more interactive, transparent communication. In one instance, the finance division gave a role traditionally reserved for management—identifying improvement priorities—to employees, by launching a “pain points” portal where they can voice their views of current challenges for everyone to see. The company appoints teams to address the highest priorities.*

*At Deloitte, our annual employee survey shows that 90% of workers who experience all three lattice ways are engaged. Contrast that with the results of a major global workforce study by Towers Perrin in 2007–2008 that found just over 60% of employees in surveyed companies were engaged.<sup>23</sup>*

Not only does a lattice framework promote internal integration and idea-sharing, the concept also promotes the use of solutions from external sources. In many cases, members of a lattice-type



USS *Freedom* and USS *John C. Stennis* are under way conducting Independent Deployer Certification exercise in surface warfare, air defense, maritime-interception operations, command and control/information warfare, C4 systems intelligence, and mine warfare, April 28, 2015 (U.S. Navy/Ignacio D. Perez)

organization are encouraged to look for nonstandard solutions to difficult problems, even if that means branching outside of organizational norms.

Analyzing a recent case, the iPhone encryption issue surrounding the San Bernardino terrorist attack is an example of a federated approach to problem-solving. The Federal Bureau of Investigation (FBI) was able to crack the iPhone's encryption, despite Apple's unwillingness to support. Apple's fear stemmed from the idea that if it provided the requested support, the government would then own the key to all encryption security measures for iPhones around the world.<sup>24</sup> When the international media reported and publically debated the issue, the FBI received calls from individuals and companies claiming to possess the tools necessary to break the encryption. In fact, one company was able to break the encryption and allowed the FBI to retrieve

the desired data from the terrorist's phone. This example shows the power of information in multiple ways; the first is the fact that the government was unable to use traditional methods of gaining support from a private company. Second, media, as the primary driver, brought attention to the problem and forced a public debate, which worked in favor of the government. There were arguments on both sides of the issue, but it should be assumed that the challenge in and of itself was enough to stimulate a solution, whether right or wrong. The key point to this example is that the proliferation of information drove a solution, regardless of Apple's standpoint, the FBI's authority, and even despite popular public opinion for or against the FBI. If the power of information can easily dictate the outcome of such an example, what are the long-term implications for warfare? The U.S. Government can take measures now,

organizationally, to harness IW concepts and be positioned to maintain the information advantage in a dynamic and unsure information age.

Future IW solutions will also need to involve multidomain skills from individuals with varying backgrounds. In today's military, once a Servicemember is branded with a specific skill set, it is challenging to break from that community and maneuver effectively between communities, while still maintaining upward mobility. To achieve greater effectiveness in IO planning and execution, cross-domain and diverse IRC careers should become a desired career path option for future leaders.

### **Amazon Meets the U.S. Government**

To harness the information age and enable IW capability toward the success of future U.S. conflicts, a new organiza-

tion should be created within the U.S. Government. The Cold War has passed, and so has USIA; however, it is possible that a new version of USIA is required as Russia continues to test its limits of power. As in the case of Ukraine, Georgia, and Estonia, as well as the need to combat terrorist groups such as ISIL, a renewed effort on U.S. information warfare is required. The dynamic and ever-changing environment requires a fundamentally different organizational structure than that of current government hierarchical structures in order to be flexible and adaptable for 21<sup>st</sup>-century problems. Additionally, as we move forward in the information age, our lives will be increasingly intertwined and connected with information systems. This information environment will continue to play a critical role in how the U.S. Government and military interact with allies, partners, and adversaries in all of the operational domains.

To shape the environment to meet our desired endstates, we must recognize the importance of information warfare and work to ensure that IO concepts are properly integrated into all actions and operations, if not become an end themselves. We must also search for innovative ways to build and employ IO concepts. Our IO experts must have the required training and expertise necessary to meet these requirements by way of strategic guidance. Operators must have flexibility and agility engrained into their ethos through a lattice-type organizational structure, which honors a multidomain career path. The ability to carry out all IW requirements must be done in a timely and succinct manner that allows for the fastest possible action with the most flexibility. If we are not able to achieve these objectives, we will most definitely fall behind in the fast-paced and constantly changing world of IT and IW, and we will likely be ineffective in identifying and combating enemy COGs, such as ISIL's reliance on IT. It is time to implement ideas that exist in industry, and force change, before change is unattainable—through a sustainable and repeatable process and organization within the U.S. Government. JFQ

## Notes

<sup>1</sup> “A mesh network is a Local Area Network (LAN), Wireless Local Area Network (WLAN), or Virtual Local Area Network (VLAN) that employs one of two decentralized connection arrangements: full mesh topology or partial mesh topology. In a full mesh topology, each network node is connected directly to others. In a partial mesh topology, some nodes are connected to all the others, but are only connected to those nodes with which they exchange the most data.” See “Mesh Network Topology (Mesh Network),” *IoT Agenda.com*, available at <<http://internetofthingsagenda.techtarget.com/definition/mesh-network-topology-mesh-network>>.

<sup>2</sup> Machine-learning is a subfield of computer science that evolved from the study of pattern recognition and computational learning theory in artificial intelligence. Machine-learning explores the construction and study of algorithms that can learn from and make predictions on data.

<sup>3</sup> Richard M. Crowell, *War in the Information Age: A Primer for Cyberspace Operations in 21<sup>st</sup> Century Warfare* (Newport, RI: U.S. Naval War College, 2010).

<sup>4</sup> Ibid.

<sup>5</sup> Joint Publication (JP) 3-13, *Information Operations* (Washington, DC: The Joint Staff, November 27, 2012), I-1.

<sup>6</sup> Julie Hirschfeld Davis, “Hacking of Government Computers Exposed 21.5 Million People,” *New York Times*, July 9, 2015.

<sup>7</sup> Brian Fung, “How Many Cyberattacks Hit the United States Last Year?” *National Journal*, March 8, 2013, available at <[www.nextgov.com/cybersecurity/2013/03/how-many-cyberattacks-hit-united-states-last-year/61775/](http://www.nextgov.com/cybersecurity/2013/03/how-many-cyberattacks-hit-united-states-last-year/61775/)>.

<sup>8</sup> Ibid.

<sup>9</sup> U.S. Information Agency, available at <[www.archives.gov/research/foreign-policy/related-records/rg-306.html](http://www.archives.gov/research/foreign-policy/related-records/rg-306.html)>.

<sup>10</sup> Alvin A. Snyder, *Warriors of Disinformation: American Propaganda, Soviet Lies, and the Winning of the Cold War* (New York: Arcade Publishing, 1995).

<sup>11</sup> Brian Nichiporuk, “U.S. Military Opportunities: Information-Warfare Concepts of Operation,” in *The Changing Role of Information in Warfare*, ed. Zalmay Khalilzad and John White (Santa Monica, CA: The RAND Corporation, Project Air Force, 1999), 181.

<sup>12</sup> Eric A. McVadon, “Systems Integration in China’s People’s Liberation Army,” in *The People’s Liberation Army in the Information Age*, ed. James C. Mulvenon and Richard H. Yang (Santa Monica, CA: The RAND Corporation, 1999), available at <[www.rand.org/content/dam/rand/pubs/conf\\_proceedings/CF145/-CF145.chap9.pdf](http://www.rand.org/content/dam/rand/pubs/conf_proceedings/CF145/-CF145.chap9.pdf)>.

<sup>13</sup> Sun Tzu, *The Art of War* (Oxford: Oxford University Press, 1963), 77.

<sup>14</sup> Maria Snegovaya, *Putin’s Information Warfare in Ukraine: Soviet Origins of Russia’s Hybrid Warfare*, Russia Report I (Washington, DC: Institute for the Study of War, September 2015), 7, available at <<http://understandingwar.org/report/putins-information-warfare-ukraine-soviet-origins-russias-hybrid-warfare>>.

<sup>15</sup> Ibid.

<sup>16</sup> Ibid.

<sup>17</sup> Dmitry Gorenburg, “Crimea Taught Us a Lesson, But Not How the Russian Military Fights,” *War on the Rocks*, May 19, 2014, available at <<http://warontherocks.com/2014/05/crimea-taught-us-a-lesson-but-not-about-how-the-russian-military-fights/>>.

<sup>18</sup> LookingGlass Cyber Threat Intelligence Group, *Operation Armageddon: Cyber Espionage as a Strategic Component of Russian Modern Warfare*, CTIG-20150428-01 (Reston, VA: LookingGlass Cyber Solutions, Inc., April 28, 2015), available at <[https://lookingglass-cyber.com/wp-content/uploads/2015/08/Operation\\_Armageddon\\_FINAL.pdf](https://lookingglass-cyber.com/wp-content/uploads/2015/08/Operation_Armageddon_FINAL.pdf)>.

<sup>19</sup> David Talbot, “Watching for a Crimean Cyberwar Crisis,” *MIT Technology Review*, March 4, 2014, available at <[www.technologyreview.com/s/525336/watching-for-a-crimean-cyberwar-crisis/](http://www.technologyreview.com/s/525336/watching-for-a-crimean-cyberwar-crisis/)>.

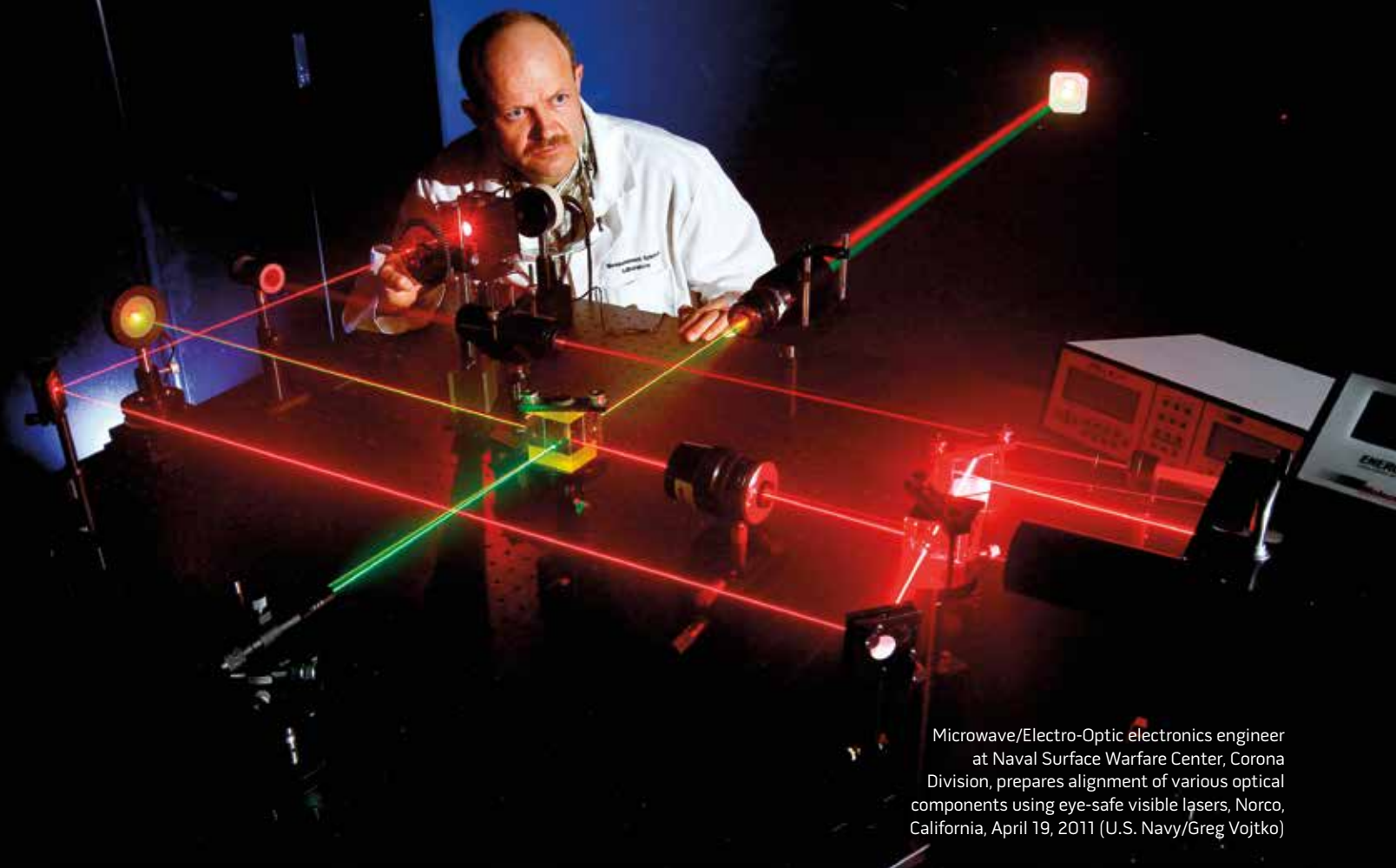
<sup>20</sup> JP 5-0, *Joint Operation Planning* (Washington, DC: The Joint Staff, August 11, 2012), II-9.

<sup>21</sup> *Report of the Defense Science Board Task Force on Strategic Communication* (Washington, DC: Department of Defense, January 2008), available at <[www.acq.osd.mil/dsb/reports/ADA476331.pdf](http://www.acq.osd.mil/dsb/reports/ADA476331.pdf)>.

<sup>22</sup> *National Framework for Strategic Communication* (Washington, DC: The White House, 2010).

<sup>23</sup> Cathleen Benko and Molly Anderson, “The Lattice that Has Replaced the Corporate Ladder,” *Forbes.com*, March 16, 2011, available at <[www.forbes.com/2011/03/16/corporate-lattice-ladder-leadership-managing-hierarchy.html](http://www.forbes.com/2011/03/16/corporate-lattice-ladder-leadership-managing-hierarchy.html)>.

<sup>24</sup> Pierre Thomas and Mike Levine, “How the FBI Cracked the iPhone Encryption and Averted a Legal Showdown with Apple,” ABC News, May 29, 2016, available at <<http://abcnews.go.com/US/fbi-cracked-iphone-encryption-averted-legal-showdown-apple/story?id=38014184>>.



Microwave/Electro-Optic electronics engineer at Naval Surface Warfare Center, Corona Division, prepares alignment of various optical components using eye-safe visible lasers, Norco, California, April 19, 2011 (U.S. Navy/Greg Vojtko)

# The Rise of the Commercial Threat

## Countering the Small Unmanned Aircraft System

By Anthony Tingle and David Tyree

The Small Unmanned Aircraft System (sUAS) is a disruptive commercial technology that poses a unique and currently undefined threat to U.S. national security. Although, as with any new technology,

the parameters of the capabilities regarding military use have yet to be fully discovered, recent events highlight the potential danger. In September 2013, an unarmed sUAS hovered near the face of German Chancellor

Angela Merkel while she delivered a campaign speech.<sup>1</sup> In January of 2015, an sUAS defied restricted airspace and landed, initially undetected, on the White House lawn.<sup>2</sup> And more recently, in August of 2016, at least five sUASs disrupted wildfire fighting efforts near Los Angeles, grounding helicopters for fear of mid-air collisions.<sup>3</sup> Likewise, sUAS altercations with law enforcement are increasing, as the Federal Aviation Administration now receives over 100 adverse UAS reports per month.<sup>4</sup> These examples emphasize the intrusive, undetectable, and potentially lethal nature of this emerging technology.

The sUAS epitomizes the difficulties with rapidly advancing commercial technology.<sup>5</sup> The sUAS is as prolific as it is disruptive, and it will challenge our joint air-defense procedures and doctrine and redefine our perspective on the military uses of commercial technology. In this article, we examine the characteristics and capabilities of the sUAS, report on

---

Lieutenant Colonel Anthony Tingle, USA, is a Strategic Initiatives Analyst at the U.S. Army Space and Missile Defense Command. Second Lieutenant David Tyree, USAF, is a Flight Student Pilot at Vance Air Force Base, Oklahoma.



current counter-UAS initiatives within the Department of Defense (DOD), and present policy ideas to mitigate the future threat from militarized commercial technology.

## Characteristics and Capabilities

The rapid rate of commercial technology's advance has directly contributed to the rise of sUASs. Improvements in communication equipment, cryptography, and lightweight materials have led to the current state of the multiple rotary-wing UASs, often referred to as "quadcopters," and extremely small fixed-wing UASs. For this article, we define aircraft that fall into the DOD UAS Category 1 (weighing less than 20 pounds) as an sUAS<sup>6</sup> because the interdiction of larger than Category 1 aircraft quickly approaches traditional defensive counterair operations.<sup>7</sup>

As technology advances, the sUAS will increase in lethality. If Moore's law continues to hold, we will see an increase in sUAS command and control distances, electro-optical sensor resolution, GPS guidance accuracy, and battlefield autonomy. With advances in material science, especially considering adaptive ("3D") printing techniques and carbon nanotubes, sUASs will become smaller, faster, and lighter, and will loiter longer and carry heavier payloads.

The basic physical structure of the sUAS (including the use of advanced materials) hinders radar technologies, the primary component of modern air defense. Radar works by bouncing energy off airborne objects and interpreting the return reflections. Although the carbon fiber and plastic components (of which the majority of most sUASs are comprised) naturally reduce radar return, size appears to contribute most to the shortcomings in sUAS radar identification and tracking.<sup>8</sup> While modern radar technology has the capability to engage smaller objects. Additionally, concerning radar, sUASs are often indistinguishable from other airborne objects (specifically birds).<sup>9</sup> While additional methods such as acoustic-phased arrays and electro-optical cameras show promise, a combination of these tracking and identification

technologies may be necessary to defend against the growing sUAS threat.

It is hard to understate the current complexity and importance of positively identifying sUASs. As sUASs continue to be used for a variety of commercial and private purposes (including package delivery and photography), the sUAS operator's intent becomes difficult to discern. Unlike traditional aircraft, which require runways and thus provide longer lead times for tracking, the average sUAS is able to become airborne quickly and close on its target. Additionally, positive identification is a necessary component of engagement authority, especially when considering deployment of sUAS countermeasures on U.S. soil, including interdiction by law enforcement and the possibility of civilian casualties. To effectively counter sUASs, it will be necessary to refine and practice procedures and doctrine, while developing the capability to effectively detect, track, and positively identify the threat.

Future advances in material and computational science will enable the sUAS to perform autonomously, increasing their efficacy as an offensive weapon. One of the characteristics of the sUAS is that it uniquely lends itself to advanced aerial tactics. As battlefield automation progresses, militaries are advancing toward the use of multitudes of sUASs in coordinated formations known as "swarming." This swarming tactic could make defense difficult, especially for large objects or fixed facilities. The use of swarm tactics increases the destructive power of the sUAS and presents adversaries with a defensive dilemma.<sup>10</sup> In this regard, militaries may have to reconsider the concept of *mass* on the battlefield.

Currently, the practical use of sUAS swarms suffers from a confluence of technological shortcomings seemingly resolved by relatively minor advances in technology. The lift capacity, speed, and agility of the sUAS is directly dependent on the amount of weight carried by the vehicle. Reductions in the weight of communications equipment, sensors, onboard processors, and kinetic payload (for example, "energetics")<sup>11</sup> will increase the range and maneuverability of these systems. Likewise, advances in small,

lightweight power sources and materials such as carbon nanotubes (and corresponding manufacturing processes such as adaptive printing) will enable smaller and faster sUASs with longer loiter and greater operating distances.

While the size and maneuverability are defining characteristics of the sUAS, advances in automation algorithms are a necessary component of the swarming tactic. Simultaneous command and control of a large number of small objects necessitates autonomy technology that will undoubtedly be available in the near future.<sup>12</sup> In fact, a number of UASs currently deployed or in development operate with varying degrees of autonomy.<sup>13</sup> It is quite feasible that attacking sUAS swarms will be able to automatically sense and communicate weaknesses in the opposing defense, thus adapting their swarming tactics accordingly.

The development of sUAS swarm tactics and techniques in many ways mirrors the introduction of Multiple Independently Targetable Reentry Vehicle (MIRV) technology in the early 1970s. The MIRV concept included the use of multiple nuclear warheads included in a single ballistic missile, greatly increasing the probability of successfully striking the enemy with nuclear missiles.<sup>14</sup> Similar to the inability of the Soviets to counter a larger number of potential inbound nuclear warheads, the sUAS overwhelms those on the defense with possible multiple aggressors. Although similar in terms of using mass, sUAS differs from MIRV in terms of maneuverability and the ability to land and wait for more opportune times to attack. Not all the sUASs in the offensive swarm need to be deadly, as the parallels with MIRVs extend beyond a simple numerical advantage. Offensive sUAS tactics could co-opt the idea of decoys from MIRV technology. With the advent of MIRV decoys, or warheads that had the same physical characteristics as their nuclear counterparts, the economic efficiency of MIRV technology enabled asymmetric advantages.<sup>15</sup> Similarly, the use of decoys may reduce the overall cost of simultaneously attacking with large numbers of sUASs, presenting adversaries with multiple deadly dilemmas.

## Current Counter-UAS Initiatives

The U.S. military currently has a multitude of ways to effectively destroy UASs. Starting in 2002, the military exercise Black Dart focused on countering the UAS threat. The exercise has tested a number of kinetic and nonkinetic methods ranging from 0.50-caliber guns to Hellfire missiles.<sup>16</sup> The ability to defend against this threat is, at its core, a problem of asymmetry and efficiency. How do we defeat swarms of \$1,500 drones in a practical, cost-efficient manner? The following sections detail existing counter-UAS methods, including traditional kinetic and directed energy means, and examine their applicability to defending against sUASs.<sup>17</sup>

### *Traditional Kinetic Methods.*

Traditional kinetic means of air defense, while ostensibly effective in a single intruder scenario, are cost inefficient versus relatively cheap sUASs. Factoring in the possibility of multiple small, low, and fast targets, existing kinetic means of defense are tactically inadequate. Current kinetic defense systems lack the coverage, range, and accuracy to counter future sUAS swarms.<sup>18</sup> It is unlikely that these weapons systems could create a necessary “dome of steel” around stationary positions. Although reducing the caliber of these defensive weapons may ostensibly increase the *rate* of fire, one would expect a corresponding decrease in range. Disregarding possible Gaussian-type weapons (for example, railguns) currently under development, the most viable direct-fire kinetic defense from sUASs may be small-caliber precision-guided rounds.

The miniaturization of precision-guided munitions may provide the capability to interdict a large number of sUASs at standoff distances. According to Deputy Secretary of Defense Robert Work, “We’re not too far away from guided 0.50-caliber rounds. We’re not too far away from a sensor-fused weapon that instead of going after tanks will go after the biometric signatures of human beings.”<sup>19</sup> In the absence of a viable “brute force” or “shotgun” method of area defense (for example, massive amounts of “dumb” kinetic projectiles),

these relatively cheap miniature guided munitions may hold the answer to countering swarms of sUASs. Another method to counter sUASs may be with the use of other sUASs.

One method to counteract swarms of attacking sUASs may be to use sUASs as “hunter-drones.” Currently, there is a “drone war” occurring over the skies of Tokyo as the Japanese Yakuza (an organized crime syndicate) frequently use sUASs to courier drugs across the city. When the Tokyo police use sUASs with nets to capture these drones, the Yakuza retaliate by attacking the police drones.<sup>20</sup> Increases in battlefield automation might allow “hunting parties” of sUASs to degrade or destroy enemy sUASs with nets or other kinetic methods. Additionally, man-portable air-defense systems like anti-UAS weapons may prove effective against sUASs.<sup>21</sup> In the near term, though, solutions may lie in more natural means of sUAS interdiction.

There has been research into the use of birds of prey for countering the sUAS threat.<sup>22</sup> The U.S. Air Force Academy has recently conducted a year-long study involving gyrfalcon falcons. Tests reveal the falcons were able to “detect, positively identify, track, and engage a specific sUAS already in flight.”<sup>23</sup> Compared to soaring birds like hawks and eagles, falcons must actively flap their wings while in flight, limiting loiter time to around 20 minutes. Additionally, the training time per falcon is approximately 4 to 5 months.<sup>24</sup> While this study did not address the use of falcons to interdict different types of sUASs, the study lead, Lieutenant Colonel Donald Rhymer, believes that it is possible to “train falcons to generalize to different types of UASs.”<sup>25</sup>

**Directed Energy.** If Army directed-energy systems are disadvantaged in terms of size and weight (compared with the Navy’s), then Air Force systems are even more so. The Air Force is constrained by attempting to develop directed-energy systems carried by aircraft. The Air Force scientific advisory board is currently assessing the requirements for these missions on the modified AC-130H model,<sup>26</sup> with a projected demonstration date of 2020.<sup>27</sup> While this lofty endeavor

recalls memories of the now defunct Airborne Laser System, the mission and domain of the Air Force forces the Service to pursue small, lightweight laser systems that can be mounted on aircraft.

Perhaps the most promising directed-energy technology in terms of defeating multiple sUASs is the use of high-powered microwaves. These microwave devices have the capability to render the electronic components of an sUAS useless, much like an electromagnetic pulse (EMP).<sup>28</sup> Although there may be practical considerations in the use of EMP devices in urban environments or on the battlefield (that is, necessitating controlled use of these weapons), microwave weapons are under development and, in the future, could be used simultaneously to destroy large numbers of sUASs.<sup>29</sup>

## Addressing the Threat: Commercial Adaptive R&D

Since the early 2000s, DOD has acknowledged the necessity to increase the integration of commercial technology into military systems and procurement. But it is a recent phenomenon that commercial technology represents complete capabilities that circumvent the long lead times of traditional government research and development (R&D) and procurement. In other words, in many sectors commercial products are no longer simply contributing to military capabilities; they *are* the capabilities.<sup>30</sup>

While DOD has adapted to the commercial influence in defense procurement, it has failed to recognize the increasing rate of impact of technology on national security. The rising capabilities of commercial technologies, such as the sUAS, presage even greater future commercial threats. Similar to the impact of civilian malware across the spectrum of cyber operations (on both civilian and military concerns), future unforeseen commercial technologies will readily lend themselves to military applications, unnerving those most concerned with maintaining national security.

The challenge is to address this new and fast-moving commercial threat under the shadow of an antiquated and



Cadet-in-charge for Academy falconry team pulls lure as Ace, a black gyrfalcon, makes pass at it, September 10, 2010 (U.S. Air Force/Bennie J. Davis III)

inadequate defense procurement process. The existing DOD procurement paradigm relies on establishing requirements that are fulfilled, in part, by commercial-off-the-shelf (COTS) systems and components. Regarding DOD R&D, this requirements-based procurement happens either directly (from the national labs, for example) or indirectly through using COTS. As emerging COTS capabilities surpass the capacity of the government R&D establishment, the United States must develop policies to maintain its technical advantage over its adversaries.

In terms of contribution to national defense, the United States currently fails to take full advantage of its indigenous private industry. We recommend that DOD should work closer with private industry prior to the release of commercial technology, a policy that we call Commercial Adaptive R&D, or CARD.<sup>31</sup> The CARD concept promotes the use of DOD partnerships and relationships with commercial firms to enhance DOD visibility of impending commercial technological release. In contrast with simply

using the results of commercial R&D in the form of COTS, under the CARD concept, DOD would seek to conduct research on technology at different stages of development. This pre-market R&D has a number of advantages for both DOD and the firm.

First, DOD gains knowledge on market-shaping technology that will inevitably find its way into the hands of our adversaries. With commercial technologies' rising level of capabilities, state and nonstate actors increasingly threaten U.S. ability to maintain technological overmatch. By conducting CARD, DOD gains vital knowledge on the possible uses of new technologies, and possible counters to these technologies, before our adversaries. Much like the development of the Defense Advanced Research Projects Agency after the launch of Sputnik in 1957, the use of the CARD strategy will help prevent the United States from being surprised by significant commercial technology.

Second, for both the firms and DOD, there exists a possible benefit from the

discovery of additional uses for their technology. The dual-use nature of technology is rarely immediately apparent, especially if the government is not exposed to or knowledgeable of that technology.<sup>32</sup> By working closely with large firms, DOD is able to discover new national defense applications for commercial technology, helping both the firm and the government.

Third, DOD can revive the chances for possibly useful technologies that have fallen "below the cut line"—or, in other words, are deemed by the firm as not commercially viable. By signaling its interest in these technologies, DOD provides an opportunity for a "second life" to the firm's technology, resulting in possible commercialization.

Lastly, the CARD construct reduces government R&D risk. The government no longer directly vets new technology as the industry bears the brunt of maturation of the innovation. Utilizing these market-shaping firms in partnership roles with government R&D is disproportionately low given the amount of R&D



Sailors assigned to USS *Jason Dunham*, U.S. Air Force Academy Cadets, and engineers from Johns Hopkins University Applied Physics Lab test unmanned aerial systems aboard rigid hull inflatable boat during exercise Black Dart, September 20, 2016, Gulf of Mexico (U.S. Navy/Maddelin Angebrand)

that is conducted (for example, the Intel Corporation R&D budget for 2013 was roughly \$10.6 billion).<sup>33</sup> A majority of the risk is placed on the commercial firm, whereas DOD begins to conduct R&D on the product in mid-to-late stream.

By adopting new policies toward government defense procurement and the degree to which they conduct research with private industry before the commercial release of COTS products, DOD will develop early defenses against threatening technologies, help shape the development of defense-related technologies, and prevent technological surprise. The greater integration of DOD into private R&D, or CARD, will help better ensure national defense in a period of increasing commercial threats.

## Conclusion

Although current state-of-the-art sUAS capabilities are sufficiently threatening, we are on the cusp of technological advances that will make the sUAS expo-

nentially more deadly. The asymmetric nature of the sUAS, especially when considering swarm tactics, makes the technology difficult to defend against. An sUAS is relatively inexpensive and ubiquitous (it is estimated that there are over one million sUASs in the United States alone).<sup>34</sup> Conversely, most defense systems are—at least at this stage of development—restrictively expensive. It may be fiscally restrictive and grossly inefficient to attempt to counter this commercial threat with large military programs. Additionally, as technologically state-of-the-art as current commercial sUASs appear, small advances in supporting technologies will yield huge leaps in sUAS capabilities, further compounding defensive problems such as detection and identification.

To protect against this threat, the United States must develop doctrines both for sUAS attack and defense. It is necessary to improve our capabilities in

*both* offensive and defensive sUAS technologies. Additionally, this is inherently a joint fight, with the technology and techniques developed by each Service synergistically contributing to the development of anti-sUAS doctrine. Now may be the time to establish a joint organization specifically to address the sUAS threat, similar to the Joint Improvised-Threat Defense Organization (formerly known as the Joint Improvised Explosive Device Defeat Organization), originally established to counter improvised explosive devices.

Additionally, since the early 2000s, it has been widely accepted that DOD needs to integrate COTS requirements solutions. In this “linear model” of innovation, private industry conducts R&D to develop the COTS product, and the government applies COTS to existing requirements. Most important, DOD needs to conduct R&D on the pre-COTS product to discover new requirements based on new capabilities.

This form of R&D should supersede the old model of simply fulfilling government requirements. DOD can accomplish this through close interaction with private industry to discover uses for emerging COTS products before they are simultaneously released to the public and our potential adversaries.

In the history of modern warfare, there have been few purely commercial technologies that so readily lend themselves to immediate weaponization as the sUAS. The threat lies not only in the technology itself, but also in the degree to which that technology is sufficiently capable and available to all potential nefarious actors. In this sense, the potential threat from sUASs should catalyze new thinking in DOD about the uses of commercial technology. Moving forward, it is this commercial availability of advanced technology that is the true threat, and it is this new technological frontier that may pose the greatest future challenge to our national security. JFQ

## Notes

<sup>1</sup> Wallace Ryan and Loffi Jon, "Examining Unmanned Aerial System Threats and Defenses: A Conceptual Analysis," *International Journal of Aviation, Aeronautics, and Aerospace*, no. 4 (January 10, 2015).

<sup>2</sup> Faine Greenwood, "Man Who Crashed Drone on White House Lawn Won't Be Charged," *Slate.com*, March 18, 2015, available at <[www.slate.com/blogs/future\\_tense/2015/03/18/white\\_house\\_lawn\\_drone\\_the\\_man\\_who\\_crashed\\_it\\_there\\_won\\_t\\_be\\_charged.html](http://www.slate.com/blogs/future_tense/2015/03/18/white_house_lawn_drone_the_man_who_crashed_it_there_won_t_be_charged.html)>.

<sup>3</sup> Michael Martinez, Paul Vercammen, and Ben Brumfield, "Above Spectacular Wildfire on Freeway Rises New Scourge: Drones," *CNN.com*, July 19, 2015, available at <[www.cnn.com/2015/07/18/us/california-free-way-fire](http://www.cnn.com/2015/07/18/us/california-free-way-fire)>.

<sup>4</sup> The latest Federal Aviation Administration (FAA) reports are available at <[www.faa.gov/uas/law\\_enforcement/uas\\_sighting\\_reports/](http://www.faa.gov/uas/law_enforcement/uas_sighting_reports/)>.

<sup>5</sup> While the militarization of the Small Unmanned Aerial System (sUAS) would ostensibly increase its lethality, this article focuses on the possible capabilities of commercial sUASs (including the addition of an explosive payload).

<sup>6</sup> Practically, the discussion of sUASs should not be limited to this weight. The FAA categorizes aircraft under 55 pounds as an sUAS.

<sup>7</sup> UAS Task Force Airspace Integration Integrated Product Team, *Unmanned Aircraft*

*System Airspace Integration Plan* (Washington, DC: Department of Defense, March 2011), available at <[www.acq.osd.mil/sts/docs/DoD\\_UAS\\_Airspace\\_Integ\\_Plan\\_v2\\_\(signed\).pdf](http://www.acq.osd.mil/sts/docs/DoD_UAS_Airspace_Integ_Plan_v2_(signed).pdf)>.

<sup>8</sup> William Camp, Joseph Mayhan, and Robert O'Donnell, "Wideband Radar for Ballistic Missile Defense and Range-Doppler Imaging of Satellites," *Lincoln Laboratory Journal* 12, no. 2 (2000), 267–280.

<sup>9</sup> In the same vein as radar, infrared systems have a similarly difficult time in detecting small heat signatures of an sUAS.

<sup>10</sup> John Arquilla and David Ronfeldt, *Swarming and the Future of Conflict* (Santa Monica, CA: RAND, 2000), available at <[www.rand.org/pubs/documented\\_briefings/DB311.html](http://www.rand.org/pubs/documented_briefings/DB311.html)>.

<sup>11</sup> *Energetics* refers to the reduction of explosive size while increasing explosive power. See John Gartner, "Military Reloads with Nanotech," *MIT Technology Review*, January 21, 2005, available at <[www.technologyreview.com/s/403624/military-reloads-with-nanotech](http://www.technologyreview.com/s/403624/military-reloads-with-nanotech)>.

<sup>12</sup> Daniel Gonzales and Sarah Harting, *Designing Unmanned Systems with Greater Autonomy* (Santa Monica, CA: RAND, 2014), available at <[www.rand.org/pubs/research\\_reports/RR626.html](http://www.rand.org/pubs/research_reports/RR626.html)>.

<sup>13</sup> One example of autonomous UAS operations is the use of the Israeli Harpy 2 for suppression of enemy air defense operations. See T.X. Hammes, "Cheap Technology Will Challenge U.S. Tactical Dominance," *Joint Force Quarterly* 81 (2<sup>nd</sup> Quarter 2016).

<sup>14</sup> Lynn Etheridge Davis and Warner R. Schilling, "All You Ever Wanted to Know About MIRV and ICBM Calculations but Were Not Cleared to Ask," *The Journal of Conflict Resolution* 17, no. 2 (1973), 207–242.

<sup>15</sup> John Wilson Lewis and Hua Di, "China's Ballistic Missile Programs: Technologies, Strategies, Goals," *International Security* 17, no. 2 (1992), 5–40.

<sup>16</sup> Richard Whittle, "Military Exercise Black Dart to Tackle Nightmare Drone Scenario," *New York Post.com*, July 25, 2015, available at <<http://nypost.com/2015/07/25/military-operation-black-dart-to-tackle-nightmare-drone-scenario/>>.

<sup>17</sup> While possible sUAS countermeasures exist, this article does not discuss technologies and techniques associated with cyber effects, such as GPS spoofing and command link capture.

<sup>18</sup> The 20-mm Phalanx (Close-In Weapon System) has a left-to-right limit of 300 degrees. For more information, see "USA 20 Mm Phalanx Close-in Weapon System (CIWS)," *NavWeaps.com*, June 16, 2010, available at <[www.navweaps.com/Weapons/WNUS\\_Phalanx.htm](http://www.navweaps.com/Weapons/WNUS_Phalanx.htm)>.

<sup>19</sup> Cheryl Pellerin, "Work Details the Future of War at Army Defense College," *Defense News*, April 8, 2015, available at <[www.defense.gov/News-Article-View/Article/604420](http://www.defense.gov/News-Article-View/Article/604420)>.

<sup>20</sup> James Vincent, "Tokyo Police Unveil Net-wielding Interceptor Drone," *The Verge.com*, December 11, 2015, available at <[www.theverge.com/2015/12/11/9891128/tokyo-interceptor-net-drones](http://www.theverge.com/2015/12/11/9891128/tokyo-interceptor-net-drones)>.

<sup>21</sup> Andrew Tarantola, "The SkyWall 100 Is a Net-launching Anti-Drone Bazooka," *Engadget.com*, March 3, 2016, available at <[www.engadget.com/2016/03/03/the-skywall-100-is-a-net-launching-anti-drone-bazooka/](http://www.engadget.com/2016/03/03/the-skywall-100-is-a-net-launching-anti-drone-bazooka/)>.

<sup>22</sup> See Peter Holley, "Watch This Trained Eagle Destroy a Drone in a Dutch Police Video," *Washington Post*, February 2, 2016, available at <[www.washingtonpost.com/news/worldviews/wp/2016/02/01/trained-eagle-destroys-drone-in-dutch-police-video/](http://www.washingtonpost.com/news/worldviews/wp/2016/02/01/trained-eagle-destroys-drone-in-dutch-police-video/)>.

<sup>23</sup> Don Rhymer et al., "Falconry: Alternate Lure Training (FALT)," Report nos. 56250 and 63300.

<sup>24</sup> Don Rhymer, telephone interview by authors, November 11, 2015.

<sup>25</sup> *Ibid.*

<sup>26</sup> William P. Head, *Night Hunters: The AC-130s and Their Role in U.S. Airpower* (College Station: Texas A&M University Press, 2014).

<sup>27</sup> Thomas Masiello and Sydney Freedberg, Jr., "Air Force Moves Aggressively on Lasers," *BreakingDefense.com*, August 7, 2015, available at <<http://breakingdefense.com/2015/08/air-force-moves-aggressively-on-lasers/>>.

<sup>28</sup> For both microwaves and lasers, there exist the possibility of countermeasures. In terms of microwaves, electronic hardening of the sUAS could provide protection. Against laser attack, countermeasures such as smoke might provide a level of survivability.

<sup>29</sup> Jason D. Ellis, *Directed-Energy Weapons: Promise and Prospects* (Washington, DC: Center for a New American Security, April 2015), available at <[www.cnas.org/sites/default/files/publications-pdf/CNAS\\_Directed-Energy\\_Weapons\\_April-2015.pdf](http://www.cnas.org/sites/default/files/publications-pdf/CNAS_Directed-Energy_Weapons_April-2015.pdf)>.

<sup>30</sup> Additionally, we especially see this commerciality phenomenon in the cyber domain.

<sup>31</sup> The authors want to thank Dr. Terry Pierce for providing the opportunity to observe the Department of Homeland Security's Center of Innovation, the operations on which the Commercial Adaptive R&D (CARD) concept is based. Dr. Pierce also provided valuable input into developing the CARD theory itself.

<sup>32</sup> John A. Alic, *Beyond Spinoff: Military and Commercial Technologies in a Changing World* (Cambridge: Harvard Business Press, 1992).

<sup>33</sup> Michael Casey and Robert Hackett, "The Top 10 Biggest R&D Spenders Worldwide," *Fortune*, November 17, 2014, available at <<http://fortune.com/2014/11/17/top-10-research-development/>>.

<sup>34</sup> Andrew Amato, "Drone Sales Numbers: Nobody Knows, So We Venture a Guess," *Dronelife.com*, April 16, 2015, available at <<http://dronelife.com/2015/04/16/drone-sales-numbers-nobody-knows-so-we-venture-a-guess/>>.



Marines with Bravo Company, 1<sup>st</sup> Battalion, 7<sup>th</sup> Marine Regiment, provide outboard security after offloading from CH-53E Super Stallion helicopter during mission in Helmand Province, May 1, 2014 (U.S. Marine Corps/Joseph Scanlan)

# Forensic Vulnerability Analysis

## Putting the “Art” into the Art of War

By Darryl Williams

*The supreme art of war is to subdue the enemy without fighting.*

—SUN TZU, *THE ART OF WAR*

Is warfare art or science? The debate, touched upon by Sun Tzu in the 6<sup>th</sup> century BCE, is still raging today. Most scholarly literature states that war is a combination of both art and science.

---

Lieutenant Colonel Darryl Williams, USAF (Ret.), is the President and Chief Executive Officer of Partnership Solutions International.

Many military scholars side with the argument that the planning and execution of warfare are art, but the tools used to wage war are science. However, in this technology-centric era of large data collection, asymmetric adversaries that employ emerging technologies, nation-states that leverage technology superior proxies, weapons that evoke a *Star Wars* familiarity, and a generation of warfighters that is more comfort-

able around instantaneous data flows than long-term incremental research, science is taking a more prominent role in warfare. For example, watch the current Department of Defense (DOD) recruiting videos. Except for the Marine Corps, which is still looking for *The Few, The Proud*, most if not all Service recruiting videos focus on technology (for example, jet fighters, cyber warriors, and space warriors).

In the kinetic arena, as weapons and weapons systems become more complex, planning and execution are moving away from art toward more reliance on science. In conflicts up to and including Vietnam, targeting was a matter of saturation to ensure destruction. However, in Operation *Desert Storm*, the public first witnessed precision-strike capabilities. Few who were in the military in 1991 can forget General Norman Schwarzkopf, USA, walking the press through the use of laser-guided bombs in Iraq, Tomahawk cruise missiles launched from ships in the Red Sea, and air-launched cruise missiles from bombers hundreds of miles from the conflict zone. In current conflicts, the integration of global positioning systems into bombs allows one B-2 to effectively prosecute 80 targets. In future conflicts, emerging directed energy weapons will enable the possibility of surgical attacks with little to no collateral damage. The bottom line is that kinetic warfare is becoming more about the science of the tools than the art of the application.

Even in the nonkinetic arena, warfare is becoming more science than art. It is all about the science behind the tools used. Executing a broad-brush, nonkinetic attack is easy and science-centric. If a country wants to take down another country's power grid or critical infrastructure, there are brute force nonkinetic tools to accomplish the task. However, the consequences are akin to General William T. Sherman's march to the sea. If the nondiscriminate attack is cyber based, the attacking country may inadvertently violate numerous sovereignties as it applies the tool. Ultimately, the negative collateral effects of a broad-brush, nonkinetic attack may be worse than the original problem that precipitated the attack.

However, in the realm of surgical, nonkinetic targeting, Sun Tzu's words are as applicable today as they were when written in 500 BCE. The key word is *surgical*. In such an attack, a specific target is affected, in a manner that may be nonattributable, for a predetermined duration that limits collateral damage. As stated by Sun Tzu, a successful surgical attack has the potential of subduing the

adversary without endangering the warfighter or innocent civilians. As this article demonstrates, surgical nonkinetic targeting requires an art form called forensic vulnerability analysis. With more than 20 years' experience as a forensic vulnerability analyst, targeteer, and warfighter, I can attest to the value of forensic vulnerability analysis in uncovering and targeting advanced terrorist planning, finding and fixing high-value assets, protecting the supply chain of national security systems, creating courses of action that maximize effectiveness and minimize negative collateral effects, and enhancing all areas of traditional campaign planning. However, its use and value have been kept in the shadows, and this lack of visibility is having dangerous consequences.

In discussions with Intelligence Community leadership, DOD planners at the combatant commands and Joint Staff, and leaders at many of the national laboratories, forensic vulnerability analysis is an art form that seems to be on the last stages of life support. In these organizations, the majority of remaining forensic vulnerability analysts are approaching retirement age. Compounding this problem is a lack of a training program to challenge, incentivize, and mentor the tech-centric next-generation warfighters to become forensic vulnerability analysts. The purpose of this article is to sound the alarm that the expertise necessary for successful surgical nonkinetic targeting is about to become organizationally extinct, and unless the problem is addressed, the art of war will become the science of war.

Forensic vulnerability analysis uses established auditing principles, due-diligence protocols, operational security survey methodologies, and exhaustive research of peer-reviewed documents to build awareness of obvious and non-obvious relationships and linkages. Then forensic vulnerability analysis leverages trusted relationships with recognized subject matter experts in industry, academia, and governments to transition and characterize the linkages into obvious and non-obvious vulnerabilities, identify and mitigate negative consequences, and establish a process to collect and measure effectiveness. As an aside, the

non-obvious vulnerabilities often produce the most favorable effects with the most limited negative consequences. Sometimes these vulnerabilities appear separate from the primary target by commercial mergers and acquisitions, joint ventures, layered boards of directors, government advisory service, venture capital, shell corporations, third-party integration, and so forth. From experience, the most critical vulnerabilities exist at 3 to 4 degrees of separation from the target. I have found that 4 degrees of separation from the target of interest usually encompass the majority of critical vulnerabilities.

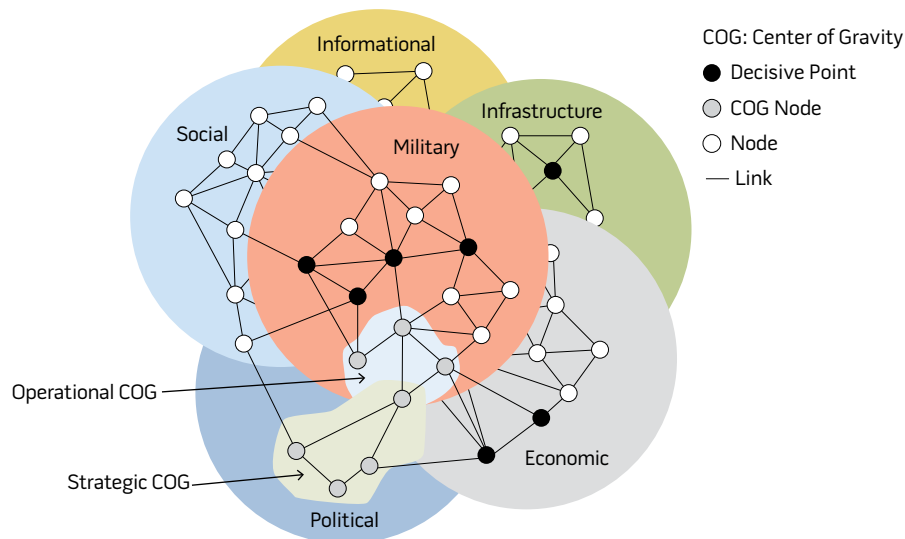
For those unfamiliar with the concept of degrees of separation, consider this scenario. A targeteer is attempting to discover a critical vulnerability in Company V, which produces a weapons system that could jeopardize U.S. national security. In the production of the weapons system, Company V receives electrical power from a hydroelectric system owned by Company W (1 degree of separation). The hydroelectric system uses turbines supplied by Company X (2 degrees of separation). The turbines are controlled by an electrical management system supplied by Company Y (3 degrees of separation). Company Y subcontracts the development of the configuration files to Company Z (4 degrees of separation). This analysis of linkages is accomplished not only for the production process, but also for the leadership, supply chain, financial, geopolitical, and cyber processes. Once these relationships are known, subject matter experts empower the targeteer so that a surgical nonkinetic attack against Company Z ripples up to Company V, accomplishing the national security objective.

In DOD capstone documents Joint Publication (JP) 3-0, *Joint Operations*, JP 2-0, *Joint Intelligence*, and many other joint publications and Service planning documents, the concept of a target system of systems is described verbally and portrayed graphically. Figures 1 and 2 from JP 2-0 portray the system-of-systems concept.

The figures portray a linear relationship matrix. Once the relational linkages

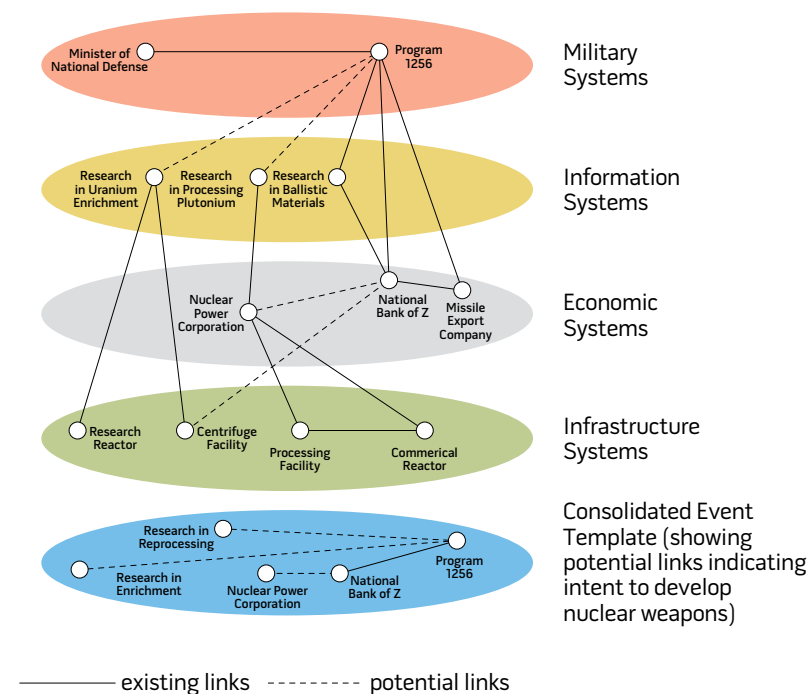
## Figure 1. Identifying Centers of Gravity

Source: Joint Publication 2-0, IV-14.



## Figure 2. Systems-Oriented Event Template

Source: Joint Publication 2-0, IV-15.



are known, targeting is accomplished to elicit a desired and measurable effect toward achieving the stated campaign objective. The system-of-systems concept is not new. In World War II, the Allies targeted ball-bearing plants in Schweinkurt, Germany, to affect

German aircraft production. During Operation *Desert Storm*, Iraqi power plants were attacked to negatively affect Iraqi defensive capabilities. The system-of-systems concept remains valid; however, the world is more complex now than at any time in history.

In today's interconnected, multinational world, the current DOD figures do not adequately portray reality. If the traditional, linear relationship methodology is used to target in a complex, interconnected, multinational world, the targeteer has the likely possibility of providing the joint force commander with courses of action (COAs) built on incorrect assessments of risk versus effectiveness. One reason for an incorrect assessment is that traditional nodal analysis defines criticality of a node via the number of linkages and analysis out to 1 to 2 degrees of separation. For example, if Company V has two critical nodes, one node with 100 linkages and one node with 2 linkages, common knowledge dictates that the node with 100 linkages must be the most critical. However, imagine that the 100 links were employees linked via social media, and the other nodes 2 links were actually the leadership and command and control networks. Now which node is more critical?

The underlying problem is that to be effective in a surgical nonkinetic strike, the targeteer needs to realize that the system of systems is a culmination of multinational, multilinked, multitiered, and non-obvious sub-targets. All that the world sees is the primary target, but in reality, the target is a culmination of numerous symbiotic units. For example, an aircraft is no longer produced at one plant. In the case of a next-generation fighter jet, there may be thousands of contractors and subcontractors all providing numerous components, any of which could jeopardize the aircraft if compromised. In the case of a power grid, there are thousands of substations, each with thousands of components that can be used to collapse the grid at any given time. Many of these subtargets are multinational. Many have nodes that are U.S. entities, which adds complexity in regard to authorities. Some of the nodes may cross established U.S. Government organizational areas of responsibility with conflicting authorities. Most nodes have critical information that is not accessible via established government collection capabilities.

The bottom line is that in a complex, interconnected world, a targeteer cannot accurately determine a critical target

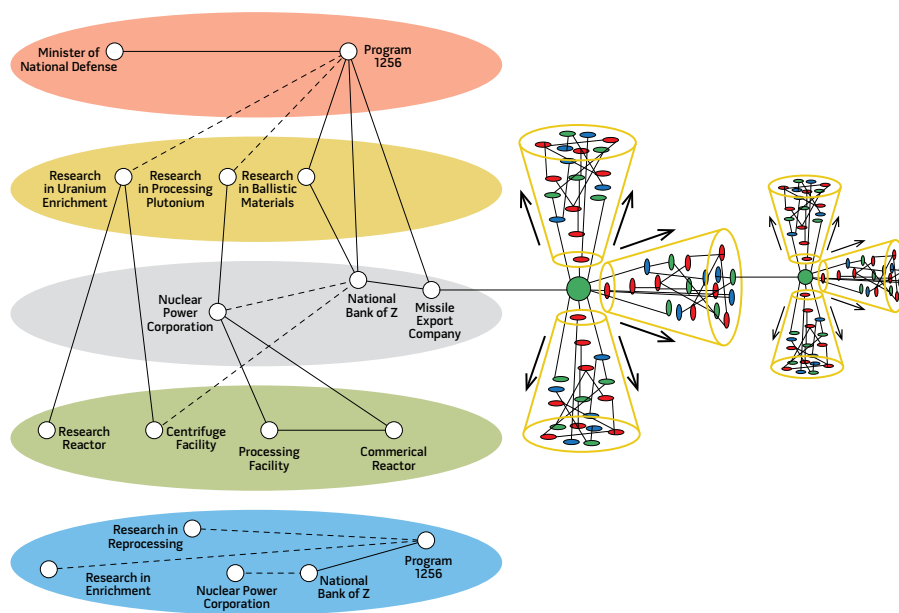


outside of a forensic vulnerability analysis that identifies both obvious and non-obvious relationships.

Figure 3 updates figure 2 to make it relevant for today's targeting solution. For the purpose of an example, the graphic identifies a missile export company in the economic tier. Traditional nodal analysis will look at the company and how it fits with the national security objective (for example, remove country X's capability to export nuclear ballistic missile airframes, warhead components, and related technology to country Y). Traditional analysis will look at the flow of money, company leadership, connectivity to other identified nodes, and so forth. The nonkinetic COA may be to infiltrate the shipping dispatch network and route the shipment of missiles to another location, thereby accomplishing the national security objective. However, this solution looks at a complex scenario through a simplistic lens and creates a logistics quagmire with potentially global negative effects. For example, if the attack is successful and the vessel transporting the missiles is rerouted, what about the other legitimate commerce on the transport vessel? That vessel is also scheduled to pick up additional legitimate cargo at the original destination (second cluster in figure 3). If the rerouting is successful, the uncertainty infused into the shipping industry drives up shipping insurance rates exponentially. This cost is handed off to the customer. Ultimately, these increased costs of business affect the ability of the multinational shipping company to conduct competitive commerce, which creates additional global issues (third cluster in figure 3).

From experience, senior government and DOD leaders understand these inherent complexities, which make them historically unwilling to accomplish surgical nonkinetic courses of action presented as part of a campaign plan. Even if these COAs religiously follow established planning doctrine to include intelligence preparation of the battlespace and are exhaustively wargamed, the commanders will know that a wargame of faulty assumptions creates faulty COAs.

**Figure 3. Interconnected and Global System of Systems**

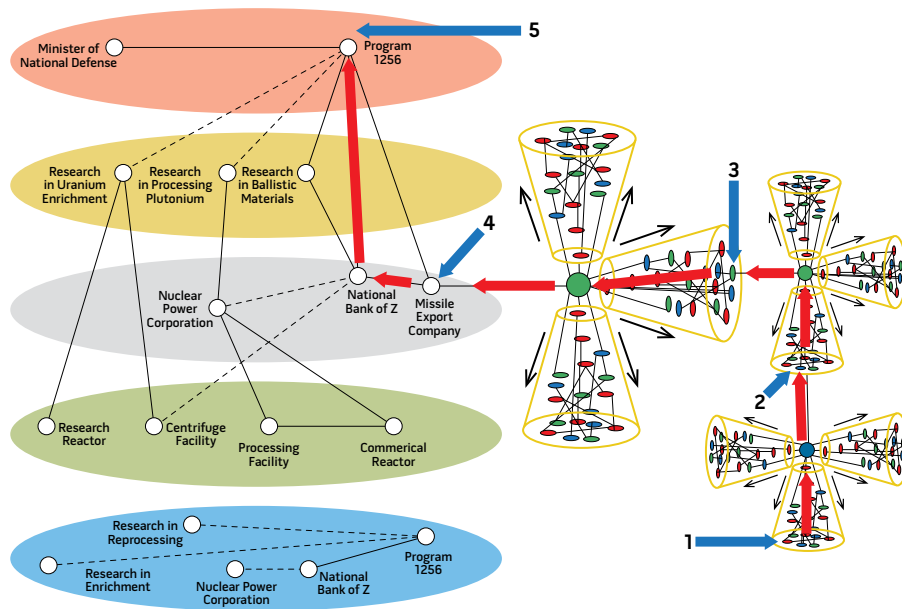


However, forensic vulnerability analysis is optimized to identify links and relationships that are usually hidden. In the previous missile export company example, the forensic vulnerability analysts would start where the traditional planners using the methodologies in figures 1 and 2 stop. From that point, the missile export company's leadership, corporate papers, and financial health would be analyzed. The leaders probably occupy leadership positions in the government, other corporate boards, or civic institutions. Each of those entities is analyzed. The banks that move the company's money are analyzed down to 4 degrees of separation. Analysis includes leadership and corporate linkages (such as joint ventures, subsidiaries, and shell companies). The shipping and dock worker companies are analyzed, as are the systems used for dispatch and all the components and companies that sell the components comprising the dispatch system. The company that transports the missiles to the dock is analyzed. The company that picks up the missiles at the desired end point is analyzed. Ultimately, the system-of-systems graphic that the traditional targeteer uses (figure 2) becomes the system-of-systems that the forensic vulnerability analyst creates.

Although complex in appearance, the links and nodes are characterized by critical and intimate information supplied via the forensic vulnerability analyst's trusted relationships in the private sector, academia, and government. Interactive wargaming provides the commander with an important "what if?" capability. Using the previous example of the missile export company, the forensic vulnerability analysis, subject matter expertise, and associated interactive wargame could produce a course of action as shown in figure 4.

The following are linked forensically: Country X's nuclear ballistic missile program (5) uses the named missile export company (4) to move airframes, warhead components, and critical technology to country Y. The leader of the missile export company has a trusted relationship with Freight Forwarder A (3), which uses an international bank (2) that has a branch in country Y. This bank (2) has a board of directors with one director who owns a freight insurance company (1), the same company that provides insurance for the export of the missile shipment. As a result of this forensic vulnerability analysis, targeteers could surgically attack the system in such a way that the export company does not receive the necessary letter of credit and insurance. Granted,

**Figure 4. Forensic Vulnerability Analysis Used in Surgical Nonkinetic Targeting**



harm's way. It is time for DOD and the Intelligence Community to make changes to strengthen this discipline and bring the art back into the art of war.

### Addendum: Forensic Vulnerability Analysis Case Study

The following is a real-world case study in which forensic vulnerability analysis was used to uncover the end stages of terrorist planning and was instrumental in validating and subsequently terminating the threat. In a touch of irony and future concern, the U.S. Government's forensic vulnerability analysis effort uncovered al Qaeda using a crude form of forensic vulnerability analysis as part of its targeting process.

**Overview.** On April 15, 2004, Osama bin Laden released an audiotape giving Europe 3 months to leave Islamic countries or face renewed attacks. By August, the 90-day deadline ended. However, based on information gleaned from a seized laptop, the U.S. Government and Intelligence Community were not looking at Europe but were preparing for an al Qaeda attack against one of five financial centers in the United States.

#### *Early Warning from Academia.*

A leader from an academic organization read an article in a newspaper from Milan, Italy. The author of the article was known to the academic (2 degrees of separation) and had a track record of unique insight into the workings of al Qaeda. In the article, the author stated that al Qaeda would not attack the United States. The attack would be against Europe to punish the countries for ignoring bin Laden's 90-day truce. He went on to state that his sources (3 degrees of separation) indicated that the attack would occur in one of five cities to include London, Rome, and Paris. Because the academic was part of a forensic vulnerability analysis trusted relationship network, this information was pushed by the academic to a DOD forensic vulnerability analyst.

#### *Early Warning from Industry.*

At the same time, a global investment banking leader, also in the trusted relationship network, notified the same

following the COA is not as flashy as launching a Tomahawk; however, the result still keeps country Y from receiving the nuclear ballistic missile system.

The cadre of forensic vulnerability analysts is dwindling due to retirement and routine attrition, and there are few to no replacements. A national lab leader recently concluded that forensic vulnerability analysis is an art form in danger of extinction. Unfortunately, as an art form, there is no present means to automate the forensic vulnerability analysis process. The problem is that much of the analysis is interpretation based on years of experience. In the future, an artificial neural network may be created that can successfully accomplish forensics. However, if such a network is created, it would still require experienced forensic vulnerability analysts to assist in the network's "learning."

The Department of Defense and Intelligence Community need to address the issue of a dwindling forensic vulnerability analyst cadre before it reaches a point of no return. There needs to be a dedicated training and recruiting effort to identify motivated warfighters. There needs to be a symbiotic relationship with academia and industry to provide unique mentoring opportunities for the trainees.

There also needs to be a dedicated career path that accounts for the longevity of specialization required to produce an expert forensic vulnerability analyst. The good news is that there are enough experienced analysts to act as instructors and mentors, and there are cooperative research and development agreements in place to leverage academia and industry. The bottom line is that this cadre death spiral can be rectified with little funding, but commitment to action needs to be made in the short term.

This article seeks to bring awareness to a unique specialty in the Department of Defense and Intelligence Community: forensic vulnerability analysis. It has stayed in the shadows since the birth of the Nation and has been instrumental in the success of many of the greatest U.S. campaigns. It is truly the "art" in the art of warfare. However, out of sight has also meant lack of attention. As the world becomes more tech-centric, there is an inadvertent momentum to make warfare more scientific. Unfortunately, the more technologically complex the world becomes, the more critical the art of forensic vulnerability analysis will be to protecting U.S. national security and safeguarding the warfighter in



Joint Cyber Analysis Course instructor at Information Warfare Training Command Corry Station helps high school student complete cybersecurity challenges during third annual CyberThon event at Naval Air Station Pensacola, January 21, 2016 (U.S. Navy/Taylor L. Jackson)

DOD analyst of interesting dialogue in financial blog sites. The banking leader stated that a particular financial blog produced a disturbing thread. A blogger posted a question asking how an entity could collapse a nation-state's economy. Other bloggers answered to forgo attacking structures and focus on attacking economic leaders. The bloggers went on to say that al Qaeda planned incorrectly when they attacked the World Trade Center; what they should have done was attack the stock exchange leadership and traders. (Note: This is a perfect example of the value of forensic vulnerability analysis [target finance leaders] versus traditional nodal analysis [target the building]). This blog thread demonstrated al Qaeda's crude attempt to accomplish forensic vulnerability analysis.

**Forensic Vulnerability Analysis.** The DOD analyst started an effort to determine if the academic thread was linked to the financial thread. An additional benefit of a trusted relationship network is that the network can find a singular

expert out to 4 degrees of separation. In this case, the analyst was directed to a finance expert familiar with the five European locations. He took part in a red team exercise hosted by the analyst. He was asked to put himself in the place of the terrorists and stage an effective attack against economic leaders. When asked, "In what European city would you stage the attack and how?" the leader responded that because of close-hold information that he was privy to, he would attack a "specified location" in London with either a chemical/biological weapon or a hijacked airliner. A successful attack in that area would cripple the United Kingdom for years.

**Corroboration from the Intelligence Community.** Intelligence databases were queried for the subject of al Qaeda in London—the "specified location"—and airliners. Message traffic identified an al Qaeda cell, but not much else was known. However, the DOD analyst was able, via non-obvious relationships and trusted subject matter expertise, to link the

academic information, business information, expert red team, and intelligence traffic. The result was actionable intelligence with increased fidelity and probable intent. The complete forensic vulnerability analysis process took 48 hours from initial message to research completion.

**Actions Taken.** The data, forensic nodal analysis, and corroborating intelligence were given to the United Kingdom liaison at DOD. In post-event talks in London between the United Kingdom's cabinet secretariat, the ministry of defense, security services, the Joint Terrorism Analysis Center, the DOD analyst, and the banking leader, it was learned that the al Qaeda unit members were arrested before they could execute their plan. Of note, the al Qaeda unit was known to the British authorities and they were actively monitoring the unit's activities. The forensic vulnerability analysis added fidelity to the United Kingdom's case for action. Information learned via interrogation confirmed the findings of the forensic vulnerability analysis. JFQ



Plane captain cleans canopy of EA-6B Prowler assigned to Electronic Attack Warfare Squadron 139 on flight deck of USS *Ronald Reagan*, Philippine Sea, June 19, 2006 (U.S. Navy/Kevin S. O'Brien)

# Operational Graphics for Cyberspace

By Erick D. McCroskey and Charles A. Mock

*The growth of any discipline depends on the ability to communicate and develop ideas, and this in turn relies on a language that is sufficiently detailed and flexible.*

—SIMON SINGH, *FERMAT'S ENIGMA*

*To promote interoperability at the information level within the area of joint military symbology, it is necessary to define a standard set of rules for symbol construction and generation to be implemented in C2 [command and control] systems.*

—JOINT MILITARY SYMBOLOGY

A sergeant looks at an arrow marked in grease pencil on a laminated map and knows that a machine gun position lies ahead. The large projection screen showing a map with a blue rectangle encompassing an oval gives the joint task force commander assurance that a tank battalion defends key terrain. A picture is worth a thousand words.

Complex subjects—mathematics, chemistry, physics, even highway driving—have specialized sets of symbols that convey information and understanding more quickly than text alone can do. Symbols have been part of military tactics, operations, and strategy since armies became too large for personal observation on the battlefield. In joint military operations, it is crucial to have a set of common symbols familiar to all users. They are especially useful to establish a common understanding across a user population with widely varying knowledge, experience, and Service backgrounds. The Department of Defense (DOD) established the newest warfighting domain via doctrinal guidance 8 years ago, yet cyber warriors still lack a coherent set of symbols that allow them to convey the intricacies of cyber warfare to the joint warfighting community. The inability of cyber warriors to easily express operational concepts inhibits the identification of cyber key terrain, development of tactics and strategies, and execution of command and control.

DOD has a standard for joint military symbology, MIL-STD-2525D, *Joint Military Symbology*, which provides a set of cyberspace symbols in an appendix. However, these symbols display cyber effects and network nodes only in the physical domain and are unable to portray cyber warfare in the logical and persona layers of cyberspace. The Institute for Defense Analyses provides analytical support for the director of the Operational Test and Evaluation

Cybersecurity Assessment Program, which evaluates cyberspace defensive operations during major exercises. To convey the operational context and importance of offensive and defensive cyber actions, we have developed a symbol set that is compliant with MIL-STD-2525, logically consistent, and capable of displaying the nuances of cyberwarfare to warfighters from all domains.

### Why Graphics?

The primitive state of cyber operational graphics, and the resulting lack of effective communication between cyber and physical domain warriors, deemphasizes operational campaign design and the application of the principles of war in cyber operations. This increases the likelihood that physical domain warfighters will accept dangerous risks because they have little conception of what is really happening on their networks. In many ways, cyber units that are composed predominantly of governmental civilians and contractors resemble medieval mercenary artillery companies—formed to provide a necessary technical function, but not really considered soldiers. As artillery became more powerful, new tactics followed, and artillerymen became co-equal members of the total force. We are seeing the same evolution in cyber, as our technicians evolve into warfighters.

Cyber organizations do not lack for symbols and graphics—network diagrams are ubiquitous—but these symbols do not conform to joint warfighting doctrine. A firewall needs to be recognized as a fortification. A honeypot *is* an ambush site or a delaying obstacle in cyberspace. Scanning *is* reconnaissance, and networks *are* areas of responsibility. Cybersecurity service providers (CSPs) and enterprise operations centers are cyber defense battalions, brigades, or higher. Offensive cyber mission teams conduct raids, strike targets, and execute active defense missions using preemptive attacks. It is no longer just the Internet; it is the battlefield. Militarizing cyber symbols will give the cyber warrior insight into the parallel and analogous activities performed in other domains.

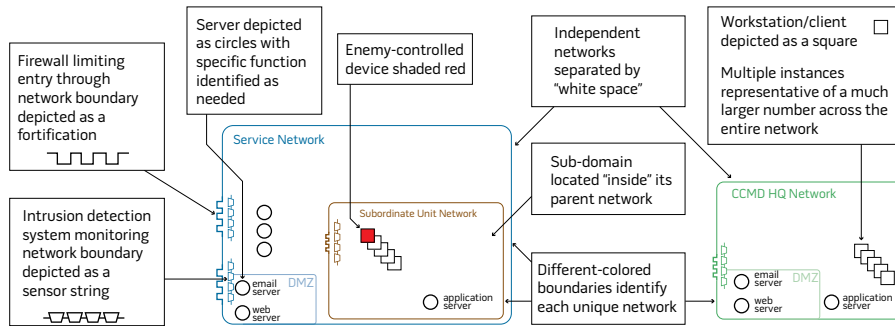
Victory in a cyber-contested environment will come at an increased cost in time, material, and manpower. The U.S. Navy commands the seas and the Air Force has controlled the skies since World War II. Technological and tactical prowess give the Army and Marines a clear edge against all comers. Only in the cyberspace domain is the U.S. military hard pressed to defend itself, let alone the Nation. This is a vulnerability that adversaries will certainly seek to exploit. Yet many non-cyber military leaders have only a surface understanding of the implications. Militarization of cyber symbols will allow joint commanders to understand just what is happening in the cyber fight. The general might be unclear on what “Mimikatz” is or how it got through the firewall, but he will intuitively understand red arrows bypassing his fortifications and driving deep into his cyber key terrain. Commanders will soon learn to discern which cyber-related decisions are risky and which are not. The cyber battle, currently fought apart from the land-sea-air battle, must and will gradually be integrated into joint operations as doctrine evolves.

Doctrine is the ultimate beneficiary of cyber symbols that conform to a joint standard. Cyber warriors already know the basic tactics to secure the battlefield, but an inability to visualize the battle hampers creation of a nuanced flow of cyber combat. At the opposite end of the spectrum, Joint Publication (JP) 3-12, *Cyberspace Operations*, brought some order to cyber command and control, but the paucity of operational doctrine has left a gulf between the tactical and strategic. With proper symbols, concepts can be developed, presented, understood, and evolved by the joint community. Standards can be created—for example, how many defenders are necessary for 50,000 accounts? Basic military precepts such as tempo and attrition can be addressed in a cyber context. Operational requirements can be identified, and the systems and equipment needed to meet that need can be acquired. For cyberspace to truly become a warfighting domain, with all that entails, development of symbols that conform to joint standard is a necessary first step.

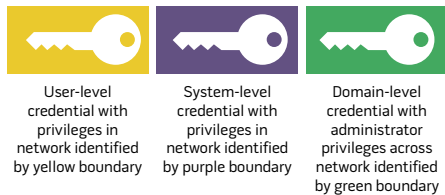
---

Colonel Erick D. McCroskey, USAF (Ret.), and Major Charles A. Mock, USMC (Ret.), are Research Staff Members in the Operational Evaluation Division at the Institute for Defense Analyses.

**Figure 1. Cyberspace Terrain Description: Networks and Common Features**



**Figure 2. Notional Cyber Credential Icons**



**Terrain Graphics**

Terrain is the fundamental medium for military action, in cyberspace as well as in the land, sea, and air domains. How terrain affects operations is different in all domains. JP 3-12 divides cyberspace into three layers: the physical, logical, and persona.

The physical layer is the hardware, located in the physical domain, on which the other two layers exist. The physical layer is not cyberspace terrain itself. Symbols for physical equipment already exist in MIL-STD-2525D and are not addressed here.

The logical layer is where cyber terrain exists, and the primary cyberspace terrain feature is the network, a collection of devices that implement applications, services, and data stores. It is often governed by Internet protocol (IP) ports and addresses accessed through a router. Networks are the cyberspace equivalent to areas of operations in the physical domain, and their very existence is provisioned by assigned Domain Accreditation Authority, which issues policy guidance and exercises some degree of command and control over subordinate units within the mission category of

DOD information network operations (DODIN ops). When protected by a firewall and monitored by intrusion-detection services at ingress points, a network becomes fortified and has a sensor line; when guarded by cybersecurity service providers and local cyber defenders (as prescribed in DOD Instruction 8530.01), it is analogous to the most common command and control area designation: the operational area (OA).

We choose to depict individual networks by the devices they comprise with a unique boundary line that represents the extent of the IP address space within it (see figure 1). For clarity, we typically depict only sufficient numbers of devices necessary to describe the planned or observed cyberspace operations, or to convey understanding of the nature of the terrain. For instance, if only one device out of hundreds on the network is attacked, we may choose to show that device alongside a half-dozen others, often with a note that the small number of devices depicted is representative of many more. We also choose to use unique color-coded boundaries for each network to enable quick understanding of the terrain because relatively few unique networks are typically required to depict a cyberspace battle and because alphanumeric designations defining the boundary with “adjacent” areas, as is typically done in the physical domain, make no sense. However, a unique alphanumeric designation for a network could certainly be used as a label to identify its boundary.

Cyberspace terrain is unique in that it is completely manmade, and distance is

measured in “hops” between computers rather than in kilometers—time and space have different relationships and affect operational decisions differently than they do in the physical domain. Cyberspace terrain is also changeable on short timescales. If you do not like how the enemy is using your terrain, you can simply change it by disconnecting from the network or shutting down vulnerable devices. Because of the nature of cyberspace, the distance between, and the relative positioning of, unique independent networks has little meaning in operational graphics depictions. However, the relationships between networks, such as where one is a sub-domain of another, are important, so we depict subdomains as existing completely within their parent networks.

Devices in cyberspace generally function simultaneously as terrain features on which forces maneuver and as installations (which provide necessary supply, transportation, command and control, defensive, surveillance, or other warfighting functions); thus, they have no clear analogies in the physical domain. We adopt common network diagram symbols in simplified form depicting an individual workstation or client as a square and a server as a circle. However, we depict two specialized devices (and the functions they perform) that are nearly always present in cyber battles with unique symbols: the firewall is represented as a fortification, and the intrusion detection equipment and services are represented as a string of sensors.

Similar to its physical counterpart, a cyberspace OA can be secured, contested, or captured. However, unlike in the physical domains, where control is often contested but never truly “shared” during typical combat operations, cyber OAs can experience “dual control” when an adversary has gained credentials that provide access to the terrain—servers, applications, and data stores—within the OA without the defenders being aware of the compromise. This situation is analogous to insurgency operations, in which a guerrilla unit operates clandestinely in the shadow of the occupying unit. Actual capture of a complete cyber OA is rare but can happen when the elements of the physical layer fall into enemy hands surreptitiously and the

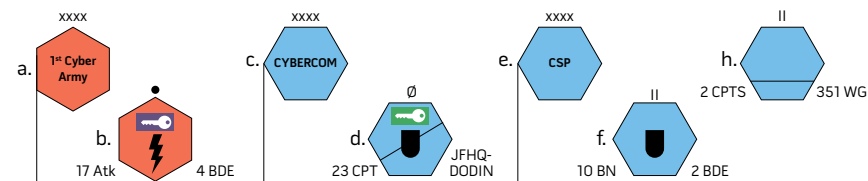
defenders do not realize that they ought to sever the connections between the OA and the rest of the network—a prime mission for special forces. Red shading represents devices that have fallen under enemy control in some way. In some instances, red shading may be used to represent enemy control over an entire network.

### Persona and Credential Graphics

The persona layer is the means by which personnel and units operate in cyberspace. JP 3-12 rightly asserts that the cyber persona layer requires a higher level of abstraction, but the publication introduces confusion when it states that the persona layer consists of people actually on the network. People do not exist in cyberspace, of course. Accounts and their associated credentials (usernames, passwords, Common Access Cards, personal identification numbers, and so forth) are the primary cyber entities that operators use to execute administrative actions, domain control, user activity, printer access, or any number of function-related activities. While we tend to think of accounts as being people, it is more logical to think of accounts in terms of cyber equipment used by operators existing in the physical domains. For example, in the air domain, a pilot (the operator) uses an F-22 (a piece of equipment) to conduct a variety of air superiority missions; similarly, a network user account is a piece of cyber equipment that allows the operator to conduct email, use a Microsoft Office application, or communicate with other accounts. The difference is that the F-22 operator is physically paired with his equipment in the air domain itself, whereas the cyber operator resides in the physical domain (where the physical layer of cyberspace exits) and conducts his mission in the cyberspace domain via the logical and persona layers, “looking in from the outside.” Cyber units thus have a foot in two domains: the living operators and physical layer hardware in one domain, and the mixed types of accounts, credentials cyber actions, and missions in another.

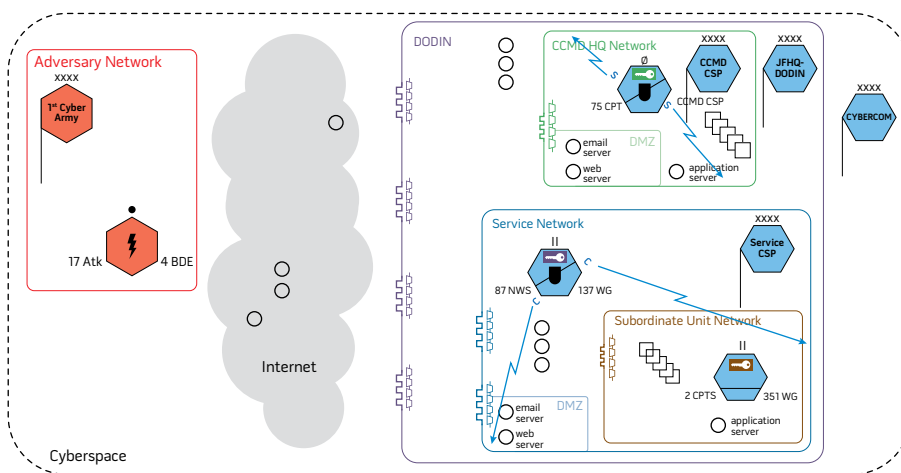
Credentials are the keys to the cyber equipment and associated accesses and

**Figure 3. Notional Cyber Unit Icons**



Key: a. Adversary headquarters (HQ); b. Adversary squad-level offensive cyberspace operations unit with captured system admin credentials; c. U.S. Cyber Command HQ; d. Friendly Defensive Cyberspace Operations (DCO) unit with reconnaissance capabilities that has been granted domain administration credentials/authorities; e. Friendly cybersecurity service provider HQ; f. Friendly DCO unit; h. Friendly DODIN ops cyber unit

**Figure 4. Notional Cyberspace Terrain Showing Boundaries, Units, and Defensive Tasks**



privileges. Adversary control of a user-level account is damaging because it allows the enemy to traverse the OA in the guise of a friendly operator. An adversary who gains credentialed access to a domain administration account is able to use the privileges associated with this account to control all the key terrain—accounts, servers, data, and applications—in that OA. Different key symbols reinforce this point: yellow for user-level, purple for system-level, and green for domain-level privileges. A colored border around the key indicates the domain or network to which the privileges pertain (see figure 2).





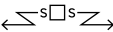

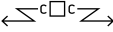






### Unit Graphics

MIL-STD-2525D prescribes the use of specific frames for icon-based symbols to depict the identities of units operating in the land, sea, air, space, and subsurface physical domains. It does

not prescribe a unique frame to identify units when depicting operations solely in cyberspace (that is, the logical and persona layers). We adopt a regular hexagonal frame to depict units in cyberspace. We use standard shading conventions for friendly, neutral, hostile, civilian, and unknown standard identities and rotate the hexagons by 30° to depict hostile units (figure 3).



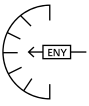

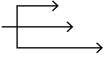



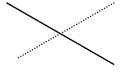
Icons, defined in MIL-STD-2525D as “the innermost part(s) of a symbol which provides an abstract pictorial or alphanumeric representation of units, equipment, installations, activities, or operations,” must necessarily represent the unique nature of cyberspace units. Cyberspace personnel receive training for particular missions using specialized software, hardware, and network “equipment.” However, the generally applicable nature of the equipment, techniques, and

**Table. Adaptation of Tactical Task Graphics to Cyberspace**

| Tactical Task                   | Operational Graphic  | Doctrinal Description*   | Potential Use in Describing Cyberspace Operations   |
|---------------------------------|--|--|---|
| Actions by Friendly Force       |  |  |   |
| Attack by fire                  |   | The use of direct fires, supported by indirect fires, to engage an enemy force without closing with the enemy to destroy, suppress, fix, or deceive that enemy.  | Overt actions where an origination (or interim relay) point can be determined, such as distributed denial-of-service attacks, broad intrusive scans, where these actions create the intended effect on the target.  |
| Breach                          |   | Break through or establish a passage through an enemy defense, obstacle, minefield, or fortification.  | Noncredential-based access (penetration through a firewall, using an exploit or hacking tradecraft).  |
| Bypass                          |   | Maneuver around an obstacle, position, or enemy force to maintain the momentum of the operation while deliberately avoiding combat with an enemy force.  | Credential-based access (use captured credentials for login).   |
| Clear                           |   | Remove all enemy forces and eliminate organized resistance within an assigned area.  | Comprehensive scans and forensics, removing all malware and adversary points of presence and external connections.  |
| Control                         | n/a  | Maintain physical influence over a specified area to prevent its use by an enemy or to create conditions necessary for successful friendly operations.   | Standard cybersecurity mission to protect a domain, typically assigned to a cyber security practitioner (CSP).  |
| Counter-reconnaissance (Screen) |   | Provide early warning to the protected force.  | Detection activities on a boundary or domain.   |
| Counter-reconnaissance (Guard)  |   | Protect the main body by fighting to gain time while also observing and reporting information and preventing enemy ground observation of and direct fire against the main body. Units conducting a guard mission cannot operate independently because they rely upon fires and combat support assets of the main body. | Domain-wide detection and hunt-type activities by a cyber protection Team or local defensive unit, augmenting the capabilities of a CSP.  |
| Counter-reconnaissance (Cover)  |   | Protect the main body by fighting to gain time while also observing and reporting information and preventing enemy ground observation of and direct fire against the main body.  | Domain-wide detection, hunt, and reposturing of defensive boundary controls by a CSP.   |
| Exfiltrate                      | <br>(No symbol exists. Symbol shows the flow of exfiltrated data, a substantial deviation from the existing definition of this task.) | Remove Soldiers or units from areas under enemy control by stealth, deception, surprise, or clandestine means.   | Movement of data from its original location to a location under enemy control, typically by means of stealth, deception, or clandestine means.  |
| Occupy                          |   | Move a friendly force into an area so that it can control that area. Both the force's movement to and occupation of the area occur without enemy opposition.   | Deployment of a cyber protection team to a domain in advance of suspected adversary activity.   |
| Retain                          |   | Ensure that a terrain feature controlled by a friendly force remains free of enemy occupation or use.  | Defense of a network device or domain to prevent any adversary access.  |
| Secure                          |   | Prevent a unit, facility, or geographical location from being damaged or destroyed as a result of enemy action.  | Defense of a network device or domain to prevent an adversary from making any changes to data or functionality.   |
| Seize                           |   | Take possession of a designated area by using overwhelming force.  | Gain control of a device, network, data, or credentials. In cyberspace, two opposing forces may have simultaneous control of any or all of these assets.  |
| Support by fire                 |   | A maneuver force moves to a position where it can engage the enemy by direct fire in support of another maneuvering force.   | Overt actions where an origination (or interim relay) point can be determined, such as distributed denial-of-service attacks, broad intrusive scans, and where these actions are designed to set the conditions for success for the primary attack actions. |



**Table. Adaptation of Tactical Task Graphics to Cyberspace**

| Tactical Task          | Operational Graphic   | Doctrinal Description*   | Potential Use in Describing Cyberspace Operations  |
|------------------------|---|--|--|
| Effects on Enemy Force |   |  |  |
| Block                  |    | Deny the enemy access to an area or prevent the enemy's advance in a direction or along an avenue of approach.<br><br>Also an obstacle effect that integrates fire planning and obstacle efforts to stop an attacker along a specific avenue of approach or prevent the attacking force from passing through an engagement area. | Use or modification of blacklists, whitelists, access control lists, routing policies, credentials (username-password pairs, or machine-issued), or filters on firewalls, domain name servers, domain controllers, Web servers, email servers, or others to prohibit or terminate access based on specific criteria.   |
| Canalize               |    | Restrict enemy movement to a narrow zone by exploiting terrain coupled with the use of obstacles, fires, or friendly maneuver.   | Use of routing policies, honeypots/honeyports/honeynets, or other defensive techniques to direct potential adversary traffic to desired network locations.   |
| Contain                |    | Stop, hold, or surround enemy forces or to cause them to center their activity on a given front and prevent them from withdrawing any part of their forces for use elsewhere.  | Not strictly possible in cyberspace, since forces exist as a function of effort being expended. However, could be used to indicate quarantine of malware or emails.  |
| Destroy                |    | Physically render an enemy force combat-ineffective until it is reconstituted. Alternatively, to destroy a combat system is to damage it so badly that it cannot perform any function or be restored to a usable condition without being entirely rebuilt.   | Deleting all files from a server, flashing basic input-output system or firmware, or causing physical damage to industrial control systems.  |
| Disrupt                |    | Integrates direct and indirect fires, terrain, and obstacles to upset an enemy's formation or tempo, interrupt the enemy's timetable, or cause enemy forces to commit prematurely or attack in a piecemeal fashion.  | Interrupting connections periodically, enforcing time limits on sessions, or actions that require an enemy to repeat previous steps, upset an enemy's tempo, interrupt the enemy's timetable, or cause the enemy's efforts to proceed in a piecemeal fashion.  |
| Fix                    |  | Prevent the enemy force from moving any part of that force from a specific location for a specific period.   | Not strictly possible in cyberspace, since forces exist as a function of effort being expended, but used to indicate actions that require an enemy to focus effort to restore function (for example, reboot a domain controller or data server following an induced system crash); to expend much greater effort than planned to obtain an objective (for example, consuming attacker resources using a realistic honeynet); or to refrain from using capabilities for fear of detection (for example, refrain from activating implants because of increased random scans for active malware). |
| Interdict              |  | Prevent, disrupt, or delay the enemy's use of an area or route.  | Denial-of-network (data transport) services, or limiting access to services.   |
| Isolate                |  | Requires a unit to seal off—both physically and psychologically—an enemy from sources of support, deny the enemy freedom of movement, and prevent the isolated enemy force from having contact with other enemy forces.  | Removal of a device infected with malware from the network, moving a phishing email from the server to a forensics sandbox.  |
| Neutralize             |  | Render enemy personnel or materiel incapable of interfering with a particular operation.   | Any action taken against another cyberspace unit that prevents it from using its offensive or defensive capabilities (for example, interrupt the sensor feeds from a target domain to the responsible cyber defense unit).   |

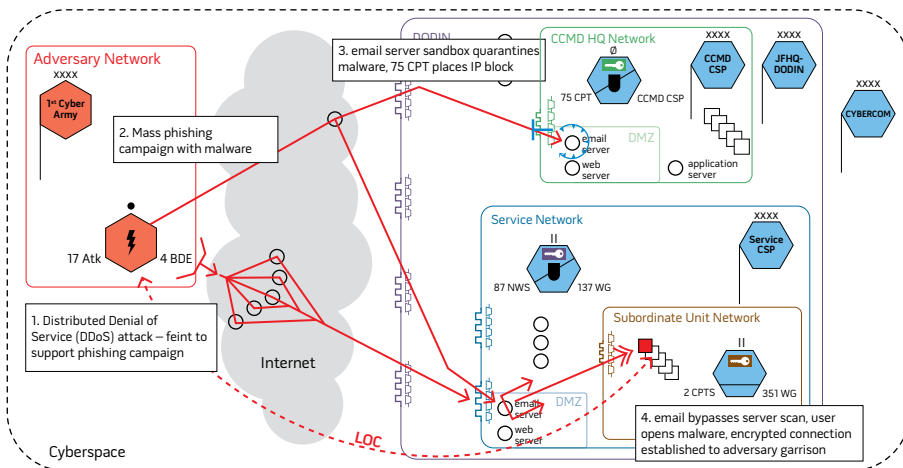
\* As described and depicted in various DOD sources, including MIL-STD-2525D, *Joint Military Symbolology*, June 10, 2014; Field Manual (FM) 1-02/Marine Corps Reference Publication 5-12A, *Operational Terms and Graphics*, February 2, 2010 (incorporating Change 1); FM 3-90-1, *Offense and Defense*, vol. 1, March 2013; FM 3-90-2, *Reconnaissance, Security and Tactical Enabling Tasks*, vol. 2, March 2013.

core technical skills allows cyber personnel and units to perform diverse functions (for example, reconnaissance, identification friend or foe, command and control, creating or modifying terrain features,

engaging targets, occupying terrain) that are often required to execute typical missions, whereas units in the physical domain tend to have a more specialized set of functions based on their training

and equipment. Although cyber units may be equipped with specific “platforms” and trained for unique missions at the lowest tactical levels, in general the diversity of the functions that cyber forces

**Figure 5. Sequential Actions in the Initial Adversary Assault: A Feint, Blocked Phishing Attack, Successful Bypass of Defenses That Gains Control of Friendly Terrain**



are capable of prohibits unique categorization by unit type based on specific equipment or mission as is typical in the physical domains (for example, infantry versus mechanized infantry versus armor battalions, F-22 versus E-3 versus KC-135 squadrons). Instead, we use symbols that identify cyber units based on which of the three general mission categories from JP 3-12 they typically perform: offensive cyberspace operations (OCO), defensive cyberspace operations (DCO), or DODIN ops. A lightning bolt identifies OCO units, a shield icon identifies DCO units, and existing support unit iconography identifies DODIN ops units.

Cyber warriors often regard detection as the most critical of their tasks, and individual cyber units are often assigned “detect” as a priority mission and are specially equipped and trained to execute it. Cyber units performing the detect mission are depicted with a diagonal slash across the frame, similar to the use of a slash to denote “reconnaissance” capabilities in the physical domains.

Cyber units are identified by the echelon command level to which they belong, just as units in the physical domain are, but the reader should take care when inferring echelon-level missions, capabilities, and resources, since these are not directly comparable to units in the physical domain. Physical domain units at the same echelon level can exhibit substantial

variation in their numbers of assigned personnel and equipment, as well as in their capabilities and “reach” (for example, an infantry battalion may have 500 persons assigned and fight on a front of perhaps a half-mile in extent, while a fighter squadron may have 150 persons and 24 aircraft assigned and fight within a 500-mile radius of its base). The variation between cyber and physical units within the same echelon, however, tends to be even greater. For example, a cyber battalion or squadron primarily responsible for *global* detection and response efforts for an entire service network might have 300 persons assigned. Additionally, there tend to be substantially fewer units at any given echelon within the total cyber force structure. We choose to adopt the existing echelon representation (used primarily in representing land force units) and apply it using the official designations of cyberspace units, with cyber protection teams representative of the lower echelons of friendly cyber forces typically portrayed, and U.S. Cyber Command as the top echelon.

Cyberspace commanders would benefit from decision graphics showing unit combat effectiveness, specific platform equipment and capabilities, and task organization composition, similar to those used tactically and operationally in the physical domains, but we defer this level of detail until cyberspace doctrine

matures to the point that these can be useful in the planning and execution of battles and campaigns.

## Mission Graphics

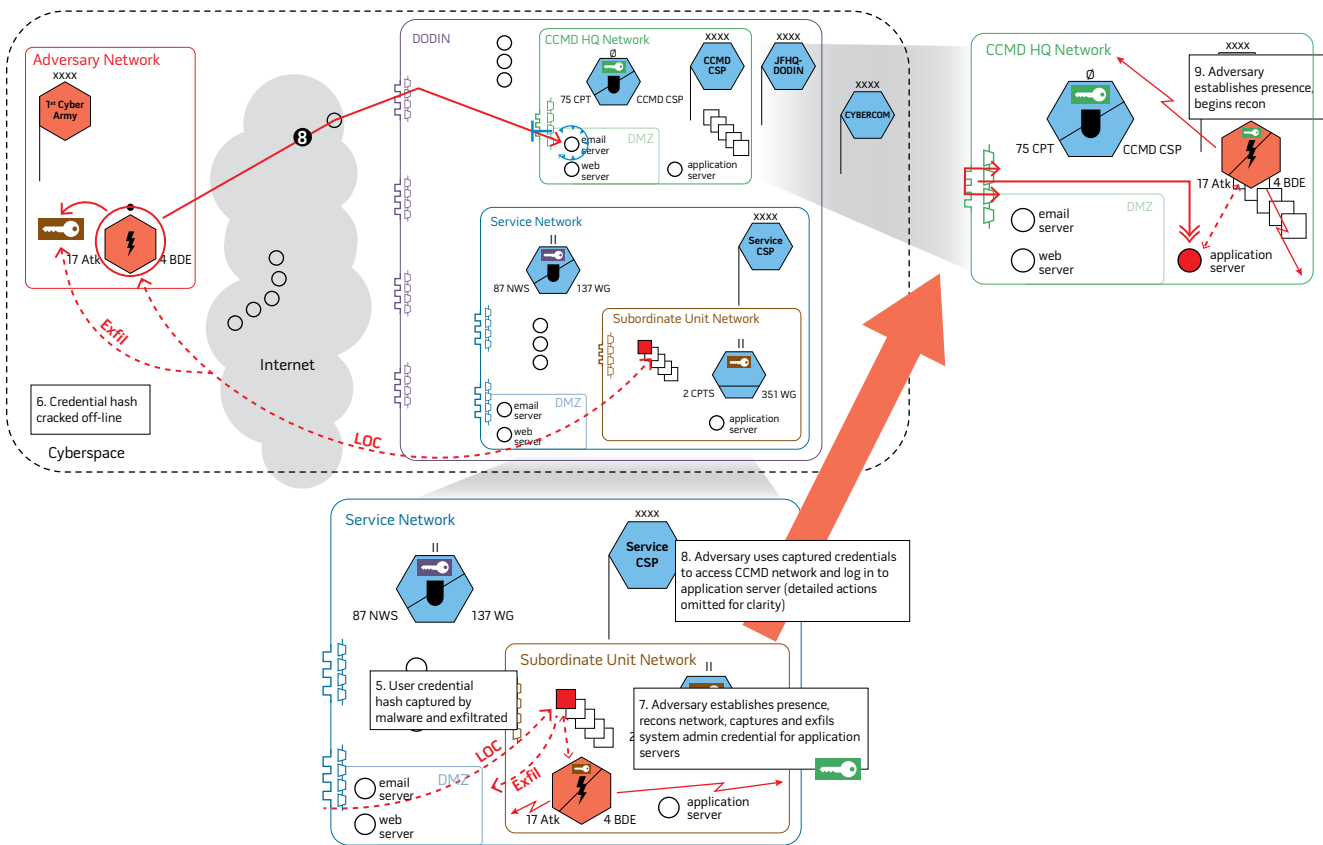
Although some graphic control measures used in the land domain (such as phase lines, assembly areas, fire support coordination measures, and check-points) may not be useful in describing operations in cyberspace, others can be readily adapted for the purposes of planning and maintaining situational awareness. In addition to the potential utility of adapting general offensive graphics (axis of advance, direction of attack), general defensive graphics (fortified line for firewall, sensor outpost for monitored intrusion detection device/system), and supply graphics (main supply routes or lines of communication for data flows), the traditional definitions of tactical mission graphics can be modified to depict actions in cyberspace. Potential adaptations of these graphics to cyberspace are provided in the table.

Other tactical tasks potentially useful for describing cyberspace actions were omitted from the table for the sake of brevity or because no associated operational graphic exists: control, counter-reconnaissance (area security, local security), disengage, follow and assume, follow and support, defeat, and suppress.

## Putting It All Together

These basic building blocks allow portrayal of cyber battles in a straightforward manner and present the action to the joint warfighter in a familiar format. The symbol set is still small—units, terrain, command and control, attack vectors—but capable of providing insights the commander needs for a rudimentary situational awareness of the operational area. Combatant command J6s already understand why firewalls and sensors are ineffective once an adversary has gained credentials through phishing and poor password protection; battle maps with an attack arrow showing an enemy task force masquerading as friendlies and penetrating a fortification to pass undetected through sensors provide the joint force commander with

**Figure 6. Subsequent Adversary Actions on Friendly Terrain: Seizing of Credentials, Reconnaissance, and Lateral Movement Within and Between Networks**



an understanding—an enormous red flag signaling risk to his mission—that has been missing from the cyber portion of joint warfighting.

Figures 4, 5, and 6 depict the progression of a notional battle in cyberspace, from the initial assignment of defensive forces to their areas of responsibility, followed by the attacker’s preparatory reconnaissance operations, and culminating in the penetration of defenses and the attacker occupying defended territory and postured to conduct follow-on operations. The astute reader will notice the similarities to historical depictions of Civil War battlefields, which motivated the development of these graphics to clearly depict complex, sequential actions over extended durations.

## Conclusion

Cyberspace operational graphics will allow cyber planners and operators to convey mission-relevant information to

warfighters who are unfamiliar with the technical details of cyberspace. Military tasks, missions, and operations share commonalities regardless of the domain in which they take place, and leveraging warfighter familiarity with the common language that has evolved to describe them will enhance rapid understanding and decisionmaking.

The concepts presented here only scratch the surface of an extremely large problem. To date, there is little official recognition that the cyber community should even conform to joint symbology standards. Cyber symbols merit only 3 of the 885 pages of MIL-STD-2525D. If DOD intends to treat cyberspace as a warfighting domain, then standards must reflect that guidance. However, that is just the beginning.

Using operational graphics to describe cyberspace actions should lead to the identification of parallels and analogies in the physical domains that

could potentially be implemented in cyberspace operational doctrine. For instance, the doctrinal concepts of culmination and attrition that are critical to operational campaign design and execution in the physical domains may finally be examined fully for application in the cyber domain. Ultimately, the joint commander will have at his disposal a coherent body of operational doctrine and the accompanying graphics that will enable him to understand, plan, and fight the cyber battle. JFQ

The authors would like to extend their appreciation to Robert Soule and Dr. Shawn Whetstone from the Institute for Defense Analyses for their continued support and encouragement in developing these ideas, and to Dr. J. Michael Gilmore, Dr. Kenneth M. Crosswait, and Dan Burgess from Director, Operational Test and Evaluation, for recognizing the utility of cyberspace operational graphics, for their insightful feedback, and for their continuing challenge to us to improve the concepts.



Air traffic controller with 31<sup>st</sup> Marine Expeditionary Unit communicates with pilot of CH-46E Sea Knight helicopter with Marine Medium Helicopter Squadron 262 (Reinforced), 31<sup>st</sup> MEU, during multilateral NEO exercise, February 12, 2011 (DOD)

# The Need for a Joint Support Element in Noncombatant Evacuation Operations

By George K. Dixon

The U.S. Government's first duty is to protect and defend the citizens of the Nation. Loss of confidence in the government's ability and willingness to safeguard citizens can shift the public narrative and may

---

Colonel George K. Dixon, USAR, is a Battalion Commander in the U.S. Army Reserve.

even compel policymakers to alter strategic direction. Noncombatant evacuation operations (NEOs) from threatened areas overseas are therefore an important strategic matter, particularly in today's world of viral videos and globalized travel. The military elements tasked on short notice to plan and execute NEOs may not always fully appreciate these strategic implications.

A quintessential image from the Vietnam era is of U.S. helicopters plucking people off rooftops amid the fall of Saigon while panicked throngs of Vietnamese plea to get onboard. Another is the spectacle of evacuation helicopters being pushed off the decks of U.S. warships and into the sea. For many around the world, these images symbolize the failure and abandonment of U.S. strategy in Southeast Asia.

Another low point for the United States were the images of blindfolded Embassy staff being held hostage by Iranian revolutionaries and of burned U.S. rescue aircraft in the desert. The Iran hostage drama punctuated a crisis of confidence in political and military leadership during the 1970s. The failed rescue attempt in April 1980 reinforced doubts about U.S. military capability and led to a complete reorganization of U.S. Special Operations. This contributed to perceptions of strategic drift and malaise leading into the 1980 Presidential campaign.

President Ronald Reagan's fundamental theme was renewing confidence in America. He ordered the invasion of Grenada, vowing not to "wait for the Iran crisis to repeat itself, only this time, in our own neighborhood—the Caribbean."<sup>1</sup> Operation *Urgent Fury* evacuated 800 American medical students and toppled a communist-aligned regime. Grenada advanced Reagan's strategic objective to reverse the "Vietnam Syndrome"<sup>2</sup> and rebuild the credibility of U.S. power. But Grenada also uncovered serious gaps in the military's ability to operate jointly, leading directly to the Goldwater-Nichols Department of Defense Reorganization Act of 1986.

Military-assisted NEOs occur infrequently, but they carry enormous diplomatic, military, and national strategic consequences. Images of noncombatants in danger are powerful, and the audience is unforgiving. Doing NEOs successfully is even more imperative in a fully globalized, cellphone-enabled, viral-video world where cameras are everywhere and images spread instantaneously.

To maximize the success of such important missions, the Department of Defense (DOD) should create a new Joint Planning Support Element specifically for NEOs. Geographic combatant commanders (GCCs) could use this entity to augment their staffs during a NEO event. This Joint NEO Support Element would coordinate the strategic and operational aspects of NEOs and provide subject matter experts. GCCs should still designate a NEO joint force commander to retain overall military control, and they

would still provide the bulk of forces, lift, and planning within their areas of responsibility (AORs).

### Policy, Doctrine, and Practice

Diplomatic evacuation events occur quite often. From 1988 through October 2007, the Department of State conducted 271 authorized and ordered departures from overseas posts,<sup>3</sup> an average of nearly one every 3 weeks. Embassy or State Department personnel carried out the vast majority of these without military assistance. However, a mass evacuation or a hostile security environment can overwhelm Embassy and State Department capabilities, leading them to call for military assistance.

Withdrawing American citizens and diplomats from a foreign location has weighty strategic and political repercussions. An ordered evacuation signals an official U.S. Government determination that the host government can no longer guarantee the safety of foreign nationals and that staying in place is no longer worth the risk. It could further undermine the host region's economy, stability, and legitimacy and may forfeit the diplomatic, informational, military, and economic assets an American presence maintained.

The Department of State is always the lead Federal agency for "protection or evacuation of United States citizens and nationals abroad,"<sup>4</sup> including the "evacuation and repatriation of United States citizens in threatened areas overseas."<sup>5</sup> The senior U.S. diplomat in a country is a Chief of Mission or Ambassador and is the personal representative of the President of the United States with extraordinary decision authority over all U.S. Government operations in their assigned country. The Chief of Mission controls all U.S. Government personnel in that country except those assigned to a GCC. Military personnel at the Defense Attaché Office (DAO), Security Assistance Office, and Marine Corps Security Guard detachment are under the authority of the Chief of Mission, not the GCC.

A 1988 memorandum of agreement describes how DOD will support State

during an evacuation.<sup>6</sup> It establishes three policy objectives:

- protect U.S. citizens and designated other persons, to include their evacuation to relatively safe areas when necessary and feasible
- minimize the number of U.S. nationals subject to risk of death and/or seizure as hostages
- reduce to a minimum the number of designated noncombatants in probable or actual combat areas so that combat effectiveness of U.S. and allied forces is not impaired.

DOD Directive 3025.14, "Evacuation of U.S. Citizens and Designated Aliens from Threatened Areas Abroad," provides further guidance on supporting State overseas evacuations. It reiterates that the primary responsibility for NEOs is with State and the diplomatic Chief of Mission. But DOD and all combatant commands must plan and prepare contingency plans to support NEOs.

Military-assisted NEOs are exceptional in that the U.S. Ambassador, not the military commander, has responsibility for the overall operation. Embassy or State Department personnel coordinate overflight and landing clearances and designate marshalling areas and safe havens. But the military commander has responsibility for execution once military forces and equipment commence operations.<sup>7</sup> A NEO is always a unity of effort situation with overlapping responsibilities requiring intense coordination.

Military-assisted NEOs generally also involve multiple Services and sometimes coalition forces. The NEO joint force typically will insert a ground security element to control evacuation sites and marshalling areas; move evacuees by land, water, or air to a temporary safe haven; provide sustainment, administrative processing, communications, and safety to the evacuees at the temporary safe haven or follow-on destinations; and then either repatriate American citizens to U.S. territory or return them to the affected area once the crisis is over. Embassy or State officials maintain overall responsibility throughout all phases of NEOs, but the military must be prepared to step in at



Airmen from 86<sup>th</sup> Aeromedical Evacuation Squadron and Critical Care Air Transport team from Landstuhl Regional Medical Center load wounded Libyan fighter onto civilian aircraft for transport to local German hospital, October 29, 2011, Ramstein Air Base, Germany (U.S. Air Force/Chenzira Mallory)

any point to maintain operations start to finish.

Joint Publication 3-68, *Noncombatant Evacuation Operations*, is the current joint doctrine for NEO operations. The main thrust of the publication is the tactical aspects of NEOs, but it also includes discussion of interagency coordination, strategic communication, military deception, defense support to public diplomacy, information-sharing, geospatial intelligence, and use of psychological operations.

The Marine Expeditionary Unit (MEU) is routinely trained and certified for conducting NEOs in uncertain or hostile environments.<sup>8</sup> An MEU, if available, is the optimum tactical force. However, military-assisted NEOs often occur at times and places where an MEU is not nearby or available. Half of all military-assisted NEOs over a recent 20-year period were executed without an MEU.<sup>9</sup>

General purpose forces from any of the military Services may be tasked to execute NEOs, typically on short notice with no prior preparation.

An MEU also lacks the staff depth to handle operational- and strategic-level coordination during a NEO event. These planning and coordination duties therefore default to the joint force commander, GCC, or Service component staff. This is a problem because NEOs require rapid response and focus, often while other operations are under way elsewhere in the AOR. Assembling a new joint force headquarters (JFHQ) or diverting GCC or Service component staff during a crisis may hinder operations elsewhere or sidetrack the NEO.

By its very nature, a NEO requires bilateral coordination with the host nation. It frequently also becomes a multilateral, allied, or coalition operation. The North Atlantic Treaty Organization (NATO),<sup>10</sup>

United Kingdom,<sup>11</sup> Australia,<sup>12</sup> France,<sup>13</sup> and Canada<sup>14</sup> each has its own established NEO doctrine. The United States has mutual agreements with a number of countries to evacuate each other's designated persons in times of crisis. The Joint NEO Support Element should build and promote interoperability with the NEO doctrines, terminologies, and rules of engagement of potential mutual support partners. Combatant commands are unlikely to maintain the same familiarity with all potential NEO doctrines, especially from countries outside their AOR, leading to potential friction if multiple nations attempt evacuations concurrently.

### Case Studies

**Vietnam: Operation Frequent Wind, April 1975.** The United States maintained a large diplomatic presence following troop withdrawals from Vietnam in 1973. The American Embassy and

DAO in Saigon were the largest of any foreign post. Tens of thousands of American citizens, U.S. Government employees, contractors, business people, and family members remained in Vietnam.

The situation across Southeast Asia deteriorated rapidly throughout early 1975. The U.S. Air Force and Marines evacuated the U.S. Embassy in Phnom Penh, Cambodia, on April 12, 1975, in Operation *Eagle Pull* 5 days before that city fell to the Khmer Rouge. Meanwhile, North Vietnamese army units invaded the South and by mid-April were closing on Saigon.

During April 1975, the United States evacuated over 130,000 people by air and sea in the largest NEO in history.<sup>15</sup> U.S. Ambassador Graham Martin, hoping to negotiate a truce and reluctant to admit failure or to cause panic, delayed final Embassy evacuation as long as possible. By the time he did request evacuation, 16 North Vietnamese army divisions surrounded Saigon, the airport was closed by ground fire, and mobs of panicked civilians and communist “home guards” filled the streets, making movement almost impossible.<sup>16</sup>

Helicopter extraction was the only remaining option. During April 29–30, 1975, Marine helicopters lifted 1,373 American citizens and 5,595 Vietnamese and third-country nationals from the U.S. Embassy compound in central Saigon and the DAO compound at Tan Son Nhut airport. U.S. casualties included two Marines killed by indirect fire and two aircrew lost at sea. As the official after action report noted: “Trying more attractive options may result in execution decision being delayed until a worse case situation has developed.”<sup>17</sup>

#### ***Mogadishu, Somalia: Operation Eastern Exit, January 5–6, 1991.***

Operation *Eastern Exit* took place during Operation *Desert Shield* and just 2 weeks before the launch of *Desert Storm*. This created some complications. Military forces in theater were concentrated in the Persian Gulf and focused on preparing for major combat operations.

Most Westerners fled Somalia by late December 1990 due to the violent

anarchy caused by civil war. Ambassador James Bishop and a minimal Embassy staff remained into January hoping for an Italian-brokered ceasefire.<sup>18</sup> As the situation worsened, however, the Ambassador requested immediate evacuation.

Confusion and ongoing miscommunications between DOD, Ambassador Bishop, U.S. Central Command (USCENTCOM), and the NEO task force caused problems throughout the operation. U.S. Naval Forces Central Command (NAVCENT) was tasked to execute the NEO but was not monitoring events in Somalia. They got their first warning order on January 1 and received the execute order the next day. NAVCENT was unenthusiastic about committing significant forces, having watched an earlier operation in Liberia morph from a NEO into a protracted military reinforcement of the Embassy.

NAVCENT assigned just two amphibious warfare ships to the operation. They departed Oman, some 1,500 nautical miles from Mogadishu, on January 2. At one point the amphibious group commander even ordered these ships to slow down to conserve fuel. Marines and Sailors onboard were instructed not to unwrap ammunition so it could be returned to contingency stocks later.<sup>19</sup>

The Embassy’s emergency action plan was to evacuate from Mogadishu airport. But by January 2, roving bands of gunmen and runway damage closed the airport. Fixed-wing evacuation attempts by the Italians, French, and Soviets all failed. By then, ground movement to the harbor was dangerous, and security near the Embassy was rapidly deteriorating. Diplomats from several nearby foreign embassies began sheltering at the U.S. compound.

Early on December 5, while still 500 nautical miles away, the task force launched an initial flight of two CH-53 helicopters carrying a ground security team. The ground team was hastily reorganized and cut to 60 men to save space and weight.<sup>20</sup> The inbound flight required two air-to-air-flight refuelings to reach Mogadishu.

Communications between the task force and Embassy were highly

problematic. The Embassy had no secure link to the task force other than by diplomatic cable to Washington and then relayed down through USCENTCOM. All radio traffic between the task force and Embassy went “in the clear.”

The flight crews had maps of Mogadishu from 1969 that did not show the location of the Embassy compound, which relocated during the 1980s. They had to circle the city for 20 minutes searching for the objective marked only by a retired Marine waving a bedsheet.<sup>21</sup>

The lead helicopters reached the Embassy just as gangs of looters were about to breach the walls. It took perhaps as long as 10 minutes to clear the landing zone and deploy into the compound. Evacuation took place under sporadic gunfire as follow-on helicopters arrived. The evacuation control cell team was cut from the mission, and the ground security team failed to fully search or distribute the evacuees properly, resulting in one foreign diplomat almost getting onboard with a loaded weapon. The mission safely evacuated some 281 people from 30 nations, including 8 ambassadors and 39 Soviet embassy staff.

***Lebanon: Israeli Invasion, July 2006.*** On July 12, 2006, Israel invaded Lebanon in response to Hizballah kidnapping two of its soldiers. The Israeli military bombed roads, bridges, and airports, blockaded seaports, cut power, and jammed cellular service, all of which created a mood of panic. This unanticipated event triggered one of the largest multinational NEO events in recent history. The scale, scope, and abruptness of the crisis overwhelmed the Embassy’s ability to manage the evacuation.

The State Department requested DOD assistance on July 14. Evacuations began with a limited helicopter extraction on July 16 and continued through August 2.<sup>22</sup> The United States evacuated 15,000 Americans from Lebanon. Other nations also evacuated thousands of their citizens: Canada (15,000), France (14,000), Sweden (8,400), Germany (6,300), Australia (5,000), Denmark (5,800), United Kingdom (4,600), and Brazil (2,950).<sup>23</sup> The massive numbers of evacuees and the breadth of countries



Mock NEO participants aboard USS *Germantown*, with embarked elements of 31<sup>st</sup> Marine Expeditionary Unit, Sattahip, Kingdom of Thailand, February 12, 2012 (U.S. Navy/Johnie Hickmon)

involved reflect globalization, with ever-increasing population mobility and dual nationalities.

Initially there were no U.S. Navy ships in the eastern Mediterranean and the closest MEU was in the Red Sea, 6 days away by ship. Airlift was in heavy demand for ongoing operations in Iraq and Afghanistan. However, U.S. Transportation Command (USTRANSCOM) used its contracting channels to procure a commercial passenger ship to transport evacuees from Beirut to Cypress. The vast majority of Americans evacuated by sea between July 19–25 using contracted commercial ships and then U.S. Navy and Marine Corps vessels.

Israel had blockaded the coastline, and all ground movement and port operations had to be cleared with the Israeli military. Evacuation also had to be coordinated with Lebanon and either

Cypress or Turkey. Lebanon is within the USCENTCOM AOR, but Israel, Cypress, and Turkey all fall under U.S. European Command (USEUCOM). This required continuous coordination between combatant commands.

The U.S. Embassy and the State Department in Washington had even bigger coordination challenges. State planners kept attempting to reserve commercial aircraft and ships, at times in direct competition with USTRANSCOM and allied countries.<sup>24</sup> State headquarters in Washington restricted the Beirut embassy from talking directly with the media. Meanwhile, the department did not communicate effectively with evacuees, family members, or the media. This created delays and miscommunications that worsened the panic and confusion.

Cypress was used as a temporary safe haven by several other Western countries. This was the height of tourist season. All

hotels, catering, and ground transportation were soon overbooked. DOD had to construct an emergency tent city and bring in additional forces and logistics for life support. U.S. evacuees flowed into Cypress faster than State could charter flights for them back to the United States, which forced DOD to also manage repatriations.<sup>25</sup>

***Japan Earthquake: Operation Pacific Passage, March 2011.*** Following the massive earthquake in Japan on March 11, 2011, DOD authorized a voluntary return of military family members and DOD civilians to the United States. U.S. Northern Command (USNORTHCOM) led the repatriation effort, which flew more than 7,800 DOD noncombatants and their pets out of Japan. Since this was a DOD-only evacuation, it was a rare instance of civilian evacuation and repatriation conducted



entirely by the military without State Department participation.

Although *Pacific Passage* was completed successfully, it uncovered issues that could have been problematic under different circumstances. DOD's computer database used to track non-combatant evacuations (NEO Tracking System, or NTS) did not interface with the passenger manifesting system used by Air Mobility Command.<sup>26</sup> Nor did NTS include all fields required for U.S. customs clearance. *Pacific Passage* was the first real-world test of NTS. Operators were able to work around the problem by using manual processes and rekeying data into multiple systems. However, these flaws increased workload and delay. In a larger emergency, these glitches could have resulted in passengers not being tracked or appropriately screened or being misrouted. DOD has programs under way to correct these issues.

USNORTHCOM's estimates and plans only encompassed repatriation and onward movement to the continental United States. However, many evacuees went to destinations in the U.S. Pacific Command AOR. The units running the Joint Reception Coordination Center had never trained in NEO or NTS and had to learn on the job. Because *Pacific Passage* was a completely DOD-run event, it bypassed normal state and Federal agencies that ordinarily handle repatriation and reception of evacuees.

*The Arab Spring Uprisings and Their Aftermath: Libya (2011, 2012), Yemen (2015)*. The Arab Spring movement that began in December 2010 demonstrated a controversial shift in U.S. policy. In Libya and Yemen, the United States decided not to attempt evacuation or did so only after allied NEOs were already under way.

Joint Task Force *Odyssey Dawn* (JTF-ODD) included a multinational evacuation from Libya and Tunisia in March 2011. By then, however, most Americans had already left. Several NATO countries conducted NEOs in February that evacuated Americans.<sup>27</sup> These included the United Kingdom (Operation *Deference*), Canada (Operation *Mobile*), Germany (Operation

*Pegasus*), and France. Operation *Deference* also included multinational contributions by Romania, Kuwait, Ireland, Spain, and Austria.

The newly created U.S. Africa Command (USAFRICOM) led JTF-ODD and then transitioned it to NATO control. USAFRICOM's intended mission was regional stability and engagement, not warfighting or JFHQ operations. Their headquarters staff was 50 percent civilian and lacked the depth to sustain a 24-hour tempo.<sup>28</sup> Although Libya is within USAFRICOM's AOR, the forces involved and staging bases were from USEUCOM or USCENCOM. USAFRICOM relied heavily on USEUCOM, NATO, and Arab League coalition partners for support.

The decision not to attempt a military rescue of U.S. Ambassador Christopher Stevens from Benghazi, Libya, on September 11, 2012, remains a topic of ongoing partisan arguments and accusations. Four Americans, including Ambassador Stevens, died in an attack on the Benghazi compound. Controversy continues over whether military assistance would have been possible and over who made that determination.

Another controversial decision was not to evacuate private U.S. citizens from Yemen. The U.S. Embassy evacuated in February 2015. An undetermined number of U.S. citizens were left to remain or find their own way out.<sup>29</sup> Several other nations, including India, China, Pakistan, and Somalia, did evacuate their citizens.

### Lessons Learned

Military-assisted NEOs will always be a unique and complex tactical, operational, and strategic mission. Despite this, a NEO is something most headquarters and units historically have just "muddled through." Every NEO has its share of unique problems, and so far the United States has avoided a repeat of the 1970s experiences. But it only takes one disaster to rewrite the strategic narrative.

We should expect a few recurring challenges in any future NEOs:

- Ambassadors and the State Department will defer requesting military assistance as long as possible. By the time they do, the range of options will be narrow.
- GCCs may struggle to devote resources to NEO, particularly if they are already committed on other operations.
- Communications, shared situational awareness, and trust between the Embassy and the NEO force will be untested or absent.
- Mission scope often expands into longer duration repatriation operations or resettlement duties and spills across combatant command boundaries.
- Globalization and modern technology put more Americans in more places with more connectivity than ever before.
- Public attention is notoriously short, but if an incident resonates emotionally, it can sway policy, politics, and perceptions dramatically.

### The Need for a Standing Joint Capability for NEO

A Joint Support Element specifically organized for NEOs could provide immediate capability and a foundation of expertise to support or augment GCC staffs during a NEO contingency. I propose that DOD create a Joint NEO Support Element (JNSE) to provide a rapidly deployable joint planning team specifically focused on NEOs. Marine Expeditionary Units remain an ideal tactical force to execute NEOs when available. Geographic combatant commands should retain ownership for NEO contingency plans in their AOR. What a proposed JNSE could provide is specialized NEO planning and coordination expertise that is deployable worldwide and has reachback to Washington.

The ideal structure for such a JNSE is under USTRANSCOM as part of Joint Enabling Capabilities Command (JECC), which was formed in 2008 as a result of past lessons learned from contingency operations and the Millennium Challenge



Marines and Sailors with Special-Purpose Marine Air-Ground Task Force Crisis Response help U.S. citizens into Marine Corps KC-130J Hercules airplane in Juba, South Sudan, during evacuation of personnel from U.S. Embassy, January 3, 2014 (U.S. Marine Corps/Robert L. Fisher III)

2002 wargame. There was often a troublesome lag at the outset of a crisis before a JFHQ could assemble and ramp to full operating capability.

The existing JECC provides fast-deploying joint headquarters staff elements to provide a nucleus for a contingency JFHQ.<sup>30</sup> Currently, there are three subordinate commands under the JECC: the Joint Planning Support Element (JPSE), Joint Public Affairs Support Element, and Joint Communications Support Element (JCSE). The JNSE would become a fourth element of JECC.

The role of the new JNSE would be similar to the existing Joint Planning Support Element. However, rather than expand the JPSE's mission set, a similarly structured but separately organized JNSE is needed. NEOs often arise concurrently with other crises that require their own joint planning support. Tasking JPSE to prepare for combat contingencies and

humanitarian assistance/disaster relief as well as NEOs would dilute their focus, training, and deployable manpower. History suggests commanders will prioritize other missions at the expense of NEOs. The JNSE could also be based closer to Washington, DC, where it could access State, other U.S. Government agencies, and foreign embassies. JPSE is located several hours away in Norfolk, Virginia.

The new JNSE could address the following concerns:

- It could increase GCC staff capabilities quickly. This would preserve a focus on the NEO even during situations where multiple simultaneous operations are unfolding in the AOR or the GCC staff is overloaded.
- JNSE staff could cultivate ongoing professional relationships and liaise with all the combatant commands, State Department, NATO, and allied

militaries that might be involved in a NEO. This could enhance interoperability, build trust, and provide reachback capability during a crisis.

- The JNSE could also liaise with other governmental agencies at Federal, state, and territory levels who share responsibility for repatriation and reception of Americans back to the homeland. This includes the Department of Health and Human Services and other entities with which most GCCs would not routinely interact.
- JNSE would serve as the subject matter expert on NEOs to refine and share doctrine, techniques, tactics, procedures, and situational awareness. They could develop exercises and training for military units, Embassies, the State Department, and allies.

Perhaps the most important strategic purpose for a JNSE will be to demonstrate a concrete U.S. commitment to prepare for evacuating American citizens anywhere, at any time, if necessary. This could be especially important in today's environment of globalization, instant communication, and extremist groups using ultraviolent propaganda footage. The strategic consequence of a disastrous evacuation or hostage situation could linger for decades. JFQ

## Notes

<sup>1</sup> Ronald W. Reagan, "United States Casualties in Lebanon and Grenada," remarks to military personnel, Cherry Point, NC, November 4, 1983.

<sup>2</sup> Ronald W. Reagan, "Peace: Restoring the Margin of Safety," speech, Veterans of Foreign Wars Convention, Chicago, IL, August 18, 1980.

<sup>3</sup> U.S. Government Accountability Office (GAO), *State Department: Evacuation Planning and Preparations for Overseas Posts Can Be Improved*, GAO Report 08-023 (Washington, DC: GAO, October 19, 2007).

<sup>4</sup> Executive Order 12656, 3 C.F.R., "Assignment of Emergency Preparedness Responsibilities," November 18, 1988.

<sup>5</sup> *Ibid.*

<sup>6</sup> Memorandum of Agreement Between the Departments of State and Defense on the Protection and Evacuation of U.S. Citizens and Nationals and Designated Other Persons from Threatened Areas Overseas, July 1998.

<sup>7</sup> *Ibid.*

<sup>8</sup> Joint Publication 3-68, *Noncombatant Evacuation Operations* (Washington, DC: The Joint Staff, November 18, 2015).

<sup>9</sup> Army Technical Publication 3-05.68, *Special Operations Noncombatant Evacuation Operations* (Washington, DC: Headquarters Department of the Army, September 30, 2014), table 6-1.

<sup>10</sup> North Atlantic Treaty Organization (NATO) Doctrine Standardization Document AJP-3.4.2, *Allied Joint Doctrine for Non-Combatant Evacuation Operations* (Brussels: NATO, March 2007).

<sup>11</sup> Joint Doctrine Publication 3-51, *Non-Combatant Evacuation Operations*, 2<sup>nd</sup> ed. (London: United Kingdom Ministry of Defence, February 2013).

<sup>12</sup> Australian Defence Force Publication 3.10, *Evacuation Operations* (Canberra: Australian Defence Headquarters, 2004).

<sup>13</sup> Joint Doctrine JD-3.4.2, *Non-combatant Evacuation Operations* (No. 136/DEF/CICDE/NP) (Paris: Joint Centre for Concepts, Doctrines, and Experimentations, July 2009).

<sup>14</sup> *Non-Combatant Evacuation Operations*, B-GJ-005-307/FP-050 (Ottawa, Canada: Department of National Defence, 2003).

<sup>15</sup> *Ibid.*

<sup>16</sup> *Ibid.*

<sup>17</sup> *Ibid.*, 70.

<sup>18</sup> Adam B. Siegel, "Eastern Exit: The Non-combatant Evacuation (NEO) from Mogadishu, Somalia, in January 1991," CNA Research Memorandum 91-211 (Alexandria, VA: Center for Naval Analyses, October 1991).

<sup>19</sup> *Ibid.*

<sup>20</sup> *Ibid.*

<sup>21</sup> *Ibid.*

<sup>22</sup> GAO, *U.S. Evacuation from Lebanon*, Report 07-893R (Washington, DC: GAO, June 7, 2007).

<sup>23</sup> World Reach Market Research Series, "Lebanon Evacuation Summary," June 7, 2007.

<sup>24</sup> *Ibid.*, 5.

<sup>25</sup> *Ibid.*, 6.

<sup>26</sup> Jeff Corthell and Chris Faith, presentation slides from the *Pacific Passage* NEO Tracking System Conference, August 8-9, 2011, available at <[www.jllis.mil](http://www.jllis.mil)>.

<sup>27</sup> Tim Ripley, "Western Militaries Conduct NEO Missions Out of Libya," *Jane's Defence Weekly*, March 4, 2011.

<sup>28</sup> Joe Quartararo, Sr., Michael Rovenolt, and Randy White, "Libya's Operation Odyssey Dawn: Command and Control," *PRISM* 3, no. 2 (March 2012), 151.

<sup>29</sup> Smitha Khorana and Spencer Ackerman, "Americans in Yemen Fear They Have Been Left Behind as Bombing Escalates," *The Guardian*, April 1, 2015.

<sup>30</sup> U.S. Transportation Command, Joint Enabling Capabilities Command (JECC), "History of the JECC," available at <[www.jecc.mil/About/BriefHistory.aspx](http://www.jecc.mil/About/BriefHistory.aspx)>.

## New from NDU Press

for the Center for Strategic Research

Strategic Forum 298

*Cross-Functional Teams in Defense Reform: Help or Hindrance?*

By Christopher J. Lamb



There is strong bipartisan support for Section 941 of the Senate's version of the National Defense

Authorization Act for 2017, which requires the Pentagon to use cross-functional teams (CFTs). CFTs are a popular organizational construct with a reputation for delivering better and faster solutions for complex and rapidly evolving problems. The Department of Defense reaction to the bill has been strongly negative. Senior officials argue that Section 941 would "undermine the authority of the Secretary, add bureaucracy, and confuse lines of responsibility." The Senate's and Pentagon's diametrically opposed positions on the value of CFTs can be partially reconciled with a better understanding of what CFTs are, how cross-functional groups have performed to date in the Pentagon, and their prerequisites for success. This paper argues there is strong evidence that CFTs could provide impressive benefits if the teams were conceived and employed correctly.



Visit the NDU Press Web site for more information on publications at [ndupress.ndu.edu](http://ndupress.ndu.edu)

Airmen from New Jersey Air National Guard's 177<sup>th</sup> Security Forces Squadron and local law enforcement officers move toward sound of gunfire, October 24, 2014, during active shooter exercise at Atlantic City Air National Guard Base, New Jersey (U.S. Air National Guard/Matt Hecht)



# Policing in America

## How DOD Helped Undermine Posse Comitatus

By Steven C. Dowell, Jr.

With the recent events of police shootings and domestic terrorism, many are calling into question whether our law enforcement strategies are standing up to the ideals that police everywhere are known to

follow—aptly, *to protect and to serve*. Claims of lingering societal racism and police brutality are under constant scrutiny by social and police reform activists and media coverage.<sup>1</sup> Other studies state these claims are myths being reported daily as facts and are, sadly, finding their way into changing public policy.<sup>2</sup> Tension between these arguments was succinctly stated best as “if you’re pro–Black Lives Matter, you’re assumed to be anti-police, and if

you’re pro-police, then you surely hate black people.”<sup>3</sup> But why should this concern the Department of Defense (DOD)?

At some point, the image of civilian police changed from the popular public servant, such as Sheriff Andy Griffith of the 1960s’ *The Andy Griffith Show*, to the strict enforcer of the law, as portrayed in the movies *RoboCop* (1987) or *Judge Dredd* (1995). Today, civilian police agencies’ capabilities and mindsets

---

First Lieutenant Steven C. Dowell, Jr., USA, is currently training to become a Civil Affairs Officer at the John F. Kennedy Special Warfare Center and School at Fort Bragg, North Carolina.

are intimately related to DOD training and resourcing. Recent questions over similarities between civilian police and the military involve the use of a robot and explosives to end a standoff between a shooter and Dallas police after several officers were murdered in July 2016. This event grasped national headlines just as the 1992 Los Angeles riots did, and again, in 2005, during Hurricane Katrina.<sup>4</sup> In fact, these instances have taken place in a variety of forms since the late 1960s and early 1970s.<sup>5</sup> Two thoughts come to mind. First, during all these events that involved either military cooperation or equipment, the Posse Comitatus Act must have been a topic of conversation. If so, and after so many instances, civilian police and DOD have supposedly found an acceptable balance between these civil events and military intervention. In contrast, however, this article argues that the militarization of a civilian police force undermines the Posse Comitatus Act, and DOD's equipment, training, and transitioning personnel have fueled this evolution for decades.

### The Posse Comitatus Act and Police Militarization

In general, the Posse Comitatus Act's intent is that the "military is currently prohibited by Federal statute from participating in domestic law enforcement."<sup>6</sup> This act was established in 1878 and allowed lawmakers to sanction those who "willfully use members of the Army or Air Force to execute the laws" of the United States.<sup>7</sup> These instances do occur in modern times, but parties disagree on how lawful their usage is versus their effectiveness toward the enforcement of the law.

One specific example would be the Washington, DC, Beltway sniper attacks, which occurred from October 2 to 24, in 2002. Two individuals systematically committed 10 murders and 3 near-fatal attacks in the National Capital Region via the use of a Bushmaster XM-15 rifle. The 3-week spur of attacks solicited heavy national media coverage. This "led to the enlistment of military aircraft and crews to search the Maryland and Virginia suburbs of Washington for the gunmen."<sup>8</sup>

When military personnel supplied their utilities in aid of law enforcement, civilian police units found it hard to ignore those units' methods given their effectiveness in locating a sniper's "point of origin," just as the military was trained to do in combat scenarios; however, if the sniper was found, it was expected that the civilian police would make contact.<sup>9</sup> In fact, it was found that "aerial photographic and visual search and surveillance by military personnel [did] not violate the Posse Comitatus Act."<sup>10</sup>

In times of great civil need the military's logistical capabilities, not to mention manpower and leadership support, are almost too invaluable for civilian police not to utilize. This was the issue particularly in the Katrina aftermath when "[many] police officers actually turned in their badges so to speak and just walked off of the job," in which the "National Guard was the quickest response force that the government could provide to fill that void."<sup>11</sup> Civilian police organizations, even those not in the midst of a disaster relief effort, understand the expanded capabilities that the military provides where civilian police in turn attempt to recreate these same aspects and features within themselves. This militarization could be what is causing reform activists to speculate that we are "going too far."<sup>12</sup> That implies that we are superseding the original intent of the Posse Comitatus Act by simply transitioning military styles, skills, technology, and tactics to civilian police officers. While we are not allowing the military to wear a badge, we *are* allowing those with badges to don combat helmets—and the mentality that comes with it.

When a civilian police force wields military equipment, it requires training. This training includes a combat mindset—an ingredient that may be more powerful than any assault rifle. The change of character and personality that a civilian police officer experiences through militarization may alter his or her perception of what a public servant's purpose truly is. In this case, the civilian police are transforming into quasi-military police, and with that comes a unique area of self-identity that drives that behavior.

Beginning with structure, researchers who study civilian policing versus militarized policing claim that there is beginning to be a "blurring of the boundary between policing and soldiering."<sup>13</sup> As mentioned, civilian police organizations receive an ever-increasing number of tactics and ideologies from the military. This training includes, but is not limited to, weapons manipulation in high-stress environments, low-visibility and urban tactical operations, counterterrorism operations, and intelligence-gathering operations. Former Servicemembers have started their own weapons training curricula or have been hired by civilian weapons training academics, such as those offered by Magpul Core, which offer courses that teach militarily developed techniques.<sup>14</sup> Some of these courses are offered both to law enforcement and current military members. Civilian police take this training back to their agencies and then train each other on the methods.

One not-so-recent change in police work involves the use of military-grade weapons by police across the Nation. In addition, police are also given ballistic protection that is able to stop projectiles fired from similar weapons in an effort to defend against violent criminals and provide the ability to fight back against ever-evolving, capable criminals and terrorist threats. It is reasonable to want law enforcement officers to have the most reliable and effective equipment, but are we attempting to focus on officer survivability or are we trying to win in a combat environment? Arguments can be made that both are occurring and are necessary. The procurement of such gear pressed the Barack Obama administration, both in rhetoric and in executive action, to prohibit the sale of "military-style equipment from the Federal government to civilian police."<sup>15</sup> But not all equipment procurements are being used to fight crime. Civilian police are also using military vehicles to aid in rescues and natural disaster relief efforts, but opinions on usefulness in the civilian police community differ.<sup>16</sup>

With this equipment and training, civilian police are continually developing



Security forces members from Oregon Air National Guard's 142<sup>nd</sup> and 173<sup>rd</sup> fighter wings train together during door-to-door search at training village in Warrenton, Oregon, during exercise Cascadia Rising, June 10, 2016 (U.S. Air National Guard/John Hughel)

specific teams more specialized than the easily recognizable Special Weapons and Tactics (SWAT) teams developed in the late 1960s. A quick online search will find units that range from the U.S. Border Patrol Tactical Unit, Federal Bureau of Investigation's National Joint Terrorism Task Force (NJTTF), U.S. Marshal's Special Operations Group, U.S. Department of Energy's Special Response Team, to the U.S. Park Police SWAT team, among numerous other state and local tactical/assault teams. Interestingly, the NJTTF has Active-duty military liaisons specifically provided by the U.S. Army Criminal Investigation Command—a division of the U.S. Army Military Police Corps. These teams are jointly using practices learned by their parent agencies decades ago from their military mentors, if they are not still learning them today.

Some have suggested that the Central Intelligence Agency originally developed many of these practices for Agency operatives.<sup>17</sup> These tactical training regimens involved techniques such as counter-surveillance, identifying dead drops, and eluding law enforcement. These tactics have good intent behind them, but the fact that their roots come from “espionage” and “special operations” should be a concern for the average citizen. Moreover, civilian police attend training with military members, sometimes through formal joint training events or by chance encounters at a local gun range or civilian training academy, and adapt the methodologies learned and bring them back to their home police departments. These militaristic mindsets carry over when Servicemembers communicate these same military principles to civilian police officers.

In the U.S. Armed Forces, Servicemembers are taught to follow all the orders of the officers appointed over them and the orders of the President of the United States as long as they are legal, moral, and ethical. This is a militaristic hierarchy of control and is enforced by the chain of command. This same chain is replicated in part in civilian police organizations. For a police officer to advance in the hierarchy of the department, “the policeman must exhibit behavior indicative of a ‘relatively unquestioning belief in and acceptance of the organizational system.’”<sup>18</sup> The same could be said for the U.S. military. If Servicemembers do not adapt to the doctrine and culture of their unit, then they will likely not progress within the ranks. Many civilian police are no different. This is what two researchers call the “quasi-military command model.”<sup>19</sup> Civilian police

departments that do indeed practice this leadership model demonstrate behavior that is naturally derived from the Armed Forces. This traditional practice in the military does produce an efficient style of mission execution, and this command model is effectively used with all other aspects of the military's operational specialties. This may be giving civilian police officers, including some civilian police who are also retired military, a false sense of militaristic purpose. This goes deeper into the personal identity of the individual civilian police officer, and how he or she sees themselves working within the community.

This militarization of police departments may be having a negative effect on police officers' self-defined job descriptions as they "began to confuse the role of police officers with a [S]ervice orientation with that of military personnel engaged in a domestic war."<sup>20</sup> This may point toward the militarization of civilian police that, in turn, creates concern for opponents of these changes. Despite the Posse Comitatus Act, which protects us from the use of Active-duty Servicemembers against our citizens, we may have bypassed this act all together simply by recreating soldiers in the civilian sector of law enforcement. While our civilian police forces are transforming to adapt to new threats, they are sacrificing significant perspectives of Service orientations and the community openness that goes with it.

## How Communities View This Change

Among U.S. citizens, 65 percent of Americans admit that "police officers have a very dangerous job" and, despite conflicts between both sides of the argument on how policing should be conducted, as many as 58 percent state that they themselves "show too little respect for police officers these days."<sup>21</sup> Over the last 25 years, a popular method called "community policing" has attempted to create a mutual support effect on the fear of crime, and thus on the overall welfare and satisfaction of the citizens of a neighborhood. In general, community policing has a basic idea: if the police

take the time to get to know their patrol areas' citizens better, talk to them about their daily lives, and take note of urban issues that the city can solve, this would result in the citizens of that area being more apt to report crimes and to assist the officers in helping to reduce and solve crimes. Police usually reduce the amount of time in patrol vehicles and increase the use of bicycles or the frequency of foot patrols. Some programs resulted in the resident citizens of the targeted areas feeling as though their police force was "more hospitable than central police [traditional patrol officers]" and thus the citizens' levels of contentment were increased.<sup>22</sup> They felt as though their rights had been protected, and they were more concerned about fighting crimes by assisting law enforcement rather than shunning police and fearing that their own rights were being sacrificed.

In contrast, there have been examples where community policing was the intent but, based on witness accounts, appeared to have a negative effect. In Richland County, South Carolina, between 2005 and 2007, the sheriff's department attempted to integrate community policing while still maintaining a standard of militarized policing. Community Action Teams (CATs) were developed in order to meet with citizens and community leaders in an effort to gain intelligence on illicit drug networks. However, after meeting with community leaders and citizens during the day, the people who made up the CATs would coordinate and execute counterdrug operations in the form of surveillance and raids during the night.<sup>23</sup> This method of community policing, swiftly followed by militarized counterdrug operations, unraveled the concept of community engagement, and citizens began to lose trust in their civilian police. Soon, CATs were avoided altogether by citizens.<sup>24</sup> Incidentally, the county sheriff at the time, Sheriff Leon Lott, was an institutionalized and trained Military Police officer with additional ties to the special operations forces community.<sup>25</sup> Even without concrete statistics on the effectiveness of Community Action Teams, it can be argued that even the

"appearance" of militarized policing dismantles any trust a community may have with its police force.

## Possible Solutions

### *Eliminating Posse Comitatus.*

The Posse Comitatus Act has several good intentions, but in recent times the act has been described as "archaic."<sup>26</sup> Additionally, any military response today is usually complicated and difficult to work through solely due to the act's own bureaucracy; thus a solution could quite possibly be to eliminate it.<sup>27</sup> This action would favor civilian police as it would widen the path the military is already on in assisting law enforcement. While civilian police would still interact with civilians on a daily basis, the military would theoretically still only ever need to be deployed in times such as crises of either natural or manmade events, but could also be used more quickly in law enforcement capacities when needed. The repeal of the act would likely necessitate a lengthy congressional action to draft and approve, but to maintain the current, loose balance between militarization and civilian policing, a recommendation could be to adopt a system more closely related to that of France.

On November 13, 2015, France suffered the deadliest attacks on its soil since World War II when 130 innocent people were killed in Paris by Islamic extremists. Given the complexity and lethality of the attacks, the French response began from a disadvantage. Numerous issues already existed with French police structure, such as a lack of history of community policing and a tradition of highly centralized decisionmaking.<sup>28</sup> However, while their immediate response has been criticized for lacking sufficient firepower and coordination, the results were surprisingly successful as local civilian police effectively contained terrorists only minutes after their initial attacks.<sup>29</sup> France's police structure is completely nationalized and is broken down into two police forces: the Police Nationale, essentially representing the civilian police, and the Gendarmerie Nationale, essentially representing the military.<sup>30</sup> When the attacks occurred, it was the

civilian police force that responded first, containing the terrorists across the city, namely at the Bataclan Concert Hall. After the attacks, an aggressive search was initiated where “within 48 hours of the attacks, 168 homes had been raided and 104 people had been placed under house arrest.”<sup>31</sup> This was accomplished by both the Police Nationale and Gendarmerie Nationale—a logistical feat that could not have been achieved without military assistance. In this case, using the military as law enforcement swiftly aided in not only ending the attacks but also bringing to justice those who had escaped or aided the terrorists.

In any case, a certain amount of trust must be placed in the military that they will not overstep their bounds. There will always be those who undoubtedly conclude that we are allowing the Armed Forces to gain too much freedom and that we should fear an eventual coup d'état. Ironically, this is exactly what happened recently in Turkey. On July 15, 2016, a faction of the Turkish military opposed the president of Turkey, Recep Tayyip Erdogan, so strongly that it attempted to topple the government and impose martial law “in order to restore democracy.”<sup>32</sup> Regarding the United States, there has never been an organized coup against our own government by the military. A reminder: the Armed Forces swear oaths to defend the Constitution of the United States prior to swearing to obey orders from anyone else. At home and abroad, the Armed Forces have time and again proved to be most accountable to the people they serve. Few countries in the world trust their militaries as much as America does theirs.<sup>33</sup> In fact, the military is the most trusted institution in American society today.<sup>34</sup> This could not be in more contrast to much of the rest of world.

#### *Maintaining Posse Comitatus.*

Maintaining the act would be more in favor of advocates for social and police reform. Ideally, no further drafting of the act would be required. While some Members of Congress would undoubtedly lobby for continued leniency toward the act if new, stricter policies were ever issued, the act would already be

enforceable, and many military leaders and civilian police agencies would be hard pressed not to follow the law without legal consequences, as well as regular media coverage scrutinizing their decisionmaking processes.

Continuing with the Obama administration's intent, prohibitions on military equipment procurement by civilian police agencies would be maintained as well as elaborated on. This would require a comprehensive review of what equipment has already made its way into civilian markets, as well as what has been restricted but authorized to sell only to law enforcement. However, any measures taken to cut the direct link between the military and civilian law enforcement would not stop the sale of military-style equipment from civilian companies that resource both the defense and law enforcement industries separately.<sup>35</sup>

Besides equipment procurement, joint training between the military and civilian police would require closer scrutiny to ensure that military-specific tactics and techniques do not find their way into civilian police agencies without an approved need. Sadly, the control measure for such a restriction would generate a maelstrom of bureaucracy. That supervisory oversight to ensure prohibitions are adhered to and training regimens are screened for necessity in civilian law enforcement agencies would add another time-sapping requirement to DOD's burden. Nonetheless, the result would be intended to satisfy opponents of militarization and, more importantly, eliminate future instances of police misconduct that could be tied to militarization. In any case, these changes would likely take years to have any effect. The military's technologies and tactics would need to evolve without substantial, routine interaction with civilian police, thus increasing the gap between the two entities. Expectedly, many within the civilian police community would still embody the remnant mentalities gained in past joint training events or even those civilian police that recently served in the military. This points toward another issue of whether separated Servicemembers should be allowed to join civilian police

agencies immediately after leaving the military; however, this issue may be more appropriately addressed by a third course of action that DOD could implement itself.

#### *DOD Oversight on Military Relations with Civilian Police.*

If Americans trust their military, then perhaps our military can serve them directly by changing DOD's relationship with civilian police themselves. Enforcing Posse Comitatus at the DOD level could present the best of both worlds for both opponents of militarization and civilian police.

Continuing with policies that prohibit equipment procurement, DOD would not only adhere to the already published list set out by the White House but also develop a required internal “trading delay” for any other equipment sales intended for combat—slightly similar to trading delays as seen in the stock market.<sup>36</sup> But unlike stock market trading delays, where the delay amounts to hours, the DOD trading delay would need to be determined in years, or even decades, but not so long that the sale would render equipment obsolete by the time civilian police would require it. Hence, if DOD sells combat equipment too soon, there will be no difference between the military and police on American streets, and if DOD sells combat equipment too late, civilian police and similar commercial industries will attempt to recreate their own, potentially less-refined solutions. The solution of trading delays could allow DOD to influence, if not control, this conundrum.

Regarding training and mindsets, joint training events could ultimately be restricted to both disaster relief and counterterrorism operations. Disaster relief is quite simple pertaining to logistical, medical, search and recovery support, and so on. Enforcing policies against the transferring of counterterrorism operational knowledge, specifically knowledge involving combat techniques, would require more scrutiny. While it would be easier to deny any and all combat-related techniques from being taught to civilian police, that course of action unfortunately overlooks the





Sailors and Federal law enforcement personnel conduct live-fire training during Navy Security Forces Training Course pilot program, training civilian and military police forces to work together, June 23, 2010, San Diego (U.S. Navy/AC Rainey)

potential for DOD to improve civilian police survivability and service to their citizens if it were to impart at least de-escalation and less-than-lethal training to civilian police, which most civilian police already receive. An example would be the U.S. Marine Corps Inter-Service Non-Lethal Individual Weapons Instructor Course, which for 2 weeks focuses on the proper use and familiarization of TASERs, batons, OC (pepper spray), ocular and acoustic hailing devices, and verbal de-escalation techniques, among other techniques. The course culminates with an understanding by the police officer that the overarching theory behind less-than-lethal capabilities is that, to avoid lethal situations, less-than-lethal options should be used “early and often.” Accordingly, a more favorable action for DOD would be to classify lethal

techniques to a higher security clearance more strictly and lower those of less-than-lethal capability than it has in the past, allowing civilian police to still benefit from those techniques that are absolutely “must share.”<sup>37</sup> This again would constrain military personnel from imparting large amounts of knowledge to civilian police, preventing further instances where police misconduct could occur due to militarization, especially when citizen encounters result in the use of lethal force.

Finally, as retired Servicemembers leave the military, a control measure would need to be implemented to ensure that they do not accelerate the procurement of these techniques to civilian police, essentially creating a loophole around both equipment and training restriction policies. Congress has addressed this type of loophole before in

the Defense Authorization Measures of 2008 and 2009, coercing DOD to enact a policy to prevent this.<sup>38</sup> The existing policy is applied to “very senior employees” of DOD concerning defense contracting companies where they are “subject to a two-year restriction” from being employed by those civilian contractors.<sup>39</sup> This policy has seen controversy and is alleged to have “done little to slow the rush” of Servicemembers transitioning to civilian agencies involved with the defense industry.<sup>40</sup> But the policy could be more effective if first enforced by DOD before the Servicemember separates from the Service and, subsequently, by the Department of Justice where waivers to that policy would be required by the former Servicemember, and second if the policy were implemented specifically toward those in the military who wish to



Servicemembers, civilians, dependents, and retirees from Joint Base Charleston, South Carolina, and local community competed during Security Forces Shooting Competition, May 15, 2013, in honor of National Police Week (U.S. Air Force/Dennis Sloan)

pursue civilian policing positions where a 2-year restriction also applies. This could mitigate that rush and allow a period of reflection for those Servicemembers post-retirement before joining the ranks of civilian law enforcement.

As recent as 2016, a criminal justice survey was taken where 54 percent of Americans stated that “police using military weapons and armored vehicles is ‘going too far,’ while 46 percent [stated] these tools are ‘necessary for law enforcement purposes.’”<sup>41</sup> This trend toward militarization cannot be ignored; however, this could be the natural progression of any law enforcement entity throughout a civilization’s lifetime. To combat new weapons and new threats and deter enemies of the peace, police will need improved forms of deterrence and apprehension. Thus, with ever-looming threats around the world, the last thing we want to do is lessen the abilities and effectiveness of uniformed civilian police officers.

Yet while police continue to serve and protect, there are those who are turning policing into something it was not meant to be. DOD has invented devastatingly effective means of eliminating its enemies, but there must be a moral question of whether we should allow civilian police to use those same methods on U.S. citizens. Even in ancient Rome, the natural progression of policing evolved from simple fire brigades meant to remedy the spread of a fire outbreak to an eventual strictly military force that was not the intent of its originator, Emperor Augustus.<sup>42</sup> And much like in ancient Rome, this change in policing in the United States is something that DOD can and should assist in for the better while there is still time, and while it still has overwhelming favor with the American people. Choosing to maintain or eliminate *Posse Comitatus* will be a question to be answered in the future. We should hope, though, that DOD understands and accepts the role it has played in police development, the

vast amount of influence it will continue to have on civilian police—and that it will have a response when this question is posed. JFQ

---

## Notes

<sup>1</sup> Emily Ekins, *Policing in America: Understanding Public Attitudes Toward the Police. Results from a National Survey* (Washington, DC: Cato Institute, December 7, 2016), 50–51.

<sup>2</sup> Richard R. Johnson, *Dispelling the Myths Surrounding Police Use of Lethal Force* (Raleigh, NC: Dolan Consulting Group, July 2016).

<sup>3</sup> *The Daily Show with Trevor Noah*, Comedy Central, July 7, 2016. Specific excerpts from Noah were that “America has a problem within its police force,” “and although it is a problem that disproportionately affects black people, it’s not just a black problem. This is an American problem,” and that “with police shootings, it shouldn’t have to work that way.”

<sup>4</sup> The California Army National Guard was activated on April 29, 1992, to assist civilian police with conducting law enforcement including conducting patrols within the city.

<sup>5</sup> Radley Balko, “The Militarization of America’s Police Forces,” *Cato’s Letter* 11, no.

4 (Fall 2013), 1–5.

<sup>6</sup> Sean T. Kealy, “Reexamining the Posse Comitatus Act: Toward a Right to Civil Law Enforcement,” *Yale Law & Policy Review* 21, no. 2 (Spring 2003), 383–442.

<sup>7</sup> *Ibid.*, 384; the Air Force was added into the language of Posse Comitatus in 1956, and the Navy and Marines were made subject to the act via a Department of Defense regulation in 1992.

<sup>8</sup> *Ibid.*, 387–388.

<sup>9</sup> Phillip Carter, “Why Can the Army Help Cops Catch the D.C. Sniper?” *Slate.com*, October 17, 2002, available at <[www.slate.com/articles/news\\_and\\_politics/explainer/2002/10/why\\_can\\_the\\_army\\_help\\_cops\\_catch\\_the\\_dc\\_sniper.html](http://www.slate.com/articles/news_and_politics/explainer/2002/10/why_can_the_army_help_cops_catch_the_dc_sniper.html)>. In addition to this exception, this article notes that there have been numerous, major exceptions to the act all in the name of quelling violence and fighting drugs or terrorism.

<sup>10</sup> Eric V. Larson and John E. Peters, *Preparing the U.S. Army for Homeland Security: Concepts, Issues, and Options* (Santa Monica, CA: RAND, 2001), appendix D, available at <[www.rand.org/content/dam/rand/pubs/monograph\\_reports/MR1251/MR1251.AppD.pdf](http://www.rand.org/content/dam/rand/pubs/monograph_reports/MR1251/MR1251.AppD.pdf)>.

<sup>11</sup> Mark Anderson, interview, Military Police Corps, U.S. Army, November 26, 2012.

<sup>12</sup> Ekins, 56–57.

<sup>13</sup> Catherine Lutz, “Making War at Home in the United States: Militarization and the Current Crisis,” *American Anthropologist* 104, no. 3 (September 2002), 723–735.

<sup>14</sup> These courses have been around for years, but the focus here is that instructors for many similar companies, not just Magpul Core, have regularly been former Servicemembers, particularly special operations personnel and law enforcement personnel who served in the military. See Magpul Core Web site at <[www.magpulcore.com/training](http://www.magpulcore.com/training)>.

<sup>15</sup> The ban was imposed on June 8, 2015. Items that were sold before the ban included 101 M113 armored personnel carriers, 6,600 bayonets, and almost 200 grenade launchers. While M113s and grenade launchers could be used for riot control, one must ask why issue civilian police bayonets, especially when some went to Lincoln University campus police. See John Kelly and Steve Reilly, “Many Local Police Already Got Banned Military Gear,” *USA Today*, May 18, 2015, available at <[www.usatoday.com/story/news/2015/05/18/police-already-have-military-gear-white-house-aims-ban/27547527/](http://www.usatoday.com/story/news/2015/05/18/police-already-have-military-gear-white-house-aims-ban/27547527/)>.

<sup>16</sup> *Ibid.* One M113 procured has “sat unused in a [police] agency’s barn for three years,” while others have used it frequently in arresting violent individuals and during rescue efforts.

<sup>17</sup> Eric L. Haney, *Inside Delta Force: The Story of America’s Elite Counterterrorist Unit* (New York: Delacorte Press, 2006), 129.

<sup>18</sup> John M. Jermier and Leslie J. Berkes,

“Leader Behavior in a Police Command Bureaucracy: A Closer Look at the Quasi-Military Model,” *Administrative Science Quarterly* 24, no. 1 (March 1979), 1–23.

<sup>19</sup> *Ibid.*, 2. This is apart from other models that deal with discretion rather than having a more authoritative system, such as the military.

<sup>20</sup> Daryl Meeks, “Police Militarization in Urban Areas: The Obscure War Against the Underclass,” *The Black Scholar* 35, no. 4 (2006), 33–41.

<sup>21</sup> Ekins, 74–75.

<sup>22</sup> Kuotsai T. Liou and Eugene G. Savage, “Citizen Perception of Community Policing Impact,” *Public Administration Quarterly* 20, no. 2 (Summer 1996), 163–179.

<sup>23</sup> Larie Lunceford, interview, Criminal Investigation Command, U.S. Army, July 20, 2016.

<sup>24</sup> *Ibid.*

<sup>25</sup> Leon Lott, biography, Richland County Sheriff’s Department, available at <[www.rcsd.net/bio.html](http://www.rcsd.net/bio.html)>.

<sup>26</sup> Richard T. Sylves, “President Bush and Hurricane Katrina: A Presidential Leadership Study,” *Annals of the American Academy of Political and Social Science* 604 (March 1, 2006); William L. Waugh, Jr., ed., *Shelter from the Storm: Repairing the National Emergency Management System after Hurricane Katrina* (Washington, DC: Sage Publishing, 2006), 26–56.

<sup>27</sup> *Ibid.*, 40.

<sup>28</sup> “The Attacks on Paris: Lessons Learned,” Homeland Security Advisory Council, Quinn Williams, LLC, June 2016.

<sup>29</sup> *Ibid.*, 25–26.

<sup>30</sup> *Ibid.*, 9.

<sup>31</sup> *Ibid.*, 16.

<sup>32</sup> Krishnadev Calamur et al., “What’s Going on in Turkey?” *Atlantic Monthly*, July 21, 2016, available at <[www.theatlantic.com/news/archive/2016/07/turkey-government/491579/](http://www.theatlantic.com/news/archive/2016/07/turkey-government/491579/)>.

<sup>33</sup> “Military and National Defense,” Gallup, available at <[www.gallup.com/poll/1666/military-national-defense.aspx](http://www.gallup.com/poll/1666/military-national-defense.aspx)>.

<sup>34</sup> “Confidence in Institutions,” Gallup, available at <[www.gallup.com/poll/1597/confidence-institutions.aspx](http://www.gallup.com/poll/1597/confidence-institutions.aspx)>.

<sup>35</sup> For example, well-known weapons manufacturers like Sig Sauer produce weapons, such as the MPX, with specific capabilities including fully automatic actions and shorter barrel lengths that are advertised as only being permitted to be sold to the military or law enforcement. This weapon was demonstrated as recently as the summer of 2016 for an undisclosed military unit for this exact purpose. I attended this weapons demonstration, which was publicly released in Quantico, Virginia. Sig Sauer demonstrated the MPX weapon system to Servicemembers to aid in their missions dealing, coincidentally, with law enforcement.

<sup>36</sup> “Trading Halts and Delays,” U.S. Securities and Exchange Commission, July 23, 2010,

available at <[www.sec.gov/answers/tradinghalt.htm](http://www.sec.gov/answers/tradinghalt.htm)>.

<sup>37</sup> *Must Share* is a phrase based on the traditional military classification system of sensitive military documents including “For Official Use Only” or “Law Enforcement Sensitive,” indicating that all relevant personnel should read or know the information marked as “Must Share” to improve the military unit as a whole toward their mission. It is a phrase used within the special operations forces community in particular.

<sup>38</sup> “Senior DOD Officials Seeking Employment with Defense Contractors,” DFARS Case 2008-D007, *Federal Register* 74, no. 10 (January 15, 2009), 2408–2410, available at <[www.gpo.gov/fdsys/pkg/FR-2009-01-15/html/E9-679.htm](http://www.gpo.gov/fdsys/pkg/FR-2009-01-15/html/E9-679.htm)>.

<sup>39</sup> Robert Brodsky, “New Pentagon Rule Tightens Revolving Door,” *Government Executive*, January 15, 2009, available at <[www.gov-exec.com/defense/2009/01/new-pentagon-rule-tightens-revolving-door/28365/](http://www.gov-exec.com/defense/2009/01/new-pentagon-rule-tightens-revolving-door/28365/)>.

<sup>40</sup> David Francis, “DOD Retirees: From 4-Star General to 7-Figure Income,” *Fiscal Times*, June 5, 2013, available at <[www.thefiscaltimes.com/Articles/2013/06/05/DOD-Retirees-From-4-star-General-to-7-Figure-Income](http://www.thefiscaltimes.com/Articles/2013/06/05/DOD-Retirees-From-4-star-General-to-7-Figure-Income)>.

<sup>41</sup> Ekins, 56–57.

<sup>42</sup> Paul Kenneth Baillie Reynolds, *The Vigiles of Imperial Rome* (London: Oxford University Press, 1926).



Member of Cameroonian Battalion d'Intervention Rapide gives eye exam with equipment provided by U.S. Navy during healthcare workshop as part of Africa Partnership Station 2013, Douala, Cameroon, March 27, 2013 (U.S. Army/Jeffrey Hernandez)

# The U.S. Government's Approach to Health Security

## Focus on Medical Campaign Activities

By George E. Katsos

---

Colonel George E. Katsos, USAR, is the Department of Defense Terminologist located on the Joint Staff, and a Deputy Director of Civil-Military Training for the Innovative Readiness Training program at the Office of the Secretary of Defense.

The U.S. Government plans, conducts, supports, and participates in activities that reinforce national interests. These interests perpetuate an international order underpinned by stable democratic governments and regional security. One critical component of national stability is the capability to protect citizens from internal and external threats. This capability normally requires a nation to draw upon its citizenry to populate internal forces

responsible for providing security; therefore, a healthy populace is a necessity. With the U.S. Government's increasing responsibility as a security provider and its political emphasis on health security, the U.S. military will undoubtedly be expected to have a larger role in support of health security objectives. While natural or manmade threats to human health can lead to illness or injury, illness transmitted by proximity between humans remains among the foremost

dangers to human health, international stability, and the global economy. In other words, health security is crucial to U.S. national security.

For purposes of this analysis, U.S. health security focuses on human health and is sought and maintained through successful public health and global health activities. While “public health” focuses on domestic or national human health issues, “global health” focuses on international human health issues that are linked to U.S. domestic security. For an overview of U.S. health security responsibilities and the role of the U.S. military in providing medical aid, this discussion is separated into four sections that capture analysis based on documents, informal discussions, and military briefings: the history of U.S. health policy through legislative actions and international engagements, health policy as articulated in Federal department strategies and other executive branch documents, medical campaign activities executed under the U.S. Code, and recommendations for strengthening U.S. Government health security efforts.

## Legislative Actions and International Engagement

U.S. legislative history and international agreements capture methods that attempt to address modern health security concerns. The government’s public health infrastructure originates from early congressional legislation that, just 9 years into the Nation’s existence, created the U.S. Public Health Service to treat those who served the country at sea.<sup>1</sup> Fifteen years after the Civil War, the American Red Cross was created to provide medical treatment for those citizens who served in uniform. Following World War I, an international League of Nations was created<sup>2</sup> that administered a separate Health Organization to address prevention and control of certain diseases.<sup>3</sup> The League and Health Organization eventually became the United Nations (UN) and World Health Organization (WHO), respectively, both of which the United States provides humanitarian assistance to upon request. During World War II, the U.S. Congress passed the Public

Health Service Act that produced an entity now known as the U.S. Department of Health and Human Services (DHHS).<sup>4</sup> Since then, the United States has steadily increased economic and social development assistance to foreign nations that, in turn, contributed to their own public health systems.

In 1949, the United States became a signatory to a set of international treaties known as the Geneva Conventions and Protocols. One subject included protecting civilian victims of armed conflict and internal violence.<sup>5</sup> Further enhancements addressed “protection of civilians” beyond hostilities to include accessibility to essential services and medical care. Over the next decade, these treaties influenced the United States to support more requests abroad for military assistance. In 1961, Congress passed the Foreign Assistance Act (FAA) to better assist partner nations with security challenges, which eventually led to public and global health support. One tenet distinguished military assistance from humanitarian and development assistance while another created the U.S. Agency for International Development (USAID), which carries out U.S. global health policy development, coordination, and execution.<sup>6</sup> In 2005, the United States became a signatory to the WHO’s International Health Regulations (IHR), a legally binding agreement among 196 state parties, which obligates member states to develop and maintain international public health threat detection, assessment, notification, and response capabilities.<sup>7</sup> Under the IHR, the United States globally assists other nations to ensure that health security capabilities are in place and procedures followed.<sup>8</sup> Additionally, the Global Health Security Agenda (GHS) and the Global Health Security Initiative (GHSI) accelerate international progress against infectious diseases and chemical, biological, radiological, and nuclear (CBRN) exposure, respectively.

With such maturation in U.S. health policy and support for human rights, a more focused national direction on health security has emerged. The following discusses Presidential and department strategies on health security policy.

## The Executive Branch

Offices, departments, and independent agencies make up the executive branch; however, our focus is on departments with Presidential-appointed department heads that implement U.S. policy. The President’s Cabinet today includes 15 department heads known as Cabinet Secretaries. A smaller group of appointed advisors known as the National Security Council (NSC) is a forum used by the President to consider national security and foreign policy matters.<sup>9</sup> One policy document that links executive policy to department activities is a national strategy. For security policy, the President’s National Security Strategy (NSS) connects U.S. policy goals managed by the NSC to objectives on security matters.<sup>10</sup> Subsequently, the U.S. National Health Security Strategy (NHSS) issued by DHHS further articulates health security policy objectives that are linked to NSS objectives. As a result, health security roles within the executive branch are further defined.

The President also articulates policy through executive orders. One order that provides the President’s position on national security matters is called a Presidential Directive. In the last 20 years, five directives set conditions that impact health security. In 1996, President Bill Clinton signed a directive on emerging infectious diseases that increased U.S. surveillance, training, research, and response. It also directed the development of the Department of Defense’s (DOD) Global Emerging Infections Surveillance and Response Program.<sup>11</sup> In 2009, President Barack Obama issued a directive on the implementation of the national strategy for countering biological threats that focused on global health security promotion with other nations to prevent, detect, and respond to infectious disease.<sup>12</sup> Shortly thereafter, the President issued a directive named U.S. Global Development Policy,<sup>13</sup> which elevated development efforts to be on par with diplomacy and defense.<sup>14</sup> Another, National Preparedness,<sup>15</sup> enhanced the Department of Homeland Security (DHS) and its National Response



Member of 89<sup>th</sup> Airlift Squadron during training on CBRN defense techniques, October 4, 2014, Wright-Patterson Air Force Base, Ohio (U.S. Air Force/Frank Oliver)

Framework (NRF) to better synchronize a whole-of-government response to a spectrum of security threats that include health security.<sup>16</sup> More recently, Security Sector Assistance was issued to promote partner-nation support of U.S. interests to include cooperation on humanitarian efforts.<sup>17</sup> All of these directives impact health security strategy development. The following department overviews capture Federal health security efforts in three cascading categories: significant, additional, and remaining.

### Significant Efforts

Two departments play significant roles in achieving U.S. health security objectives: the Department of State and DHHS. State manages foreign affairs for the President and persuades other nations to support U.S. international efforts that impact global economic stability, regional security, and national health security. Two strategic documents that provide guidance to organizational efforts are the non-congressionally mandated *Quadrennial Diplomacy and Development Review* and

the *Department of State and USAID Joint Strategic Plan*.<sup>18</sup> For the purposes of this discussion, the U.S. Government development agency responsible for administering civilian foreign aid known as USAID, although considered a separate government agency, is categorized as an entity here under State as they both share one Cabinet Secretary.<sup>19</sup>

For disaster relief missions, State regional bureaus take the diplomatic lead due to their regional expertise. However, USAID's Office of U.S. Foreign Disaster Assistance (OFDA) administers government responses that include medical aid. Generally, when a foreign disaster is declared or humanitarian crisis emerges, the President selects USAID as the operational lead for coordinating the government response. Although not a member of the President's Cabinet, USAID's administrator is elevated to Cabinet-level member status separate from the Secretary of State and invited to NSC meetings when development and global health issues are concerned.<sup>20</sup> For domestic response, State manages potential international contributions of support.

State also manages diplomatic efforts that result in foreign assistance to other nations including countering threats to human health. One effort is focused on global health, which is identified as the largest component of U.S. long-term development assistance.<sup>21</sup> Within global health is an integrated approach to improve global health conditions known as the Global Health Initiative (GHI). Distinct from the GHSA and GHSI international agreements, USAID-led GHI implementation includes the defense against threats toward population health,<sup>22</sup> fight against communicable diseases transmitted by contact, and support of international health advances.<sup>23</sup> Separate from USAID efforts, State manages the U.S. HIV/AIDS effort via the President's Emergency Plan for AIDS Relief.<sup>24</sup>

DHHS is the other department that pursues U.S. health security objectives.<sup>25</sup> Per its Strategic Plan and Global Health Strategy, DHHS cooperates with scientists worldwide to diagnose, prevent, and control the spread of disease.<sup>26</sup> Additionally, DHHS produces the

congressionally mandated quadrennial NHSS<sup>27</sup> that guides health consequence mitigation of large-scale emergencies, provides strategic direction, and streamlines health security approaches.<sup>28</sup> DHHS information-sharing, disease surveillance, and laboratory research capabilities also play significant roles in its illness mitigation strategy.

In support of U.S. global efforts, DHHS provides assessments, disease control mitigation, crisis and disaster response, and CBRN support.<sup>29</sup> Via its components, the Centers for Disease Control and Prevention (CDC) personnel, National Institutes of Health laboratory researchers, and Food and Drug Administration scientists support responses to prevent further consequences to human health.<sup>30</sup> Moreover, under GHSA and GHSI arrangements, the CDC assists partner nations in health surveillance against emerging infectious diseases, combats injuries from CBRN events and infectious diseases such as pandemic influenza with immunizations,<sup>31</sup> manages the President's Malaria Initiative, participates with DOD in informal international partnerships such as the Global Outbreak Alert and Response Network and the Laboratory Response Network,<sup>32</sup> and actively engages in global partnerships to reduce the impacts of HIV/AIDS.

For domestic activities, DHHS leads U.S. efforts to protect against public health threats and provide countermeasures for mitigation, as well as contributes to crisis response.<sup>33</sup> As such, DHHS conducts public outreach as well as maintains the federally coordinated National Disaster Medical System (NDMS). This system encompasses out-of-hospital medical care during crisis response to disaster stricken areas, patient movement for those unable to transport themselves, and treatment at participating hospitals in unaffected areas.<sup>34</sup> DHHS activates the NDMS under its own authorities or through the NRF where it is delegated authority by DHS to be the operational lead for Emergency Support Function #8, Public Health and Medical Services.<sup>35</sup> Furthermore, DHHS leads the reception of evacuees in the United States,

administers domestic quarantine stations at U.S. ports of entry in support of DHS,<sup>36</sup> and maintains a unique force of 6,700 uniformed but nonmilitary health professionals known as the U.S. Public Health Service (USPHS) corps.<sup>37</sup> In times of national emergency, the corps can deploy with other U.S. departments.<sup>38</sup> DHHS also oversees a domestic network of volunteers known as the Medical Reserve Corps program that strengthens public health systems and improves preparedness, response, and recovery capabilities.<sup>39</sup> Furthermore, CDC Epidemic Intelligence Service personnel identify global causes of disease outbreaks, recommend prevention and control measures, and implement strategies to protect people from health threats.<sup>40</sup>

### Additional Efforts

The following departments make substantial contributions to U.S. health security: DHS; DOD; and the Departments of Agriculture, Commerce, Energy, and Treasury. DHS guidance is provided in the DHS Strategic Plan<sup>41</sup> and the congressionally mandated *Quadrennial Homeland Security Review*.<sup>42</sup> DHS core responsibilities are to provide domestic security and coordinate domestic Federal crisis response to include establishing Federal response structures, delegating domestic emergency response to the Federal Emergency Management Agency (FEMA), maintaining a maritime domain capability through the U.S. Coast Guard,<sup>43</sup> and supporting medical cooperative efforts through the NDMS with DHHS and other interagency stakeholders.<sup>44</sup> However, DHS does play a supporting role in global health efforts through cross-border protection to include U.S. airports and seaports.<sup>45</sup>

DOD supports health security efforts primarily through its military workforce. Key strategic documents include the Defense Security Guidance,<sup>46</sup> the National Military Strategy,<sup>47</sup> and the congressionally mandated Defense Strategic Review (formerly known as the Quadrennial Defense Review).<sup>48</sup> In support of U.S. capacity-building activities

abroad, DOD contributes to engagement and prevention programs, surveillance and response systems, and a network of overseas research laboratories. DOD also supports civil authorities through medical research, preparation, surveillance, and response to biological threat requests. In addition, DOD provides military medical support to the NDMS<sup>49</sup> as well as pre-planned domestic medical civic action events with local communities through its Innovative Readiness Training program.<sup>50</sup>

The Department of Agriculture's strategic plan addresses animal health, public health, plant health, environmental health, and improved access to nutritious food.<sup>51</sup> This includes participation in activities abroad with DOD on provincial reconstruction efforts, countering terrorism, and managing animal disease control.<sup>52</sup> The Department of Commerce's strategic health objectives focus on fostering healthy and sustainable marine resources such as fish stocks, habitats, and ecosystems.<sup>53</sup> It also administers a nonmilitary but uniformed response service<sup>54</sup> known as the National Oceanic and Atmospheric Administration,<sup>55</sup> which interacts with the U.S. Navy via the Global Fleet Station sea base program.<sup>56</sup> The Department of Energy's<sup>57</sup> non-congressionally mandated Quadrennial Energy Review<sup>58</sup> and Quadrennial Technical Review<sup>59</sup> both articulate strategies to prevent the proliferation of weapons of mass destruction abroad,<sup>60</sup> address threats to public health and the environment from energy transmission,<sup>61</sup> and pursue the cleaning up of legacy nuclear waste locations.<sup>62</sup> Also the Treasury Department<sup>63</sup> uses its significant global reach to fund immediate needs that may include medical activities based on U.S. approval and mitigate emerging threats against the U.S. and global economies by relieving or enforcing sanctions.<sup>64</sup>

### Remaining Efforts

A couple of remaining departments maintain significant capabilities to address domestic public health concerns but have minimal, if any, equity in support of global health efforts.<sup>65</sup> The Department of Transportation administers a National Defense Reserve



Airman treats patient during U.S. Pacific Command's Operation *Pacific Angel* 12-4 in Nepal, on September 11, 2012 (U.S. Air Force/Jeffrey Allen)

Fleet, Ready Reserve Force, and Civil Reserve Air Fleet that can augment the transportation of military Services to potentially support public health activities.<sup>66</sup> Moreover, the Department of Veteran's Affairs (DVA) provides health professionals and incident-related medical care via Federal medical stations and coordinating centers to care for those with injuries in support of NDMS hospital activation.<sup>67</sup>

As U.S. Government departments continue to develop their own strategies to achieve health security objectives, the future is uncertain on how they will plan for a robust international workforce response. Currently, USAID-led foreign disaster relief is effective for routine disasters but additional progress is needed to better coordinate U.S. humanitarian assistance for catastrophes with cascading effects to public infrastructure (for example, the loss of electrical power grids and exposure to chemical and radiological events).<sup>68</sup> One solution is to use the domestic NRF as

a framework. Such a framework could produce a mechanism that would be useful due to the fact that most foreign governments are not prepared to respond to out-of-the ordinary, severe catastrophes that overwhelm local and regional response capacity. In Haiti, for example, relief efforts were hampered as responders, including U.S. forces, operated in a severely disrupted environment. The ability of Haiti's leadership to prioritize and coordinate U.S. humanitarian assistance was disabled and healthcare infrastructure to be supported was destroyed. Future demands on the United States for more coordinated relief and lifesaving assistance will continue to be expected, placing more burdens on the U.S. Government departments that make up the NSC system to prepare and contribute.

Furthermore, while departments develop their own strategies, they should also keep a watchful eye on how they are portrayed in joint doctrine—the core foundation of military workforce best

practices. Relevant Joint Publications (JPs) for this discussion include JP 4-02, *Joint Health Services*, JP 3-07, *Stability*, JP 3-08, *Interorganizational Cooperation*, JP 3-20, *Security Cooperation*, JP 3-28, *Defense Support of Civil Authorities*, JP 3-29, *Foreign Humanitarian Assistance*, and JP 3-57, *Civil Military Operations*.

### Medical Campaign Activities

DOD leads or supports Federal efforts that shape operational environments to set, establish, reestablish, or maintain interaction with political entities. One effort is the provision of U.S. humanitarian assistance that includes medical, general engineering, food and water, educational, professional exchange, and disaster preparation activities. DOD contributions underpin these efforts known in joint doctrine as maintaining stability or building capacity abroad via foreign humanitarian assistance (FHA), providing crisis response support through domestic defense support to



civil authorities (DSCA), and delivering foreign disaster relief under FHA. While there are many terms that describe DOD medical contributions to U.S. medical efforts (*medical civil-military or stability operations, global health or partnership engagement, public health services, health diplomacy, disease surveillance, security assistance or cooperation, etc.*), this discussion refers to those contributions as “medical campaign activities.” Medical campaign activities are DOD specific, unlike the categorization of U.S. Government or other entity medical efforts or activities. Selecting a label is not to minimize the importance of the mission, operation, activity, or task; it is used only to provide clarity for those in uniform who participate in or implement it. The following articulates medical campaign activities within Title 10 and Title 22 legal authorities of the U.S. Code.

### **Title 10 of the U.S. Code**

Title 10 is a compilation of permanent legal authorities that the Secretary of Defense uses to authorize federalized military forces to conduct military missions in support of U.S. efforts including humanitarian mission preparation and response. For this discussion, DOD medical campaign activities fall under three categories: disaster relief, byproduct of conflict, and force health protection. While it is important to acknowledge that DOD provides for the well-being of military personnel and supports U.S. stabilization efforts that sets or reestablishes interaction with political entities, the following focuses on the first mentioned category of DOD disaster relief via combatant commander oversight.

For crisis situations abroad, USAID/OFDA generally leads the U.S. response when disaster relief is requested of the Federal Government. In support of U.S. humanitarian assistance, DOD, with its sheer size, budget, and ready capabilities make it an attractive candidate for international aid requests; however, DOD normally contributes to less than 10 percent of all OFDA managed disaster relief.<sup>69</sup> When DOD does contribute to

FHA, its unique and time-sensitive capabilities deliver medical campaign activities mostly in the form of direct patient care, medical supplies transportation, and casualty evacuation generally funded by Overseas Humanitarian, Disaster, and Civic Aid. In 2010, DOD medical campaign activities in support of USAID-led Haiti earthquake disaster relief response efforts included immediate and urgent medical treatment by medical teams from the USNS *Comfort*.<sup>70</sup> When the ship reached capacity, severely injured Haitian patients were evacuated to U.S. hospitals under the authority of the NDMS and were treated by DHHS and DVA personnel.<sup>71</sup> In 2014, DOD conducted medical campaign activities to support the U.S. response to Ebola in Western Africa.<sup>72</sup> These medical campaign activities included laboratory testing and oversight of Ebola treatment unit construction.<sup>73</sup> DHHS/USPHS personnel cooperated with DOD to stabilize, mitigate, and prevent contagion<sup>74</sup> through expeditionary medical system support and training of international health workers.<sup>75</sup>

When domestic Federal disaster relief assistance is requested, DHS/FEMA leads domestic coordination with DHHS managing the medical response. Medical campaign activities to DSCA includes restoring essential health services in collaboration with the state and local health entities.<sup>76</sup> In support of 2005 Federal assistance to Hurricane Katrina victims, medical campaign activities included airlift operations and medical treatment in support of civilian organization efforts along the Gulf Coast.<sup>77</sup> In support of 2012 Federal assistance to Hurricane Sandy victims, medical campaign activities conducted by preventive medicine personnel included testing the safety of food, water, and air in the storm-damaged areas where military personnel were sent to assist.<sup>78</sup> DOD also approved FEMA’s request for transport of over 120 medical personnel to serve as augmentation for hospitals and nursing homes.<sup>79</sup> Veterinarian services were also provided.

In noncrisis situations that include preparation, risk reduction, and building capacity, medical campaign activities generally focus on training U.S. forces

and assisting in the development of or improving medical capacity of government entities. Medical campaign activities in foreign countries funded by Humanitarian and Civic Assistance include events that allow U.S. military medical professionals to practice on real patients to improve their skills.<sup>80</sup> Geographic combatant commands conduct these preplanned medical readiness training exercises and dental or veterinarian exercises in conjunction with foreign Ministries of Health and Defense that impact people, livestock, and pets in distant regions and remote villages.<sup>81</sup> Additionally, these activities bolster host-nation health service capabilities that in turn build local civilian population confidence in the delivery of government essential services. In 2015, DOD’s Continuing Promise and Pacific Partnership missions conducted FHA activities in 15 foreign nations across Central America and the Caribbean with nongovernmental organizations as well as Southwest Asia and the Oceania regions with allied nations, respectively. Medical campaign activities included over 142,000 patients treated in local ports and over 1,900 surgeries conducted aboard hospital ships.<sup>82</sup>

Other medical campaign activities abroad include risk reduction and building capacity programs, communicable disease prevention, infectious disease surveillance and response, an overseas research laboratory network,<sup>83</sup> and academic courses taught by DOD institutions. On the domestic front, DOD conducts medical campaign activities in the form of preplanned civic events with local communities.

### **Title 22 of the U.S. Code**

Title 22 is a compilation of permanent legal authorities that the Secretary of State uses to provide foreign assistance to partner nations. DOD components participation in activities authorized in the FAA and by the President that include health security. Per the FAA, U.S. foreign assistance provides a comprehensive list of assistance, some of which DOD personnel deliver for State.<sup>84</sup> Within foreign assistance,



Army microbiologist on Edgewood Chemical Biological Center in vitro research team conducts laboratory research (U.S. Army/Conrad Johnson)

elements such as security assistance, humanitarian assistance, and development assistance are codified in law.<sup>85</sup>

Formerly known as military assistance in the FAA, security assistance is the most profound way that DOD supports State in delivering foreign assistance. Most likely, the term *security assistance* was later adopted by Congress to lessen the appearance of the militarization of diplomatic efforts during the Cold War. Per the FAA, *security assistance* is defined as a group of planned programs authorized by law where the U.S. provides defense articles, military training, and other defense-related services, by grant, loan, credit, or cash sales to further national policies and objectives.<sup>86</sup> Within U.S. security assistance programs, medical campaign activities range from medical training to medical equipment and donation of medical supplies. Prioritized by both State and DOD, DOD personnel administer medical campaign

activities that fall within Foreign Military Sales (FMS), Foreign Military Finance (FMF), International Military Education Training (IMET), and the Global Peace Operations Initiative (GPOI). For FMS, military material is delivered to partner nations upon formal agreement (for example, first aid kits, warrior aid and litter kits, bandages, and medical equipment sets). Under FMF, funding includes defense article acquisition, provision of services, medical facility construction, and training to nations with weak economies<sup>87</sup> (for example, in the 1990s the U.S. Government provided Egypt with tens of millions of dollars that went to constructing a 650-bed international medical center for the Egyptian military).<sup>88</sup> Moreover, IMET funds the educational instruction by U.S. offices, employees, contract technicians, and contractors to foreign military students, units, and courses on a nonreimbursable (grant) basis that includes health

security.<sup>89</sup> Furthermore, GPOI funds certain activities that build partner country peacekeeping capacity and proficiency for the deployment of foreign militaries that include medical training to foreign forces that may deploy to UN peacekeeping operations.

As for State-managed U.S. Government humanitarian and development assistance, they do not normally involve military personnel. Per the FAA, humanitarian assistance is aid that meets humanitarian needs, including medicine, medical supplies, equipment, and education.<sup>90</sup> U.S. Government development assistance is aid in support of another nation's self-help efforts that are essential to successful long-term development.<sup>91</sup> As DOD has no formal leadership role in the delivery of Title 22 humanitarian assistance or development assistance, it has been the view of some civilian-led organizations that certain long-term humanitarian or development-like Title

10 activities, which include medical campaign activities, mostly fall under traditional civilian-led responsibilities. To mitigate confusion, DOD is encouraged by these organizations to label humanitarian efforts as something other than humanitarian assistance and only provide support to U.S. development efforts.<sup>92</sup>

## Conclusion

DOD *medical campaign activities* is a useful term to identify medical contributions within DOD activities to U.S. health security efforts and programs. In support of U.S. national interests, medical campaign activities are a core element of strategic competition and will continue to be planned for in support of DOD FHA activities to overall U.S. Government efforts. Abroad, medical campaign activities provide a good tool for not only mitigating threats to health security but also countering insurgencies that offer their own medical care to influence and control local civilian populations.<sup>93</sup> At home, medical campaign activities provide immediate lifesaving assistance to U.S. state and local governments and build confidence in Federal government intentions.

Although medical campaign activities that defend against infectious disease efforts such as the Ebola virus are less common, involvement by the U.S. military most likely will increase considerably due to its robust logistics and rapid transportation and surveillance capabilities. In 2015, DOD conducted medical campaign activities in support of U.S. humanitarian assistance efforts to protect civilians from the Zika virus.<sup>94</sup> With national direction on health security and missions of the U.S. military evolving, changes in joint doctrine should more clearly reflect the shift beyond force health protection toward the protection and medical treatment of civilians in multiple types of operating environments.

To more adequately address health security issues in the future, the following recommendations would be of value to assist the United States in improving health security response capabilities:

Congressionally mandate a Quadrennial Security Review to better coordinate a government approach to national security matters, including human health security, therefore forcing departments to plan for non-DOD workforce emergency and disaster relief packages.

Create a Presidential Directive for an International Response Force to assist in codifying a U.S. Government catastrophic coordination mechanism that will raise department priorities for development of a complex medical response capacity.

Create a Presidential Directive on Health Security to raise the priority for planning and importance of U.S. health security efforts expressed and implied in existing directives and strategic documents.

Identify non-DOD U.S. entities that can potentially execute existing DOD medical campaign activities and assist in the development of their capabilities to plan for and fill potential DOD health security capability shortfalls in future missions due to constrained budget environments and sequestration.

Encourage interorganizational participation in joint doctrine development to capture best practices and create awareness of extant non-DOD health security capabilities used in cooperation with DOD to further expose stakeholders to each other's capabilities and systems.<sup>95</sup> JFQ

## Notes

<sup>1</sup> *An Act for the Relief of Sick and Disabled Seamen*, 1 Stat. L., 605, 5<sup>th</sup> Cong., 2<sup>nd</sup> sess., July 16, 1798.

<sup>2</sup> Derek Licina, "The Military Sector's Role in Global Health: Historical Context and Future Directions," *Global Health Governance* 6, no. 1 (Fall 2012), 4; League of Nations, *Covenant of the League of Nations*, April 28 1919, available at <www.refworld.org/docid/3dd8b9854.html>.

<sup>3</sup> Iris Borowy, *Coming to Terms with World Health: The League of Nations Health Organization 1921-1946* (Frankfurt: Internationaler Verlag Der Wissenschaften, 2009), 57.

<sup>4</sup> *Public Health Service Act of 1944*, Public Law 78-410, 78<sup>th</sup> Cong., 2<sup>nd</sup> sess., July 1, 1944.

<sup>5</sup> International Committee of the Red Cross, *Geneva Convention Relative to Protection of Civilian Persons in Time of War*, August 12,

1949, 6 UST. 3516, 75 U.N.T.S. 287.

<sup>6</sup> *Foreign Assistance Act of 1961*, Public Law 87-195, 87<sup>th</sup> Cong., 1<sup>st</sup> sess., September 4, 1961.

<sup>7</sup> *International Health Regulations (2005)*, 2<sup>nd</sup> ed. (Geneva: World Health Organization, 2008), available at <www.who.int/ihr/publications/9789241596664/en/>.

<sup>8</sup> *National Health Security Strategy and Implementation Plan (NHSS/IP) 2015-2018* (Washington, DC: Department of Health and Human Services, 2015), 30.

<sup>9</sup> Barack H. Obama, Presidential Policy Directive (PPD)-1, *Organization of the National Security Council System* (Washington, DC: The White House, February 13, 2009).

<sup>10</sup> *National Security Strategy* (Washington, DC: The White House, May 2010), 39.

<sup>11</sup> William J. Clinton, Presidential Decision Directive NTSC-7, *Emerging Infectious Diseases* (Washington, DC: The White House, June 12, 1996).

<sup>12</sup> Barack H. Obama, PPD-2, *Implementation of the National Strategy for Countering Biological Threats* (Washington, DC: The White House, November 23, 2009).

<sup>13</sup> Barack H. Obama, PPD-6, *U.S. Global Development Policy* (Washington, DC: The White House, September 23, 2010).

<sup>14</sup> *Foreign Assistance Act of 1961*, Public Law 94-161, 94<sup>th</sup> Cong., 1<sup>st</sup> sess., December 20, 1975. In 1993, President Clinton nominated the Director for the U.S. Agency for International Development (USAID) as the Special Coordinator for foreign humanitarian assistance and disaster relief; PPD-6.

<sup>15</sup> Barack H. Obama, PPD-8, *National Preparedness* (Washington, DC: The White House, March 8, 2011).

<sup>16</sup> *Ibid.*

<sup>17</sup> Barack H. Obama, PPD-23, *Security Sector Assistance* (Washington, DC: The White House, April 5, 2013).

<sup>18</sup> The first combined Department of State and USAID strategic plan was published in 2003.

<sup>19</sup> Title 22 U.S. Code § 6592, Foreign Affairs Agencies Consolidation, Administrator of AID [the Agency for International Development] reporting to Secretary of State. For organizational purposes, under U.S. law, USAID falls under State.

<sup>20</sup> *Quadrennial Diplomacy and Development Review* (Washington, DC: Department of State, July 2009), 115; PPD-6, 5.

<sup>21</sup> *FY 2014-2017 Department of State and USAID Strategic Plan* (Washington, DC: Department of State, 2014), 23.

<sup>22</sup> *U.S. Global Health Policy, The U.S. Government Engagement in Global Health: A Primer* (Washington, DC: The Henry J. Kaiser Family Foundation, January 2013), 20-25.

<sup>23</sup> See Global Health Initiative, available at <www.ghi.gov>.

<sup>24</sup> *FY 2014-2017 Department of State and USAID Strategic Plan*, 23.



DOD deployed medical teams from Joint Task Force–Bravo to Peru to provide aid in aftermath of 8.0 magnitude earthquake that struck area on August 15, 2007 (DOD/Jeremy Lock)

<sup>25</sup> Edwin K. Burkett, “Foreign Health Sector Capacity Building and the U.S. Military,” *Military Medicine* 177 (March 2012), 298.

<sup>26</sup> *The Global Health Strategy of the U.S. Department of Health and Human Services* [DHHS] (Washington, DC: DHHS, October 13, 2011). See also “Strategic Goal 3: Advance the Health, Safety, and Well-Being of the American People,” available at <[www.hhs.gov/strategic-plan/goal3.html](http://www.hhs.gov/strategic-plan/goal3.html)>.

<sup>27</sup> *Public Health Service Act*, Public Law 109-417 § 103, 109<sup>th</sup> Cong., 2<sup>nd</sup> sess., December 19, 2006, 120; see also *National Health Security Strategy and Implementation Plan (NHSS/IP) 2015–2018*.

<sup>28</sup> See the *National Health Security Strategy*, Public Health Emergency, available at <[www.phe.gov/Preparedness/planning/authority/nhss/Documents/nhss-ip.pdf](http://www.phe.gov/Preparedness/planning/authority/nhss/Documents/nhss-ip.pdf)>.

<sup>29</sup> *The Global Health Strategy of the U.S. Department of Health and Human Services*, 10.

<sup>30</sup> *Strategic Plan FY 2014–2018* (Washington, DC: DHHS, March 2014).

<sup>31</sup> JP 3-08, *Interorganizational Coordination* (Washington, DC: The Joint Staff, Revision First Draft), 173–174.

<sup>32</sup> *Ibid.*, 174.

<sup>33</sup> *Ibid.*, 171.

<sup>34</sup> See the National Disaster Medical System, Public Health Emergency, available at <[www.phe.gov/preparedness/responders/ndms/Pages/default.aspx](http://www.phe.gov/preparedness/responders/ndms/Pages/default.aspx)>.

<sup>35</sup> *National Response Framework* (Washington, DC: Department of Homeland Security, January 2008).

<sup>36</sup> JP 3-08, 172.

<sup>37</sup> *Strategic Plan FY 2014–2018* (Washington, DC: DHHS, March 2014).

<sup>38</sup> Committee on Oversight and Investigations, “Testimony from Rear Admiral Boris D. Lushniak on Update on the U.S. Public Health Response to the Ebola Outbreak,” November 18, 2014, available at <[www.hhs.gov/asl/testify/2014/11/t20141118b.html](http://www.hhs.gov/asl/testify/2014/11/t20141118b.html)>.

<sup>39</sup> See the Medical Reserve Corps Program Web site, available at <<https://mrc.hhs.gov/HomePage>>.

<sup>40</sup> See the Centers for Disease Control’s Disease Detectives, available at <[www.cdc.gov/eis/diseasedetectives.html](http://www.cdc.gov/eis/diseasedetectives.html)>.

<sup>41</sup> *Strategic Plan for Fiscal Years (FY) 2012–2016* (Washington, DC: Department of Homeland Defense, 2012).

<sup>42</sup> *Quadrennial Homeland Security Review* (Washington, DC: Department of Homeland Security, June 18, 2014). See *Homeland Security*

*Act of 2002*, Public Law 107-296 § 707, 107<sup>th</sup> Cong., 2<sup>nd</sup> sess., November 25, 2002, 154.

<sup>43</sup> JP 4-06, *Joint Mortuary Affairs* (Washington, DC: The Joint Staff, October 12, 2011), VII-1.

<sup>44</sup> See “Standard National Disaster Medical System Provider Memorandum of Agreement for Definitive Medical Care,” Public Health Emergency, available at <[www.phe.gov/ndms/reimbursement/Documents/NDMS-Provider-MOA.pdf](http://www.phe.gov/ndms/reimbursement/Documents/NDMS-Provider-MOA.pdf)>.

<sup>45</sup> *Ibid.*, 31.

<sup>46</sup> *Sustaining U.S. Global Leadership: Priorities for 21<sup>st</sup> Century Defense* (Washington, DC: Department of Defense [DOD], January 2012).

<sup>47</sup> *National Military Strategy* (Washington, DC: The Joint Staff, January 2012).

<sup>48</sup> *National Defense Authorization Act for Fiscal Year 2015*, Public Law 113-291 § 1701, 113<sup>th</sup> Cong., 2<sup>nd</sup> sess., December 19, 2014, 128.

<sup>49</sup> See Emergency Support Function Annexes, Federal Emergency Management Agency, available at <[www.fema.gov/pdf/emergency/nrf/nrf-annexes-all.pdf](http://www.fema.gov/pdf/emergency/nrf/nrf-annexes-all.pdf)>.

<sup>50</sup> See DOD Innovative Readiness Training Web site, available at <<http://irt.defense.gov>>.

<sup>51</sup> *Strategic Plan for FY 2014–2018* (Washington, DC: Department of Agriculture, 2014).

<sup>52</sup> JP 3-08, 114.

<sup>53</sup> *FY 2014–FY 2018 Strategic Plan* (Washington, DC: Department of Commerce, 2014), 26.

<sup>54</sup> See Uniformed Service Rank Chart, U.S. Public Health Service, available at <[www.usphs.gov/docs/pdfs/uniform/Uniformed%20Service%20Rank%20Chart.pdf](http://www.usphs.gov/docs/pdfs/uniform/Uniformed%20Service%20Rank%20Chart.pdf)>.

<sup>55</sup> JP 3-08, 117.

<sup>56</sup> Ibid.

<sup>57</sup> *Strategic Plan 2014–2018* (Washington, DC: Department of Energy, March 2014).

<sup>58</sup> *Quadrennial Energy Review: Energy Transmission, Storage, and Distribution Infrastructure* (Washington, DC: Department of Energy, April 2015).

<sup>59</sup> *Quadrennial Technical Review: An Assessment of Energy Technologies and Research Opportunities* (Washington, DC: Department of Energy, September 2015).

<sup>60</sup> JP 3-08, 122.

<sup>61</sup> *Quadrennial Energy Review*, 251.

<sup>62</sup> Ibid., 3.

<sup>63</sup> *Strategic Plan for Fiscal Years 2014–2017* (Washington, DC: Department of Treasury, 2014).

<sup>64</sup> Ibid., 27.

<sup>65</sup> For example, the Departments of Education, Housing and Urban Development, Interior, Justice, Labor, Transportation, and Veteran's Affairs.

<sup>66</sup> JP 3-08, 137, 140.

<sup>67</sup> Ibid., 175.

<sup>68</sup> Paul N. Stockton, *All-Hazards Foreign Response: Lessons Learned from Haiti, Fukushima, and Other Catastrophes* (Falls Church, VA: Anser, October 30, 2013).

<sup>69</sup> Ibid.

<sup>70</sup> See "Operation Unified Response: Support to Haiti Earthquake Relief 2010," U.S. Southern Command, available at <[www.southcom.mil/newsroom/Pages/Operation-Unified-Response-Support-to-Haiti-Earthquake-Relief-2010.aspx](http://www.southcom.mil/newsroom/Pages/Operation-Unified-Response-Support-to-Haiti-Earthquake-Relief-2010.aspx)>.

<sup>71</sup> *Independent Review of the U.S. Government Response to the Haiti Earthquake, Final Report* (Washington, DC: USAID, March 28, 2011), 54; Gary Cecchine et al., *The U.S. Military Response to the 2010 Haiti Earthquake: Considerations for Army Leaders* (Washington, DC: RAND, 2013), 27.

<sup>72</sup> Kristina Peterson, "Congress Releases Funding to Aid Fight Against Ebola," *Wall Street Journal*, October 10, 2014, available at <[www.wsj.com/articles/congress-releases-funding-to-aid-fight-against-ebola-1412959345](http://www.wsj.com/articles/congress-releases-funding-to-aid-fight-against-ebola-1412959345)>.

<sup>73</sup> U.S. Senate Appropriations Committee, "Statement for the Record Honorable Michael D. Lumpkin, Assistant Secretary of Defense Special Operations and Low-Intensity Conflict," 113<sup>th</sup> Congress, November 12, 2014; House Armed Services Committee, "HASC Update: DOD Response to the Ebola Outbreak

in West Africa," October 9, 2014.

<sup>74</sup> Government Accountability Office (GAO), *Regionally Aligned Forces: DOD Could Enhance Army Brigades' Efforts in Africa by Improving Activity Coordination and Mission-Specific Preparation*, GAO 15-568 (Washington DC: GAO, August 26, 2015), 8.

<sup>75</sup> See Haiti Earthquake 2010, Public Health Emergency, available at <[www.phe.gov/emergency/news/sitreps/Pages/haitiearthquake.aspx](http://www.phe.gov/emergency/news/sitreps/Pages/haitiearthquake.aspx)>.

<sup>76</sup> JP 3-29, xii.

<sup>77</sup> Steve Bowman, Lawrence Kapp, and Amy Belasco, *Hurricane Katrina: DOD Disaster Response*, RL33095 (Washington, DC: Congressional Research Service, September 19, 2005), 6.

<sup>78</sup> "Military Provides Critical Assistance in Aftermath of Massive Storm Sandy," U.S. Medicine, December 2002, available at <[www.usmedicine.com/agencies/departments-of-defense-dod/military-provides-critical-assistance-in-aftermath-of-massive-storm-sandy/](http://www.usmedicine.com/agencies/departments-of-defense-dod/military-provides-critical-assistance-in-aftermath-of-massive-storm-sandy/)>.

<sup>79</sup> "DOD Provides Hurricane Sandy Response, Relief Update," November 3, 2002, available at <<http://archive.defense.gov/news/newsarticle.aspx?id=118438>>.

<sup>80</sup> DOD Instruction 2205.02, "Humanitarian Civic Assistance Activities," Washington, DC, June 23, 2014.

<sup>81</sup> See Joint Task Force–Bravo, available at <[www.jtfb.southcom.mil](http://www.jtfb.southcom.mil)>.

<sup>82</sup> U.S. Senate Armed Services Committee, "Posture Statement of Admiral Kurt W. Tidd, Commander, United States Southern Command, Before the 114<sup>th</sup> Congress"; "Infographic: Pacific Partnership and Continuing Promise," *NavalToday.com*, available at <<http://navaltoday.com/2015/10/02/infographic-pacific-partnership-and-continuing-promise/>>; Jeanette Steele, "Mercy Returns from Medical Mission," *San Diego Union-Tribune*, September 25, 2015, available at <[www.sandiegouniontribune.com/news/2015/sep/25/mercy-returns-10th-pacific-partnership/](http://www.sandiegouniontribune.com/news/2015/sep/25/mercy-returns-10th-pacific-partnership/)>.

<sup>83</sup> Kellie Moss and Josh Michaud, *The U.S. Department of Defense and Global Health: Infectious Disease Efforts* (Washington, DC: The Kaiser Family Foundation, October 2013), 7–15; James B. Peake et al., *The Defense Department's Enduring Contributions to Global Health: The Future of the U.S. Army and Navy Overseas Medical Research Laboratories* (Washington, DC: Center for Strategic and International Studies, June 2011).

<sup>84</sup> *Foreign Assistance Act of 1973*, Public Law 93-189 § 23, 87 Stat, 93<sup>rd</sup> Cong., 1<sup>st</sup> sess., December 17, 1973, 727.

<sup>85</sup> JP 3-29, GL-7.

<sup>86</sup> *International Security Assistance and Arms Export Control Act of 1976*, Public Law 94-329 § 301, 90 Stat, 94<sup>th</sup> Cong., 2<sup>nd</sup> sess. (June 30, 1976), 750.

<sup>87</sup> JP 3-20, 37.

<sup>88</sup> Aram Roston and David Rohde, "Egyptian Army's Business Side Blurs Lines of U.S.

Military Aid," *New York Times*, March 5, 2011.

<sup>89</sup> JP 3-20, 37.

<sup>90</sup> *Foreign Assistance Act of 1961*, Public Law 87-195, 87<sup>th</sup> Cong., 1<sup>st</sup> sess., September 4, 1961, as Amended Through Public Law 113-76 § 499 (January 17, 2014), 160.

<sup>91</sup> Ibid., § 102, 3. See also JP 3-08, 268.


DOD defines *development assistance* as programs, projects, and activities carried out by USAID that improve the lives of the citizens of developing countries while furthering U.S. foreign policy interests in expanding democracy and promoting free market economic growth.

<sup>92</sup> *Independent Review of the U.S. Government Response to the Haiti Earthquake, Final Report*, 71.

<sup>93</sup> JP 3-24, *Counterinsurgency* (Washington, DC: The Joint Staff, November 22, 2013), II-15.

<sup>94</sup> Patricia Kime, "Zika Virus: Pentagon Will Relocate At-Risk Family Members," *Military Times*, February 1, 2016, available at <[www.militarytimes.com/story/military/benefits/health-care/2016/02/01/zika-virus-pentagon-relocate-risk-family-members/79515660/](http://www.militarytimes.com/story/military/benefits/health-care/2016/02/01/zika-virus-pentagon-relocate-risk-family-members/79515660/)>.

<sup>95</sup> James C. McArthur et al., "Interorganizational Cooperation III of III: The Joint Force Perspective," *Joint Force Quarterly* 81 (2<sup>nd</sup> Quarter 2016), 129–139.



As seen from back seat of Fighter Squadron 41 F-14A Tomcat aircraft, pilot brings aircraft in for arrested landing on flight deck of USS *Theodore Roosevelt* during Operation *Desert Storm* (DOD/Parsons)

# The Advent of Jointness During the Gulf War

## A 25-Year Retrospective

By Christopher G. Marquis, Denton Dye, and Ross S. Kinkead

---

Major Christopher G. Marquis, USAF, is an Instructor in the Joint Warfighting Department at the Air Command and Staff College. Lieutenant Colonel Denton Dye, USA, is a Member of the Interoperability and Standardization Team at North Atlantic Treaty Organization Headquarters, Supreme Allied Command Transformation. Major Ross S. Kinkead, USA, is a Member of the Directorate for Intelligence at the Joint Intelligence Center, U.S. European Command, following his most recent assignment as the Executive Assistant to the Director for Intelligence, Joint Staff J2.

It has been three decades since the passage of the Goldwater-Nichols Department of Defense Reorganization Act of 1986, a piece of legislation that changed how the Department of Defense (DOD) functions and how the military conducts operations. By adopting the concept now known as “jointness,” it restricted the Services to an administrative and organizational role as force providers, while combatant commanders held operational authority with a chain of command leading directly to the Secretary of Defense and the President.<sup>1</sup> The intent of the legislation could be compared to that of the Constitution supplanting the Articles of Confederation, which drew the relatively independent states into a more closely centralized political body.

Less than 5 years after its passage, Goldwater-Nichols encountered its first big test when Saddam Hussein’s forces invaded Kuwait in August 1990. In response, a U.S.-led coalition reacted

with a buildup of forces in Saudi Arabia and an offensive that drove the Iraqis out of Kuwait—the Gulf War. Its success seemed a vindication for Goldwater-Nichols specifically and joint operations more generally. General H. Norman Schwarzkopf, USA, the commander in chief of U.S. Central Command, answered to Secretary of Defense Richard Cheney through the Chairman of the Joint Chiefs of Staff, General Colin Powell. Lieutenant General Charles Horner, USAF, who held the newly established position of Joint Forces Air Component Commander (JFACC), was in control of the air war.

With the hindsight of a quarter-century since the conflict, the verdict on jointness in the Gulf War is now more nuanced. In part, this is due to the fact that the U.S. military failed to replicate the spectacular success of Operation *Desert Storm* in subsequent engagements.<sup>2</sup> Also, the Services had not all embraced jointness without reservations. The Marine Corps seemed the most skeptical of the benefits of jointness, and their limited interoperability with other Services during the Gulf War appeared to reinforce their doubts.

Jointness clearly was not the decisive factor in the coalition victory in the Gulf War, although it was likely a positive contributing factor. The superiority of the coalition forces over Iraqi forces was so comprehensive that it alone was sufficient to achieve the mission objectives. The coalition was better equipped, better trained, and better led than the Iraqis. The coalition benefited from widespread international support, especially regional support, and focused objectives. Moreover, jointness was not fully realized during the operation. In some cases, it was improperly applied. U.S. forces are much closer to realizing the full possibilities of jointness today, after several years of major combat operations and counterinsurgencies in the Middle East. The concept of globally integrated operations, introduced by then-Chairman of the Joint Chiefs of Staff General Martin Dempsey in 2012, may further help in the development of jointness as a continuous state of military operations.

This article examines the concerns Goldwater-Nichols was meant to address and demonstrates that the United States and its coalition partners would have achieved victory in the Gulf War even without the legislation. What follows is an explanation of the historic context leading to Goldwater-Nichols, its application in Operation *Just Cause* (1989), and an abridged overview of Operations *Desert Shield* and *Desert Storm*. The balance of the article deals with the varying opinions of jointness in the Gulf War. It provides an analysis summarizing the ideas of the authors and delivers recommendations to military leadership. Above all, jointness must be continually developed in order to maintain its effectiveness.

### Operations Eagle Claw and Urgent Fury

On November 4, 1979, militant followers of the Ayatollah Ruhollah Khomeini overran the U.S. Embassy in Tehran, taking 66 American citizens hostage. When diplomatic negotiations proved fruitless, DOD planned a raid to liberate the hostages with a joint task force (JTF) comprised of personnel from four of the military Services. In April 1980, the JTF attempted its rescue operation, codenamed *Eagle Claw*. The result was a complete disaster, culminating in a fatal collision between a U.S. helicopter and supporting C-130. No hostages were rescued, and eight members of the JTF were killed. Additional losses included aircraft, equipment, and secret documents.<sup>3</sup>

In May 1980, a special commission chartered by the Joint Chiefs of Staff examined the operation's failure. The review's chairman, Admiral J.L. Holloway III, USN (Ret.), identified the "major issues" that ultimately led to the operation's demise.<sup>4</sup> These included separate training between the units prior to the mission, a muddled command and control hierarchy, and problems with equipment interoperability.<sup>5</sup> Congress failed to act decisively on the findings of the Holloway Commission, but events in the Caribbean a few years later would further the argument for legislative reform.

On October 14, 1983, rivalry within the Marxist People's Revolutionary Government of Grenada resulted in a militant coup and the execution of the country's leader, Prime Minister Maurice Bishop. The resulting chaos threatened the safety of more than 650 American medical students on the island.<sup>6</sup> This led to the U.S. launch of Operation *Urgent Fury* on October 25. The deployed force for this mission consisted largely of a joint Army and Marine ground force, supported by special operations, naval, and air assets. The mission resulted in the successful rescue of 720 U.S. and foreign citizens and the restoration of popular government on the island at a cost of 135 U.S. casualties.<sup>7</sup>

Although generally viewed as a success by military leaders, *Urgent Fury* was marred by many of the same issues that plagued *Eagle Claw*. There were failures of communication and equipment shortfalls, as Army units were unable to coordinate air support with naval assets. Assault plans were not coordinated between Services prior to combat operations, leaving units largely unaware of what adjacent unit objectives were and how they fit into the overall scheme of maneuver. These shortcomings resulted in fratricide and the inadvertent bombing of noncombatants.<sup>8</sup> The complications suffered in Iran and Grenada eventually led Congress to pass Goldwater-Nichols, triggering the largest reorganization since the formation of DOD in 1947.<sup>9</sup>

### Passage of Goldwater-Nichols

The year prior to *Urgent Fury*, Chairman of the Joint Chiefs of Staff General David C. Jones told the House Armed Services Committee, "The system is broken. I have tried to reform it from the inside, but I cannot. Congress is going to have to mandate necessary reforms."<sup>10</sup> He stressed the need for "an organization which will allow us to develop the proper strategy, necessary planning, and the full warfighting capability."<sup>11</sup> To accomplish these goals, Congress sought the following changes:

- clarifying the military chain of command from operational com-

manders through the Secretary of Defense to the President

- giving Service chiefs responsibility for training and equipping forces, while making clear that they were not in the chain of command for military operations
- elevating the Chairman of the Joint Chiefs of Staff relative to other Service chiefs by making him the principal military advisor to the President, creating a Vice Chairman position, and specifying that the Joint Staff worked for the Chairman
- requiring military personnel entering strategic leadership roles to have experience working with their counterparts from other Services (so-called joint credit)
- creating mechanisms for military Services to collaborate when developing capability requirements and acquisition programs, and reducing redundant procurement programs through the establishment of the Office of the Under Secretary of Defense for Acquisition.<sup>12</sup>

These reforms met with staunch resistance from within the Pentagon. However, by late 1986, the experiences of *Eagle Claw* and *Urgent Fury* had shifted political opinion decisively toward the need for legislation. Congress voted overwhelmingly for Goldwater-Nichols, with only four Members of both houses voting in opposition.<sup>13</sup>

### Operation Just Cause

Congress would not have to wait long before its reorganization efforts were put to the test. In 1989, tensions in Panama began to rise as the actions of General Manuel Noriega's government became increasingly provocative. The situation reached a boiling point on December 15, when Panama's National Assembly declared a state of war with the United States and a Marine lieutenant was killed by Noriega's forces at a roadblock in Panama City.<sup>14</sup> As a result, President George H.W. Bush activated a contingency plan to secure American interests in Panama and remove Noriega from power.<sup>15</sup>

The operation, codenamed *Just Cause*, began on December 20 and would be the largest military undertaking since Vietnam. The campaign comprised a joint force of over 20,000 personnel and 300 aircraft deployed from both the United States and Panama to strike 27 different locations simultaneously.<sup>16</sup> The results from the operation in Panama appeared to be generally positive. The military accomplished its objectives within a few days.<sup>17</sup> Clear lines of authority and command were established early through a JTF headquarters.<sup>18</sup> The Joint Staff kept policymakers informed and provided latitude for lower headquarters. Joint rehearsals and appropriate training by the Services were also credited with the success.<sup>19</sup>

It appeared that Goldwater-Nichols had passed its initial test. However, the *Just Cause* operation was short lived and small scale. Operations lasted only a few days, and only about 4 percent of the participating U.S. troops would be deployed in the Gulf War, so few concrete lessons were drawn from it. There would be a much greater challenge the following summer, when Iraqi forces marched into the small nation of Kuwait.

### Operations Desert Shield and Desert Storm

In the early morning hours of August 2, 1990, three Iraqi divisions crossed the border into Kuwait. The small Kuwaiti army and navy provided courageous but futile resistance against the superior invading force. Kuwait's ruler, Sheikh Jaber al-Ahmad al-Sabah, fled to Saudi Arabia. By August 4, Iraqi troops had completed their conquest and were lining up on the Saudi-Kuwaiti border.<sup>20</sup>

Most officials in the U.S. Government were surprised by Iraq's action. Although Iraqi officials had made threatening charges against Kuwait in the months leading up to the invasion, U.S. officials had assumed it was merely a bluff.<sup>21</sup> Having realized this assumption was a mistake, President Bush decided to act and made his determination clear to his administration and the public.<sup>22</sup> American and British leaders began to gather an international coalition with the United

Nations' backing to oppose Saddam's forces. On August 6, King Fahd of Saudi Arabia consented to allow coalition troops to deploy into his nation.<sup>23</sup>

Eighteen nations provided ground forces to the effort. The United States alone deployed 500,000 troops and 2,000 tanks, with the British in second place, providing 35,000 troops and 210 tanks.<sup>24</sup> On paper, the Iraqi military was a formidable opponent. Its army consisted of about one million troops. Coalition analysts estimated that 43 Iraqi divisions, including 12 armor, were in the Kuwaiti theater of operations, although only 4 of these divisions were from the elite Republican Guard.<sup>25</sup> Even though the coalition held the airpower advantage with a maximum strength of 1,820 combat aircraft,<sup>26</sup> the Iraqi air force appeared ready to challenge air superiority with about 750 combat aircraft, the sixth largest air force in the world, and a vast air defense system.<sup>27</sup>

General Schwarzkopf used his authority to organize forces as he saw fit. He made the decision to organize air components under one functional command. He then named Lieutenant General Horner, commander of U.S. Central Air Force, as the JFACC "to provide centralized planning, decentralized execution, and the integration of both service and allied air capabilities."<sup>28</sup> In contrast, he did not appoint a separate Joint Force Land Component Commander.

Operation *Desert Storm*, also known as the Gulf War, began at 1:30 a.m. on January 17, when U.S. Navy ships in the Persian Gulf and Red Sea launched Tomahawk cruise missiles toward Baghdad. Throughout Iraq on that first night, coalition helicopters and fixed-wing aircraft struck key targets to cripple air defenses and disable communications.<sup>29</sup> Tomahawks and F-117s scored a number of hits in Baghdad, shutting down the electrical system and knocking out CNN's live telecast.<sup>30</sup>

The Iraqi air force and air defenses proved no match for the sudden onslaught. Coalition forces achieved air superiority within a week, forcing Iraqi pilots to attempt to hide their planes, place them next to residential buildings





Airman, front, of 68<sup>th</sup> Aeromedical Evacuation Squadron (AES), Norton Air Force Base, Airman, right, of 118<sup>th</sup> AES, Tennessee Air National Guard, and Airman, left, of 137<sup>th</sup> AES receive mission briefing during Operation *Desert Storm* (U.S. Air Force/Kimberly Yearean)

or landmarks, or fly them to Iran for protection.<sup>31</sup> Moreover, Iraqi responses were disjointed and ineffective. They launched Scud missiles at Saudi Arabia to cause terror and at Israel to draw it into the conflict and thus wreck the coalition, but these efforts ultimately failed.<sup>32</sup> Similarly, a desperate Iraqi assault at Khafji in late January was repulsed.<sup>33</sup>

The coalition launched its ground offensive at 3:00 a.m. on February 24 with a three-pronged attack. In the east, the 1<sup>st</sup> Marine Expeditionary Force advanced into southeast Kuwait, supported by the multinational Joint Forces Command-East.<sup>34</sup> In the west, XVIII Corps, including the 101<sup>st</sup> Airborne Division and 24<sup>th</sup> Infantry Division, along with the French Daguet 6<sup>th</sup> Light Armored Division, maneuvered north before swinging east toward Highway 8, to the rear of Iraqi forces in Kuwait.<sup>35</sup> In the center, U.S. VII Corps and the British 1<sup>st</sup> Armored Division drove into Iraq near

the Kuwaiti border, engaging a mechanized infantry division and armored division of Saddam's elite Republican Guard.<sup>36</sup> All the attacks succeeded spectacularly, and by February 26, Kuwaiti forces were able to march into Kuwait City as part of an army of liberation.<sup>37</sup> The Iraqi forces had been reduced to a disorganized mob attempting to retreat back to their homeland. The next day, the coalition declared a ceasefire. Kuwait was liberated. The Gulf War was won.<sup>38</sup>

### Positive Reactions to Jointness in Desert Storm

Many viewed the overwhelming success of the Gulf War as a vindication of Goldwater-Nichols and a clear sign of the benefits of joint warfighting. Harry G. Summers, in *On Strategy II*, stated that the legislation was “long overdue” and credited it with attaining unity of effort in the operation.<sup>39</sup> Robert H. Scales, in *Certain Victory*, wrote of how

*Desert Storm* “raised the execution of joint warfare to an unprecedented level of competence.”<sup>40</sup>

James Locher, a former staffer on the Senate Committee on Armed Services, observed the widespread approval of the operational chain of command established by the legislation. He considered the recognition of its success to be “universal.” According to Locher, William Perry, Secretary of Defense in the Bill Clinton administration, remarked to the committee, “All commentaries and after-action reports on [*Desert Shield/Desert Storm*] attribute the success of the operation to the fundamental structural changes in the chain of command brought about by Goldwater-Nichols.”<sup>41</sup>

Katherine Boo, writing for the *Washington Monthly*, proclaimed that the effects of Goldwater-Nichols were “gloriously apparent” in the Gulf War victory.<sup>42</sup> She placed upon the Services much of the blame for the then-recent

chain of military disasters, such as the helicopter crash during Operation *Eagle Claw*, the Beirut Marine barracks bombing, and the friendly fire incidents during Operation *Urgent Fury*.<sup>43</sup> “By elevating international safety over service politics,” Boo wrote, “Congress helped the military win the Gulf War—a fact crucial to recognize now, not for the sake of praising Congress, but for the cause of broader military reform.”<sup>44</sup> By her reasoning, Goldwater-Nichols was an antidote for the follies of the Services’ control of operations.

### Other Factors in the Gulf War Victory

To many observers, however, the legislation was a minor factor in the coalition victory. Dominic Caraccilo, writing for *Army Magazine* in 2015, made no mention of jointness in his article and instead credited the success of the mission to the fact that the goals were “well-defined, resourced, and limited to driving the Iraqis out of Kuwait and defending the Kingdom of Saudi Arabia.”<sup>45</sup> Richard Weitz of the Institute for Foreign Policy Analysis noted the Gulf War was “over-determined” and that “so many factors favored an allied victory” that a change in any single factor, jointness presumably included, would not have affected the ultimate result.<sup>46</sup>

Don D. Chipman, a retired military professor from the faculty at Air University’s Squadron Officer College, acknowledged the positive effect of joint doctrine on the success of the Gulf War but compiled it with other elements, including the use of modern technology such as precision-guided munitions and stealth technology, training, and strong leadership, particularly in the person of General Schwarzkopf. “Yet, even with all of these factors,” Chipman observed, “ultimately the final victory depended on the proper application of airpower.”<sup>47</sup>

General Fred Franks, who commanded VII Corps during *Desert Storm*, and his co-author Gregory Fontenot concluded in a recent article in *Army Magazine* that the key to the victory in the Gulf War lay with improved leadership

development, along with a “revolution” in training and doctrine from the 1970s.<sup>48</sup> As these opinions make clear, the changes brought about by Goldwater-Nichols were not universally recognized as the key to victory in *Desert Storm*.

### Skeptical Reactions to the Impact of Jointness

Some researchers went even further, arguing that *Desert Storm* was actually a poor example of jointness. Michael R. Gordon and Bernard E. Trainor, in *The Generals’ War*, addressed this point:

*The campaign was “joint” more in name than in fact. Each service fought its own war, concentrating on its own piece of the conflict with a single-minded intensity, and the commanders in Washington and Riyadh failed to fully harmonize the war plans. In this sense, the Gulf War shows that there is much to be done if the American armed forces are to operate in a truly coordinated and integrated manner.*<sup>49</sup>

Weitz, writing in 2004, largely agreed with this opinion. He elaborated on how the Services, in the lead-up to *Desert Storm*, each focused on its own war plans, rather than collaborating jointly. The Special Planning Group, working on the air plan, was known as the “Black Hole.” The ground campaign was devised by the “Jedi Knights,” many of whom were Army graduates of the U.S. Army School of Advanced Military Studies. The Marines seemed to lack easy access to either group and were left to generate their own plan.<sup>50</sup>

Even Katherine Boo conceded the imperfect application of jointness in the Gulf War, documenting the important detail that Navy communication systems were not able to receive messages over secure modems from Riyadh. This necessitated the physical transfer of the air tasking order to the Navy Service component commander aboard his aircraft carrier in the Persian Gulf or Red Sea each day.<sup>51</sup>

Mackubin T. Owens, writing in 1996, made a key point when he noted that “there have been several operations in the Goldwater-Nichols era that match earlier

operations inefficiency for inefficiency. Aspects of both Somalia and Bosnia come to mind.”<sup>52</sup> The failure to replicate the overwhelming success of *Desert Storm* suggests that jointness is not by itself a decisive factor. If it were, we might expect every operation to turn out with a similar degree of success.

Furthermore, even if the Services recognized the Gulf War as a “joint” victory, they took different lessons from the conflict and emerged with different opinions of jointness. Some viewed it as a zero-sum game, with one Service benefiting at another’s expense. Bruce Watson and his team exemplified this idea in *Military Lessons from the Gulf War*, when they declared the Air Force “prevailed,” while the Marines afloat were “reduced to posing a threat that was never realized.”<sup>53</sup>

### Jointness and Airpower

For many, the Gulf War was a vindication not of joint warfare, but of the strategic use of airpower. Within the Air Force, the Gulf War was seen as the culmination of many of the previously unfulfilled promises of airpower advocates. For those who shared this perspective, the success of the operation would usher in an era in which the air domain would be the most prominent.

Price T. Bingham, then an Air Force lieutenant colonel, expressed an opinion widely held within that Service when he wrote, “Campaign success now depends on superiority in the air more than it does on surface superiority.”<sup>54</sup> According to Bingham, existing joint doctrine was outdated and needed to be brought into alignment with Air Force doctrine.<sup>55</sup>

Perhaps of all the Services, the Air Force most favorably embraced the potential of joint operations. Air Force doctrine defines the *Airmen’s Perspective* as including a belief in the centralized control of airpower by Airmen.<sup>56</sup> Since 1947, fixed-wing air assets had been distributed between the Air Force, Navy, and Marines. The innovation of the position of JFACC, used in *Desert Storm* under the control of Lieutenant General Horner, at long last brought many of these assets under the tactical control of one Airman.



Air-to-air view of two U.S. Air Force F-15C Eagle fighter aircraft of 33<sup>rd</sup> Tactical Fighter Wing, Eglin Air Force Base, and Royal Saudi air force F-5E Tiger II fighter aircraft during mission in support of Operation *Desert Storm* (U.S. Air Force/Chris Putman)

However, this championing of both airpower and jointness was not necessarily shared by the other Services. According to Weitz, Navy aviators believed the joint air campaign limited their involvement. Both the Navy and Marine Corps were skeptical of the doctrinal legitimacy of the JFACC concept.<sup>57</sup> The communication systems aboard Navy aircraft were incompatible with the secure systems of the Airborne Warning and Control System, which limited the Navy's ability to conduct missions over Kuwait and Iraq.<sup>58</sup> There were plenty of disputes between Army and Air Force personnel regarding target selection. The mutual distrust manifested itself with the Army disputing many of the claimed strikes and damage assessments of the Air Force pilots.<sup>59</sup>

Perhaps the most serious disagreements were between the Air Force and Marines. The Marines, distrustful of the joint air tasking cycle process that selected targets and assigned sorties, admittedly gamed the system by offering

late changes to the air tasking order and listing preferred targets as secondary in the hope of increasing the likelihood for approval.<sup>60</sup>

It should come as no surprise that the Marines were the most reluctant to buy into the joint warfighting concept. The Marines had, and retain, a reputation for independence and self-sufficiency in land and air operations. Their symbiotic relationship with the Navy was in place centuries before Goldwater-Nichols. They were thus less likely to embrace a concept that would potentially disrupt this composition. As a case in point, special conditions regarding the deployment of Marine air assets have been incorporated into joint doctrine.<sup>61</sup>

### Jointness for the Long Term

This article is not a criticism of the idea of jointness. The current nature of war, in both tempo and scope, and the limited resources now available for national defense make jointness impera-

tive and inevitable. The point is that the Services must see jointness as a normal state of operations, not a special condition to be used only during wartime. Also, jointness is not a cure-all for the multitude of problems that emerge in the conduct of war. In fact, the learning curve of the Services operating together can create its own short-term problems. The ultimate benefit of achieving unity of effort necessitates the Services work through these challenges.

Jointness requires continuous interoperability among the Services. The idea that the U.S. military would fight as a joint team, then separate into its Service corners in peacetime, mutes the long-term benefits of joint operations. Now that our military has waged major combat and counterinsurgency operations for 15 years in Afghanistan and Iraq, it is adopting a more realistic, workable method of operating jointly.

In 2014, William Odom and Christopher Hayes stated, "Today the



Oil wells burn out of control after set ablaze by retreating Iraqi forces during Operation *Desert Storm* (DOD)

separate military Services that make up America's Armed Forces work together more often than at any time in the Nation's history. Their success over the last decade of war has cemented the power of 'jointness' in accomplishing military objectives.<sup>62</sup> It is only through time, and continuous operations, that a truly joint force can take form. Fittingly, "perseverance" is a joint principle of war.<sup>63</sup>

General Martin Dempsey offered a viable solution to these issues with the introduction of globally integrated operations in the *Capstone Concept for Joint Operations* in September 2012. The idea was to require "a globally postured Joint Force to quickly combine capabilities with itself and mission partners across domains, echelons, geographic boundaries, and organizational affiliations."<sup>64</sup> Among the implications of globally integrated operations are a professional military education focus on mission command and jointness. General

Dempsey's goal was for the Services to become "pervasively interoperable," with the result being that Servicemembers throughout the military would see themselves as part of a joint force.<sup>65</sup>

D.H. McCauley of the Joint Forces Staff College concurred with General Dempsey's advocacy of globally integrated operations. The dynamic nature of the modern international environment demanded a change in force posture:

*Given the Chairman's new operating concept of globally integrated operations, the military will transform from a conventionally focused and capital-intensive (for example, costly weapons systems such as the F-35) force to one oriented on small, adaptable, globally deployable units that require well-trained, experienced counterinsurgency forces and military police.<sup>66</sup>*

Although it took over two decades to recognize, if jointness is going to

work properly, it must be a continuous state, not merely a temporary condition for the Services to participate in during contingencies. While *Desert Storm* obscured its impact on mission success, 15 years of continuous joint operations have provided a more sober perspective. Globally integrated operations are a practical attempt to apply jointness to modern warfare.

## Conclusion

Jointness was not the decisive factor in the coalition's victory over Saddam Hussein's Iraqi forces in the Gulf War. There were several factors to the victory, including superior technology, leadership, international support, plentiful resources, and limited objectives. It is more accurate to say jointness was a positive contributing factor.

Goldwater-Nichols was an attempt to correct the failings of coordination and synchronization between the Services

and to allow the combatant commanders to conduct operations as they best saw fit without undue interference from multiple commands. Its simplification of the operational chain of command is perhaps its most highly valued and enduring contribution. It is less clear how well it accomplished its other goals by the time of the Gulf War. The Service chiefs had to tolerate their new role as advisors subordinate to the Chairman of the Joint Chiefs of Staff, and the Services had to accept their restriction to administrative and organization functions, but inter-Service rivalry persisted. It appeared that the Services saw jointness as a wartime condition, while peacetime would remain Service-centered. The problem with this notion was that the Services would have to learn to be joint again each time a new conflict arose.

It was not until the continuous joint operations of the war on terror compelled the Services to work together on a regular basis that the concept of jointness started to become fully realized. General Dempsey's concept of globally integrated operations is poised to continue this development, so that future military leaders will think of jointness as second nature to their operations. It is recommended that military officers at all levels study and recognize both the benefits and the challenges of jointness. It is only through persistent synchronization and collaboration that the Services can fully realize the possibilities of joint operations and build appropriate coordinating mechanisms and practices organically. JFQ

## Notes

<sup>1</sup> Doctrinally described as "cross-Service combination wherein the capability of the joint force is understood to be synergistic, with the sum greater than its parts." See Joint Publication (JP) 1, *Doctrine for the Armed Forces of the United States* (Washington, DC: The Joint Staff, 2013), ix.

<sup>2</sup> Mackubin T. Owens, Jr., "Goldwater-Nichols: A Ten-Year Retrospective," *Marine Corps Gazette* 80 (1996), 52–53.

<sup>3</sup> Kathleen J. McInnis, *Goldwater-Nichols at 30: Defense Reform and Issues for Congress*, R44474 (Washington, DC: Congressional Research Service, June 2, 2016), 3.

<sup>4</sup> James L. Holloway, *Rescue Mission Report* (Washington, DC: Joint Chiefs of Staff, 1980), 56.

<sup>5</sup> McInnis, 3.

<sup>6</sup> Sharon Tosi Lacey, "Grenada 1983: Small Island, Big Lessons: A Three-day Cold War Clash in the Caribbean Had Far-Reaching Impacts on American Joint Operation," *Military History* (2013), 46–48.

<sup>7</sup> Ronald H. Cole, "Grenada, Panama, and Haiti: Joint Operational Reform," *Joint Force Quarterly* 20 (Autumn–Winter 1998/1999), 59.

<sup>8</sup> Lacey, 52.

<sup>9</sup> *Ibid.*, 53.

<sup>10</sup> James R. Locher III, "Has It Worked?" *Naval War College Review* 54, no. 4 (2001), 101.

<sup>11</sup> McInnis, 6.

<sup>12</sup> *Ibid.*, 8.

<sup>13</sup> Katherine Boo, "How Congress Won the War in the Gulf," *Washington Monthly* 23, no. 10 (October 1991), 35.

<sup>14</sup> Richard Fournier, "A Just Cause in Panama," *Veterans of Foreign Wars Magazine* 1 (2015), 23.

<sup>15</sup> James H. Embrey, "Operation Just Cause: Concepts for Shaping Future Rapid Decisive Operations," in *Transformation Concepts for National Security in the 21<sup>st</sup> Century*, ed. Williamson Murray (Carlisle Barracks, PA: Strategic Studies Institute, 2002), 202.

<sup>16</sup> *Ibid.*, 198, 205.

<sup>17</sup> *Ibid.*, 223.

<sup>18</sup> *Ibid.*, 236.

<sup>19</sup> *Ibid.*, 234.

<sup>20</sup> Bruce W. Watson et al., *Military Lessons of the Gulf War* (London: Greenhill Books, 1993), 15.

<sup>21</sup> Michael R. Gordon and Bernard E. Trainor, *The Generals' War: The Inside Story of the Conflict in the Gulf* (Boston: Little, Brown and Company, 1995), 14.

<sup>22</sup> *Ibid.*, 49.

<sup>23</sup> *Ibid.*, 52.

<sup>24</sup> Watson, 81.

<sup>25</sup> *Ibid.*, 246.

<sup>26</sup> *Ibid.*, 226.

<sup>27</sup> *Ibid.*, 69.

<sup>28</sup> Damian J. McMarthy and Susan A. Medlin, "Two Hats for the Joint Force Commander?" *Joint Force Quarterly* 25 (Summer 2000), 91.

<sup>29</sup> Gordon and Trainor, 209–210.

<sup>30</sup> *Ibid.*, 216.

<sup>31</sup> Watson, 70.

<sup>32</sup> *Ibid.*, 180–181.

<sup>33</sup> Gordon and Trainor, 285–286.

<sup>34</sup> Watson, 96–98.

<sup>35</sup> *Ibid.*, 99, 111.

<sup>36</sup> *Ibid.*, 101–102, 111–113.

<sup>37</sup> *Ibid.*, 110.

<sup>38</sup> *Ibid.*, 116–118.

<sup>39</sup> Harry G. Summers, Jr., *On Strategy II: A Critical Analysis of the Gulf War* (New York: Dell Publishing, 1992), 241.

<sup>40</sup> Robert H. Scales, Jr., *Certain Victory* (Washington, DC: Office of the Chief of Staff of the United States Army, 1993), 370.

<sup>41</sup> James R. Locher III, "Taking Stock of Goldwater-Nichols," *Joint Force Quarterly* 34 (July 2003), 36–37, brackets in source document.

<sup>42</sup> Boo, 32.

<sup>43</sup> *Ibid.*, 33–35.

<sup>44</sup> *Ibid.*, 33.

<sup>45</sup> Dominic J. Caraccilo, "Desert War Taught Lessons in How Superpower Uses Force," *Army Magazine* 65, no. 7 (2015), 45.

<sup>46</sup> Richard Weitz, "Jointness and Desert Storm: A Retrospective," *Defense and Security Analysis* 20, no. 2 (2004), 133.

<sup>47</sup> Don D. Chipman, "Desert Storm and the Triumph of Joint Warfare Planning," *Air Power History* 52, no. 1 (2005), 54.

<sup>48</sup> Fred Franks and Gregory Fontenot, "Decisive U.S. Response Was Both End of an Era, Birth of a New One," *Army Magazine* 65, no. 7 (2015), 43.

<sup>49</sup> Gordon and Trainor, xiv.

<sup>50</sup> Weitz, 146.

<sup>51</sup> Boo, 36.

<sup>52</sup> Owens, 52–53.

<sup>53</sup> Watson, 218.

<sup>54</sup> Price T. Bingham, "Air Power in Desert Storm and the Need for Doctrinal Change," *Airpower Journal* 5, no. 4 (1991), 33.

<sup>55</sup> *Ibid.*

<sup>56</sup> LeMay Center for Doctrine, "Airmen's Perspective," available at <<https://doctrine.af.mil/download.jsp?filename=V1-D24-Airmans-Perspective.pdf>>.

<sup>57</sup> Weitz, 136–137.

<sup>58</sup> *Ibid.*, 141.

<sup>59</sup> *Ibid.*, 137.

<sup>60</sup> *Ibid.*, 139.

<sup>61</sup> JP 1, IV-4.

<sup>62</sup> William O. Odom and Christopher D. Hayes, "Cross-Domain Synergy: Advancing Jointness," *Joint Force Quarterly* 73 (2<sup>nd</sup> Quarter 2014), 123.

<sup>63</sup> JP 3-0, *Joint Operations* (Washington, DC: The Joint Staff, 2011), A-4.

<sup>64</sup> Martin E. Dempsey, *Capstone Concept for Joint Operations (CCJO): Joint Force 2020* (Washington, DC: The Joint Staff, 2012), 4.

<sup>65</sup> *Ibid.*, 8–10.

<sup>66</sup> D.H. McCauley, "Globally Integrated Operations: A Reflection of Environmental Complexity," *Joint Force Quarterly* 71 (4<sup>th</sup> Quarter 2013), 66.



## Mission Failure: America and the World in the Post-Cold War Era

By Michael Mandelbaum  
Oxford University Press, 2016  
485 pp. \$29.95  
ISBN: 978-0190469474

Reviewed by Bruno Carvalho

**R**eactionary, expansive, naive: these are the themes that Michael Mandelbaum alludes to most often in his extensive look at U.S. foreign policy since the end of the Cold War. Mandelbaum examines foreign policy from the end of the George H.W. Bush Presidency through the Barack Obama administration, highlighting the mix of wishful thinking and lack of focus that prevailed as the United States found itself unchecked on the global stage following the decline and eventual dissolution of the Soviet Union in 1991. Mandelbaum assesses several notable foreign policy failures: the North Atlantic Treaty Organization expansion and the bungled rapprochement with Russia; the failure to instill democracy in China; Bill Clinton's interventions in Bosnia, Haiti, and Somalia; and the mixed record on the Israeli-Palestinian conflict and U.S. attempts at nation-

building in Iraq and Afghanistan. Mandelbaum paints a picture of a foreign policy apparatus beset by lack of interest and political cohesion, demotion in importance to domestic policy, and a repeated failure to understand key aspects of the societies in which the United States chose to intervene.

Mandelbaum's early chapters highlight key points that set the stage for the later portions of the book: the U.S. insistence on imposing its ideals on other nations, a lack of a clear post-Cold War goal in regard to foreign policy, and the absence of a counterweight to oppose U.S. ambitions overseas. The United States was caught unaware by the relative freedom to act in which it found itself; Mandelbaum refers to this when he mentions that "historically, where their foreign policies are concerned sovereign states inhabit the realm of necessity; they do what they must to survive. The United States after the Cold War, by contrast, dwelled in the difficult-to-reach kingdom of choice." With a policy apparatus built mainly to deter and dissuade the Soviet Union, the United States emerged from the Cold War determined to spread its core ideals of democracy and the free-market system. At the same time, Mandelbaum notes how the United States, having "won" the Cold War, switched its priorities to a domestic focus, with its domestic political class also losing the cohesion that the need to counter the Soviet Union had fortified.

Mandelbaum's strength lies in demonstrating the results of a less focused foreign policy, with goals driven by niche wants and domestic popularity rather than actual strategic needs or interests. A case in point is his description of the Clinton administration's Somalia intervention in 1993, which details how a humanitarian mission descended into mission creep that resulted in U.S. casualties. The resulting fallout would then set the stage for future American interventions to be casualty averse and beholden to politicians focused on domestic needs and approval ratings.

This pattern of shallow interventions would be repeated in both Haiti and the Balkans, as the United States attempted

to export its political and democratic ideals into societies with little capacity for change. Mandelbaum draws excellent comparisons with the U.S. occupations in both Germany and Japan, describing how their prewar national identities and civil structures were instrumental in their postwar success. In contrast, when American policymakers intervened in Haiti and Bosnia, they encountered kinship-based societies with little record of accountable, impersonal institutions or rule of law, facts that were repeatedly ignored.

Mandelbaum adequately addresses actions prior to 9/11, but the book takes an interesting shift when he pivots to discussing post-9/11 foreign policy. These chapters are truly the highlight of the book, as the author delves into the minutiae of the American response. Pointing out how 9/11 reprioritized foreign policy for U.S. policymakers, Mandelbaum describes the shifting perception of terrorism from being a crime to being an act of combat as al Qaeda focused its methods on mass slaughter. This change set the stage for other U.S. actions of the time, such as the increasing use of targeted drone strikes, the extralegal rendition of suspected terrorists, the use of torture, and the National Security Agency's domestic collection programs—all done in the name of fighting terrorism. Pointing out that in hindsight, the lack of attacks after 9/11 means that the terrorist threat may have been overblown, Mandelbaum frames this change as the United States returning to acting on its interests instead of its ideals. The U.S. intervention in Afghanistan in 2001 is described the same way; in acting on its interests to root out al Qaeda and capture Osama Bin Laden, the United States failed to give Afghanistan's government the tools it would need to succeed later, setting the stage for the corruption of the Hamid Karzai regime.

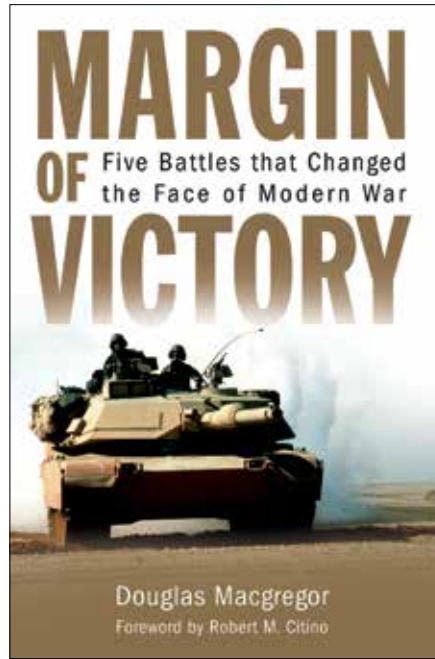
Mandelbaum's description of the Iraq War and the continuous failure of U.S. involvement in the Israeli-Palestinian peace process further highlights his overall theme of U.S. foreign policy shortcomings. Briefly describing Iraq's history as a nation with kinship- and

tribal-based societies, he lambasts the U.S. expectation that such a fractious country would embrace American-style democracy and freedom. The author details how the United States, in its attempts at post-invasion order, simply replaced Iraq's Sunnis with its Shia population in the ruling structure, setting the stage for a sectarian government, reprisals, and the eventual start of Iraq's brutal insurgency and civil war. Mandelbaum describes the Iraqi mission as one doomed to fail from the start—a "struggle between American will and the laws of gravity of the region." The U.S. involvement in the Israeli-Palestinian peace process is similarly described as an attempt to force dissimilar cultures to accept American concepts of negotiation, acceptance, and rule of law.

The thread that ties together *Mission Failure* is the repeating theme of disinterested, unfocused, and mismanaged foreign policy after the end of the Cold War. Describing an American public and government apparatus eager to return to domestic needs, Mandelbaum paints a picture of conflicts defined by ideology and not interests; of interventions run according to fickle domestic popularity; and, perhaps most damaging, of under-resourced and mismanaged missions, from Haiti, Somalia, and Bosnia to Iraq, Afghanistan, and the Israeli-Palestinian peace process. In his closing chapter, Mandelbaum describes a "restoration" of historic power politics and declares the end of the post-Cold War period of U.S. preeminence in world affairs. Ironically, Mandelbaum describes this return to form as an opening for the United States to revert to its interest-based roots—a conclusion that may assure students of history but leaves us wondering, who will fill that vacuum? JFQ

---

Bruno Carvalho is a graduate student in the School for Conflict Analysis and Resolution at George Mason University. He previously served 6 years with the U.S. Army.



### Margin of Victory: Five Battles that Changed the Face of Modern War

by Douglas Macgregor  
 Naval Institute Press, 2016  
 288 pp. \$34.95  
 ISBN: 978-1612519968

Reviewed by John Dethlefs

Douglas Macgregor's newest book offers a tutorial and blueprint for the strategically guided development of the U.S. military. This is timely, as the Department of Defense finds itself preparing for our future national defense strategy, which in the Barack Obama administration was often referred to as the Third Offset. Planning for it should be nested within the current and anticipated strategic environment, emerging technologies, and how we intend to fight our next war. Macgregor analyzes the preparation for, execution of, and consequences of belligerence in five significant battles. He also includes a chapter with recommendations (some of which are quite controversial) for the U.S. military's development.

In the opening chapter, the author recounts how Sir Richard Haldane, who

was appointed the British Secretary of War in December 1905, reformed the British army despite its well-established naval supremacy and significant spending restraints. After analyzing the strategic environment, Haldane concluded he did not know precisely which power or alliance Britain would face in the next war. He asked first-order questions: Whom do we fight? Where do we fight? And how do we fight? The reforms were nested under the answers to these questions. The subsequent battle of Mons in 1914 would reveal that Haldane's reforms served the British army well. The British Expeditionary Force proved to be strategically decisive in protecting France until the Allied powers, which eventually included U.S. forces, could defeat Germany.

Next, Macgregor details the Japanese rise to power and embrace of many Western ideas in the early 1900s. General Ugaki Kazushige "embodied the fight for change inside the Imperial Japanese Army (IJA)," as the Japanese struggled with reform and balancing resources between the navy and army. Much like Haldane, many of his reforms were resisted, blocked, or ignored by some military leadership. The subsequent battle of Shanghai in 1937 put these reforms to the test: "The disparity in Chinese and Japanese losses highlights the impact of Ugaki's modest modernization efforts and the high quality of Japanese troops and leadership, but the struggle for control of Shanghai was harder and bloodier than it should have been. The IJA had failed to change enough to achieve a true margin of victory." Herein lies a subtle warning to U.S. planners that they must be ruthless with our reform as we adjust to the new strategic environment and growing capabilities of possible adversaries.

The author next analyzes the modernization of the post-World War I Soviet and German forces and subsequent destruction of the German Army Group Center in June 1944 by Soviet forces in Eastern Europe. Macgregor argues the German defeat was decided well before any German forces entered the Soviet Union. The difference was

ultimately how the Soviets and Germans approached military reform based on desired strategy.

Before the war, “the idea of waging total war to make Germany a world power was absent from German strategic thinking.” Macgregor goes on to explain Adolf Hitler’s demand that officers obey orders without dissent and his replacement of very capable officers with obedient technocrats. Their efforts in developing mechanized forces did not go far enough, as the Wehrmacht remained too reliant on horses and light infantry. The Soviets made many mistakes (including their own purges of capable officers), but weather and distance granted them the time to recover and regenerate their officer corps. The Soviets ultimately learned from their mistakes more quickly and developed more strategic agility wherein a Soviet marshal had more joint command authority than General Dwight D. Eisenhower did or our current combatant commanders can. The subsequent warfare rewarded operational agility, mobility, protection, and firepower—attributes Macgregor contends are even more important today.

In assessing the Yom Kippur war in the Sinai in 1973, the success of Egypt’s reforms after its defeat in 1969–1970, coupled with Israeli complacency, almost led to an overwhelming victory for Anwar Sadat. However, Israeli culture, leadership, training, technology, and adaptability eventually turned the tide. Considering this battle, Macgregor contends that recent ideas to convert the Israeli army largely into a light force of riflemen that depends on airstrikes for effectiveness is perilous. He highlights the enduring Israeli principle that diversity of capability is vital to success and implies it should be copied. He correctly points out that unless Egyptian and Arab society changes in fundamental ways, they are unlikely to acquire the capabilities required for success in war against modern forces such as those of Israel.

The last battle analyzed is one that Macgregor participated in personally. The Battle of 73 Easting during Operation *Desert Storm* is regularly cited as an overwhelming success. While Macgregor

concurs with that assessment at the tactical level, he makes the argument that the campaign was a lost strategic opportunity for the United States. While successful, this battle did reveal flaws in our strategic thinking and execution. Macgregor contends that “although the twentieth century closed on a note of unrivaled American superiority in military affairs, the failure of policymakers and military leaders in Washington to define the purpose, method, and end state of military operations robbed the United States and its coalition partners of a decisive strategic victory.” He argues that U.S. aversion to risk allowed most of the Republican Guard to escape, ensuring Saddam Hussein would remain in power. From this, he claims that “the myth of the bloodless victory was born, and with it, the seductive promise of silver bullet technology that encourages arrogance and fosters illusions of victory with zero casualties was made.”

Macgregor concludes by looking at America’s “margin of victory” for the 21<sup>st</sup> century. He is quite critical of the current strategic direction. He correctly warns that “without effective strategic direction, battles such as 73 Easting can be won, but wars can still be lost.”

His more detailed recommendations are quite controversial. The first discusses the need for a change in U.S. national military strategy, contending that “the United States must act now to build the means of commanding its armed forces and impose unity of effort across service lines,” which he finds currently lacking. He writes expansively about ruthless reform focused on building joint integrated command structures at the operational level. This will improve American political and military leaders’ ability to comprehensively and decisively direct military power. Macgregor recommends that we have fewer command and control echelons, faster decision cycles, and more independence at lower levels, and that we become more mobile and dispersed. This is a direct challenge to the current “fighting by concept of operations,” in which four-star commands need approval for almost all actions in their own area

of responsibility and lower echelons face even greater micromanagement.

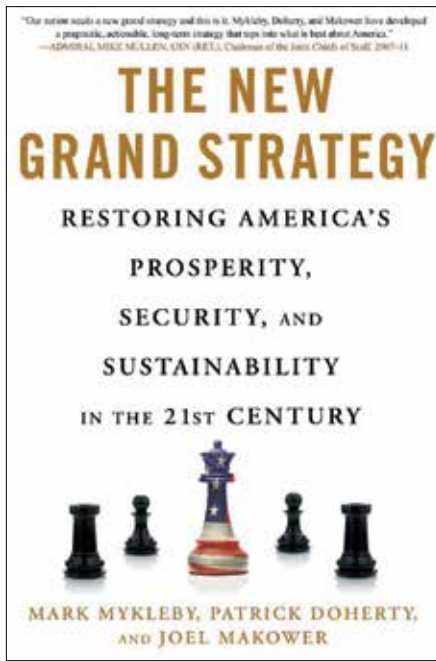
Macgregor recommends changing the way we fight, stating that “full spectrum military dominance on a global basis is both unaffordable and unnecessary,” which directly challenges our past emphasis on building global security. This makes sense in the face of decreasing budgets and changes in the strategic environment. Other recommendations include reducing the number of light infantry forces due to the increase in lethality of modern weapons and replacing them with more armored combat formations requiring fewer—but more mobile, protected, and lethal—people. Hardening or expanding intelligence, surveillance, and reconnaissance (ISR), communications, and space-based capabilities is important, as our potential adversaries arguably see disrupting these as the best method to gain parity with us.

Macgregor makes many profound recommendations based on significant historical evidence. This is a must-read for strategic leaders seeking ideas on military reform. In what I have read about future strategy and the defense innovation (including the Third Offset), few to none of Macgregor’s proposals are being considered. The focus is on technology improvements—mostly in regard to ISR and autonomous systems—and not the fundamental changes Macgregor champions. They deserve serious consideration. JFQ

---

Colonel John Dethlefs, USAR, is the Commander of the 209<sup>th</sup> Digital Liaison Detachment and a student at the U.S. Army War College.





## The New Grand Strategy: Restoring America's Prosperity, Security, and Sustainability in the 21<sup>st</sup> Century

By Mark Mykleby, Patrick Doherty, and Joel Makower

St. Martin's Press, 2016

288 pp. \$18.61

ISBN: 978-1250072306

Reviewed by Micheal D. Russ

In *The New Grand Strategy*, the authors correctly assert that the United States cannot rely on the bureaucracy of international and national entities to move forward and purposefully lead change, when and where it matters. This book is a call to action in which a synthesis of strategy, planning, and operations trumps analysis, avoids trivial pursuits, and catalyzes action by “we the people.” Whereas “grand strategy” is largely debated in academia and think tanks as an abstraction, strategy requires purpose and implementing operations. It also necessitates frequent institutional reflection, refinement, and changing of paradigms that inhibit the ability to adapt to a changing world order. Though the book may not account for every element

that could encompass “grand strategy,” its recommendation that strategy be purposeful, systematic, and forward thinking to ensure that resilience and sustainability are the foundation of longevity and continued greatness should be heeded.

*The New Grand Strategy's* key theme is that “we the people” must lead the shaping and rebuilding of the world, the bid for resilience and self-sustainability. For Americans, leading change begins in our own communities and by example, extending influence to all global residents. The days of expending vast amounts of time and resources on seemingly “important” current issues and treating symptoms must give way to addressing root causes and investing for the long term in our most precious asset, the human. Though the authors propose a way to address the challenges forecast in the 21<sup>st</sup>-century narrative, the nature (versus the character) of their argument is sound: addressing generational challenges, demand, and sustainability in a systematic solution that shows that “the whole [is] greater than the sum of its parts” is integral to collectively formulating strategy.

Within this theme, *The New Grand Strategy* addresses three aspects of today's environment and suggests how designing and implementing a strategy where the “representative democracy” supports “demand-plus-capital” sustainability is possible. The first section, “The Challenge of a Generation,” outlines the idea that implementing a plan to tap into the “vast stores of pent-up capital” in response to “new pools of demand” is a powerful mechanism for the rapid, sustainable growth of a “secure America.” The next section, “Pools of Demand,” shows that collective security is at risk due to the fact that it is caught in a whirlpool of self-centered activities that encourage and “incentivize waste” rather than reward “resource efficiency.” In the last section, “Full-Spectrum Sustainability” is touted as integral to multilevel community resilience and prosperity and focused on the long term rather than looking backward to “keystone industries designed for the last economic engine.” The authors also profess the need for

a “purpose driven application of . . . resources to . . . synergistically converge with, reinforce and leverage one another.” The major implication is that Americans need to create a cycle in which demand, skill, diversity, and global systems combine to ensure sustained, systemic resilience and prosperity becomes and remains the foundation to our security. This is a broader definition of grand strategy than many military readers will initially appreciate, but it bears strong consideration for our greater overall security.

The altruistic and idealist character of *The New Grand Strategy* may be both the strongest and weakest feature for readers. Ideas such as bringing together public, private, and civil sectors in an integrated and coordinated system and aligning long-term planning as the essence of community sustainability and resilience may be difficult to compartmentalize. Moreover, collectively understanding that efforts to impact and achieve successes at the local levels inevitably engender productivity at the highest levels of the Nation and world may be seen as a stretch to attain. However, this is the challenge the text argues we undertake with some urgency. I agree with the authors that the above is possible because Americans and global citizens embrace liberty and understand the communal aspect of preserving it community. It will take time to think, create, implement, and iterate a strategy that works.

*The New Grand Strategy* is pertinent to all sectors of society. When building resilient, sustainable communities, we can achieve positive, distinct gains for all citizens of the world when we strive for and achieve collective impacts. Moving forward to address generational challenges and the issues of demand and sustainability systematically is going to be difficult, but it is also our greatest responsibility. The authors are clear: with “a spirit of innovation, a stubborn grit, and an irrepressible belief that nothing is beyond our grasp,” we will move forward. JFQ

---

Lieutenant Colonel Micheal D. Russ, USMC, is the Associate Dean and Warfighting Department Head at the Marine Corps Command and Staff College, Marine Corps University, Quantico, VA.



AV-8B Harrier aircraft pilot with Marine Attack Squadron 211, Marine Aircraft Group 13, 3<sup>rd</sup> Marine Aircraft Wing (Forward), relocates Harrier to Camp Bastion, Helmand Province, to increase overall readiness level after September 14, 2012 attack (DOD/Keonaona Paulo)

# Improving Joint Doctrine for Security in Theater

## Lessons from the Bastion-Leatherneck-Shorabak Attack

By Nicholas J. Petren

In September 2012, Taliban insurgents conducted one of the most significant attacks against an airfield from which U.S. forces were operating since the Vietnam War. On September

14, 15 insurgents exploited a weakness in the perimeter of the sprawling Bastion-Leatherneck-Shorabak (BLS) complex to gain access and attack coalition equipment and personnel. Over the next 6 hours, responding U.S. and British personnel captured 1 attacker and killed the other 14. However, the insurgents were able to destroy six

Marine Corps AV-8B Harriers and severely damage two others. In addition, an Air Force C-130 Hercules, a C-12, three MV-22 Ospreys, and a British Sea King helicopter were damaged, while several aircraft shelters, hangars, fuel bladders, and other equipment in the area were damaged or destroyed. In all, the attack caused over

---

Major Nicholas J. Petren, USAF, is a student at the U.S. Army Command and General Staff College.

\$200 million in damage,<sup>1</sup> but the most tragic losses were two U.S. Marines, killed during the firefight that also injured 17 U.S. and British personnel.<sup>2</sup>

The causal factors permitting this attack to happen included a convoluted force protection task organization, lack of unit integration, and failure to identify a single tactical-level commander with the responsibility for base defense, all of which contributed to and were exacerbated by failures in risk management.<sup>3</sup> Complex operating environment or not, this tragic incident was avoidable. If the defending security forces were better organized and not decremented to the point that they were not reasonably capable of effectively maintaining a secure perimeter or dominating the terrain immediately around the base, the insurgents would have been much less likely to have gained access to the aircraft parking area.

Clearly, this incident required the assessment of responsibility. The U.S. commanders responsible for the defense of the BLS complex, Marine Corps Major Generals Charles Gurganus and Gregg Sturdevant, were censured and asked to retire following the completion of the U.S. Central Command (USCENTCOM) investigation. Furthermore, as the British House of Commons Defence Committee's report concluded:

*Insufficient attention was given to the fundamental requirement of defending Camp Bastion from external assault. We believe that this was complacent. Given that the attack took place in the British sector of the camp, British commanders must bear a degree of responsibility for these systemic failures.<sup>4</sup>*

It is evident that the risk management decisions of the British commander of Camp Bastion were found to be lacking.

Beyond individual accountability, an examination of the doctrinal and operational context is necessary in order to address shortcomings and decrease the possibility of similar incidents during future operations. Specifically, joint doctrine addressing security in theater must stress the importance of planning to secure strategic airfields and logistical hubs.

## Background

By September 2012, the International Security Assistance Force (ISAF) was in the midst of the drawdown from the Afghanistan surge and was under pressure to begin turnover of responsibility for security to the Afghan forces. The overall number of ISAF soldiers in Afghanistan was steadily drawing down from a high of more than 130,000; on September 10, the number stood at 112,579, with 74,400 of those from the United States.<sup>5</sup> The BLS complex (now called Camp Shorabak by the Afghan government) in Helmand Province was home to more than 20,000 coalition personnel. Major General Gurganus was commander of ISAF's Regional Command-Southwest (RC[SW]), headquartered on BLS. RC(SW) encompassed a 99,700-square-kilometer area made up of Nimruz Province and the troubled Helmand Province, with a host nation population of approximately 1.1 million.<sup>6</sup> RC(SW) was supported by the 3<sup>rd</sup> Marine Aircraft Wing (Forward), commanded by Major General Sturdevant, headquartered and primarily operating from BLS. In March 2012, RC(SW) included 17,800 U.S. Marines. By September 2012, there were 7,400.<sup>7</sup> This force drawdown necessitated operational and tactical force allocation and mission curtailment decisions. These decisions were risk management calculations, accounting for force protection. Major General Gurganus's higher commander, U.S. Army Lieutenant General James Terry, stated that "there was a constant balance between projecting forces and protecting the force during this period with priority to protecting the force."<sup>8</sup>

In terms of tactical elements organized to defend BLS, the base was a complex of camps grouped primarily in three areas. Camp Bastion, including the airfield, was operated and defended largely by British forces. Camp Leatherneck was the Marine Corps area, and Camp Shorabak was the Afghan National Army area. The entire complex was contained within a 37-kilometer-long perimeter. The security force (SECFOR) available included a broad array of

coalition forces and contractors that were not operating as one team. The interactions between these units were regulated by a memorandum of understanding, under which the Camp Bastion and Camp Leatherneck SECFOR operated independently with separate standard operating procedures and did not effectively coordinate perimeter surveillance or patrol activity on and off base.

Camp Bastion was defended by a 134-person unit from the Royal Air Force (RAF) regiment, assisted by an augmenting force drawn from other assigned units along with a small force of the Tongan Defense Services. The RAF provided headquarters, a quick reaction force (QRF), and patrols, while the Tongans and the augmentation force personnel manned the perimeter towers. Of the 24 towers on Camp Bastion, only 11 were routinely manned due to a lack of available personnel, a risk accepted by the RAF Camp Bastion commander.<sup>9</sup>

The Camp Leatherneck defense comprised 255 contractors, a 288-person force from the Jordanian military, a 105-member element from the Bahraini armed forces, and a 110-member team from 2<sup>d</sup> Battalion, 10<sup>th</sup> U.S. Marine Regiment (2/10), a field artillery unit.<sup>10</sup> The contractors and non-U.S. military personnel manned entry control points, perimeter towers, and provided internal QRF for Camp Leatherneck, while the Marines performed a myriad of security-related tasks. Camp Shorabak (formerly Camp Bastion) is an Afghan ministry of defense airbase located northwest of the city of Lashkar Gah, in Helmand Province, and the 2/10 commander had primary responsibility for off-base patrolling in the approximately 1,000-square-kilometer area of operation (AO) surrounding BLS.<sup>11</sup> The task force responsibilities included "providing [field artillery] support for Task Force (TF) Leatherneck, operating the Combined Joint Operations Center (CJOC), manning [entry control points] on Camp Leatherneck, manning a QRF, manning Patrol Base Boldak, and manning the Tactical Recovery of Aircraft and Personnel (TRAP) mission."<sup>12</sup> Due to their varied responsibilities, the 110

members of 2/10 could only generate one squad per 24-hour period to patrol off base. The RAF regiment element was able to generate one to three squad-sized patrols as well, but their activity was not consistent or effectively integrated with U.S. security forces. Although the CJOC existed in order to coordinate force protection activity and performed in that task during the attack, coordination was primarily reactive, as structured in the memorandum of understanding. If the combined manpower available for force protection had operated as a single, effective unit, the BLS perimeter would likely have been more secure.

In June 2012, a Joint Staff Integrated Vulnerability Assessment (JSIVA) team visited Camp Leatherneck and Bastion airfield. The team concluded that the airfield's security was inferior to that at Bagram Airfield and identified six vulnerabilities. Further, the team "assessed the two routine patrols assigned to the airfield as largely ineffective from a preventative/detection perspective, primarily because of the size of the airfield and ramps, the aircraft dispersion, the lighting, the lack of detection and warning systems in place," and "not being able to control access (vehicle and pedestrian) to the airfield."<sup>13</sup>

During June and July 2012, Camp Bastion perimeter breaches were discovered after the fact but were accepted by the 3<sup>rd</sup> Marine Air Wing and RAF Camp Bastion commanders as criminal "scraping" rather than evidence of insurgent probing of perimeter defenses in preparation for an attack.<sup>14</sup> The July breach was performed by individuals who penetrated the same area of Camp Bastion targeted in the September 2012 attack and then exited the base through their breach point undetected. Surveillance video of another breach revealed reconnaissance of an empty guard tower.<sup>15</sup>

## The Attack

The Taliban attackers were provided with intelligence on their targeted area of the Camp Bastion airfield. They were transported to just outside the camp, where they donned U.S. Army uniforms. At approximately 2000 hours,

they made their way toward the Camp Bastion perimeter using a ravine to mask their approach. They were armed with AK-47s, rocket-propelled grenades (RPGs), and fragmentation grenades, and some of the attackers were huffing paint. On that night, there was 2 percent illumination, and per Camp Bastion standard operation procedures, only every other perimeter tower was manned.<sup>16</sup> The insurgents breached the perimeter fence with wire cutters 150 meters from unmanned tower 16 and entered the base undetected to begin their attack at approximately 2200. They split into three groups of five, targeting Harriers, helicopters, and personnel, respectively. After the insurgents started shooting, it took 16 minutes for the first elements of the Camp Bastion QRF to make contact with the enemy. Over the next few hours, the insurgents caused the damage described earlier before 14 of them were neutralized by RAF, Marine Corps, and Air Force personnel on the ground with supporting fire from attack helicopters, while the fifteenth was captured wounded. Post-attack analysis showed the attackers used Soviet-era F1 grenades to destroy the Harriers, meaning they were close enough to accurately roll, throw, or place them under the aircraft.<sup>17</sup> This is significant because it illustrates the failure of the combined elements of the Camp Bastion SECFOR or organic units to detect the approach of the Taliban, their breach of the perimeter, or their free movement around the Harriers on the flight line until the attack was under way. Furthermore, the initial contact with the enemy and disruption of the Taliban attack was conducted by maintenance/support personnel and pilots of the 3<sup>rd</sup> Marine Air Wing rather than base SECFOR. During the attack, integration of highly effective fire from Marine aviation was as much the result of ad hoc coordination by Marines and Airmen who rose to the occasion as it was a controlled integration of fires in the BLS CJOC.

As the USCENTCOM report states, "Only heroic action by U.S. and UK forces on the scene prevented greater

loss of life and equipment."<sup>18</sup> Of note, Lieutenant Colonel Christopher Raible, the Harrier squadron commander, was killed while valiantly leading the charge to defend his aircraft and fellow Marines along with Sergeant Bradley Atwell. The Air Force pararescue team that voluntarily ran into the firefight and played an important role in defeating the attackers by coordinating with attack helicopters and participating in clearing operations with the RAF QRF is another example of the day's heroic actions.

## Improving Joint Doctrine

Doctrine is relevant to the tactical-level decisions of base defense because it guides how leaders in the joint force think about and prepare for expeditionary base defense. The 2014 version of Joint Publication (JP) 3-10, *Joint Security Operations in Theater*, incorporated numerous constructive updates based on lessons learned in Operation *Iraqi Freedom* (OIF) and Operation *Enduring Freedom* (OEF). However, given the likelihood of similarly complex joint interagency intergovernmental multinational operations in the future, there is still room for significant improvement.

First, large, joint-use airfields, often collocated with equally critical ground force-operated sustainment hubs, are often the primary platforms from which the force projects military power across joint operational areas or theaters, and their protection must be a priority. This must be formally acknowledged and planned for in initial phases of joint operations planning. Defending these types of bases or base clusters is critical across the spectrum of conflict. Surely, they will appear on a near peer enemy's high value target list equivalent, just as they will continue to be targeted by insurgent or terrorist forces. JP 3-10 states that when facing Level I and II threats (including terrorists or enemy special operations forces), commanders should organize security forces "drawing from the units available."<sup>19</sup> This is appropriate for small command observation posts or forward operating bases in lower threat environments, but for large air bases or sustainment hubs, it exacerbates the



Marine with Mobile Assault Platoon 4, Weapons Company, 1<sup>st</sup> Battalion, 25<sup>th</sup> Marine Regiment patrols southern Washir District, Helmand Province, October 2, 2011

tension between projecting power and force protection. JP 3-10 should direct commanders to incorporate all available units into base security plans but not to draw from them as the primary source of SECFOR. Units tasked as SECFOR must be specifically identified, trained, and deployed for that mission. This will provide commanders in theater the flexibility to shift focus without taking imprudent risk.

Second, doctrine must stress the need for a single commander at the appropriate level with the authority and responsibility over not only the base or base cluster, but also the surrounding tactically relevant AO. JP 3-10 currently includes “Air Base Defense Considerations”<sup>20</sup> and the “establishment of base and base cluster command relationships,”<sup>21</sup> directing “it is critically important that the JFC [joint force commander], normally through the JSC [joint security coordinator], delegate the authority to conduct JSO

[joint security operations] within the base boundary<sup>22</sup> to a single commander.”<sup>23</sup> These are valuable improvements to the document, but some thorny issues remain unresolved. For example, the challenge of incorporating coalition forces is addressed only superficially. It is understood that U.S. joint doctrine only applies to U.S. forces. However, joint doctrine should clearly direct commanders to ensure a single commander retains tactical control of all coalition forces incorporated into a base cluster SECFOR. The United States should be more insistent on this when it comes to national caveats or coalition command and control arrangements. Rather than dismissing this assertion as politically naive, challenge others to justify why irresponsibly vague command structures are acceptable. In the case of BLS, the USCENCOM report stated that “the BLS Complex also lacked a single commander with unity of

command. . . . Unity of command would have provided the single commander with common oversight and enforcement of standards for all units responsible for protection of the BLS Complex.”<sup>24</sup> If current or future leaders see a fragmented SECFOR chain of command or lack of organization similar to that which existed at BLS prior to the 2012 attack, red flags should immediately go up, and corrective action must be taken promptly.

Lastly, the joint force must overcome cultural resistance to expanding the base boundary of critical air bases in theater based on threat, vulnerability, and terrain analysis. Currently, the concept of expanding the base boundary is included in JP 3-10 as something commanders should “consider.” Rather, it should be the preferred procedure, while retaining the flexibility to adjust due to local conditions. A base commander with base defense as a key component of the



Security during Relief in Place ceremony at Base Defense Operations Center, Camp Leatherneck, Afghanistan, to commemorate Transition of Authority from 1<sup>st</sup> Battalion, 23<sup>rd</sup> Marines to 1<sup>st</sup> Battalion, 25<sup>th</sup> Marines, September 13, 2011 (Royal Air Force/Mitch Moore)

mission will have the focus and ability to drive intelligence-based operations to reduce indirect, direct, small unmanned aerial systems, and improvised explosive device (IED) attacks affecting the area. For proof, one needs to look no further than the success of Task Force 1041 at Joint Base Balad during OIF or Task Force 455 at Bagram Air Base during OEF.

In late 2004, Balad Air Base was under frequent indirect fire attack and located in one of the region's most violent areas.<sup>25</sup> Balad Air Base had an effective perimeter defense, but the base commander had no authority outside of it. After successful negotiations with higher and adjacent commanders, the base commander was granted the authority to temporarily expand the base boundary. Task Force 1041 consisted of a reinforced company-sized element whose mission was to operate off base in a 5-by-10-kilometer area between the base perimeter and the Tigris River, where the majority of indirect fire and IED attacks affecting base operations originated. After focused intelligence preparation, Operation *Desert Safe Side* commenced on January 1, 2005. Over the next 60 days Task Force 1041 captured 17 high-value individuals, 98 other insurgents, and 8 major weapons caches.

Indirect fire attacks on the base and other attacks inside TF 1041's AO were reduced to nearly zero.<sup>26</sup>

In part, due to this demonstrated success, when Joint Base Balad was later reorganized in 2008 under the command of the 332<sup>nd</sup> Expeditionary Air Wing, the 332<sup>nd</sup> Expeditionary Security Forces Group (ESFG) stood up. Its commander was an O-6 leading a nearly 1,000-person coalition SECFOR team focused on the mission of defending Joint Base Balad.<sup>27</sup> This combination of unity of command, authority, responsibility, and clear task organization set conditions for effective base defense. While the ESFG achieved notable results, inconsistent willingness to more permanently expand the base boundary around Balad remained problematic.

Bagram Air Base was mentioned in the 2012 Leatherneck JSIVA report as an example of superior perimeter security. In May 2010, the Taliban conducted an attack on Bagram Air Base that was more determined than the September 2012 attack on BLS. Between 20 and 30 Taliban insurgents assaulted the base around 0300 hours.<sup>28</sup> They were armed with AK-47s, RPGs, and hand grenades, and were supported by coordinated indirect fire. The attackers were wearing U.S. military uniforms, and some were

wearing suicide vests. They attempted to breach the perimeter in two separate locations simultaneously.<sup>29</sup> In contrast to the BLS incident, the attackers were detected outside the perimeter and were defeated before they could penetrate the base defenses. Sixteen of the attackers were killed in the firefight.<sup>30</sup> The attack failed to inflict any major damage to the base, although nine friendly personnel were injured. A critical factor that contributed to a better outcome than the BLS attack was clear responsibility and authority for base defense. The 455<sup>th</sup> Air Expeditionary Wing commander was the base commander responsible for base defense, and the SECFOR was led by the 455<sup>th</sup> Expeditionary Security Forces Squadron (ESFS) commander. The ESFS was responsible for the perimeter defense, internal QRF, and screening of personnel and vehicles entering base. The 455 ESFS also operated the joint defense operations center, which effectively coordinated support from Air Force aircraft, Army aviation, and Army ground units operating outside the perimeter during the attack. In order to build upon this success and better defend the largest coalition military operating location in Afghanistan, in November 2012 Task Force 455 stood up. The initial 1,200-member 455<sup>th</sup> Expeditionary Security Forces Group evolved into a 2,200-person Expeditionary Base Defense Group (EBDG) and Combined Joint Task Force with the addition of a U.S. Army field artillery battalion, a Jordanian infantry battalion, and a Czech Republic force protection company. Tasked to defend Bagram and patrol the surrounding AO, the 455 EBDG commander effectively operated as a brigade-level battlespace owner under the tactical control of the 101<sup>st</sup> Airborne Division (Air Assault)/Regional Command East commanding general within a 570-square-kilometer area.<sup>31</sup>

This evolution of command structures and responsibilities evolved at Joint Base Balad and Bagram from lessons learned, and they should serve as positive examples of large base defense in theater. This is not to say that each should be replicated exactly in the future, but the basic model of unity of base defense responsibility,

authority, command, and effort is critical to success and applicable to joint or coalition forces. The Air Force uses the term *base security zone* to describe the area outside of the base perimeter fence/obstacle line from which enemy forces could attack the base or affect air operations using standoff threats. This concept is not unique to the Air Force as it is equally important to all large joint use bases supporting joint operations. The base security zone should be identified during a terrain and threat analysis and be used to modify the base boundary as described in JP 3-10 to enable effective base defense operations driven by a single commander at the appropriate tactical level.

## Conclusion

U.S. forces took courageous action during attacks on Bagram, Joint Base Balad, and BLS. In 2010 at Bagram, a complex attack was defeated without significant impact on coalition operations, and Balad was never penetrated by a significant insurgent force. Both stand in stark contrast to BLS, where the appearance of a secure perimeter did not withstand scrutiny. The key differences at BLS were the fragmented base defense chain of command, incoherent responsibility for security below the two-star RC(SW) level, and lack of SECFOR integration. These factors, combined with optimistic risk management decisions by key leaders, left the base vulnerable to enemy attack.

In future operations, enemies will continue to target critical coalition air and logistics hubs in theater in order to disrupt our ability to project power and sustain operations. During major combat operations, these threats will likely include unconventional means such as enemy special operations forces or proxy insurgent/terrorist groups, in addition to conventional attack. Future attackers may be much better trained and prepared than those at BLS in 2012. Therefore, effective integrated base defense planning and execution in theater are critical across the spectrum of conflict and must not be dismissed as an exercise in preparing for the last war.

We can do better to set up future commanders for success by improving JP 3-10 to increase the likelihood of sound risk management and coherent, tactically effective base defenses around our power projection platforms in theater. Our responsibility to current and future Soldiers, Marines, Sailors, and Airmen demands no less. JFQ

---

## Notes

<sup>1</sup> Alissa J. Rubin, "Audacious Raid on NATO Base Shows Taliban's Reach," *New York Times*, September 16, 2002, available at <[www.nytimes.com/2012/09/17/world/asia/green-on-blue-attacks-in-afghanistan-continue.html?pagewanted=all&\\_moc.semityn.www](http://www.nytimes.com/2012/09/17/world/asia/green-on-blue-attacks-in-afghanistan-continue.html?pagewanted=all&_moc.semityn.www)>.

<sup>2</sup> "Army Regulation (AR) 15-6 Investigation of the 14-15 September 2012 Attack on the Camp Bastion, Leatherneck, and Shorabak (BLS) Complex, Helmand Province, Afghanistan," August 19, 2013, 2.

<sup>3</sup> *Ibid.*, 23-31.

<sup>4</sup> House of Commons, Defence Committee, "Afghanistan—Camp Bastion Attack," April 16, 2014, 15.

<sup>5</sup> "ISAF: Key Facts and Figures," September 10, 2012, available at <[www.nato.int/isaf/placemats\\_archive/2012-09-10-ISAF-Placemat.pdf](http://www.nato.int/isaf/placemats_archive/2012-09-10-ISAF-Placemat.pdf)>.

<sup>6</sup> Institute for the Study of War, "Regional Command South," 2009, available at <[www.understandingwar.org/region/regional-command-south-0](http://www.understandingwar.org/region/regional-command-south-0)>.

<sup>7</sup> Jim Michaels, "Two Generals Asked to Retire in Wake of Bastion Attack," *USA Today*, September 30, 2013, available at <[www.usatoday.com/story/news/world/2013/09/30/bastion-marines-afghanistan-gurganus/2897953/](http://www.usatoday.com/story/news/world/2013/09/30/bastion-marines-afghanistan-gurganus/2897953/)>.

<sup>8</sup> AR 15-6, 7.

<sup>9</sup> *Ibid.*, 8.

<sup>10</sup> *Ibid.*, 9.

<sup>11</sup> Katherine Keleher, "Task Force Belleau Wood Marines, Partners Celebrate Corps' 236<sup>th</sup> Birthday," November 12, 2011, available at <[www.iimef.marines.mil/News/NewsArticle/tabid/472/Article/528985/task-force-belleau-wood-marines-partners-celebrate-corps-236th-birthday.aspx](http://www.iimef.marines.mil/News/NewsArticle/tabid/472/Article/528985/task-force-belleau-wood-marines-partners-celebrate-corps-236th-birthday.aspx)>.

<sup>12</sup> AR 15-6, 10.

<sup>13</sup> *Ibid.*, 17.

<sup>14</sup> House of Commons, 12.

<sup>15</sup> AR 15-6, 18.

<sup>16</sup> *Ibid.*, 22.

<sup>17</sup> *Ibid.*, 6.

<sup>18</sup> *Ibid.*, 2.

<sup>19</sup> Joint Publication (JP) 3-10, *Joint Security Operations in Theater* (Washington, DC: The Joint Staff, November 13, 2014), xiv-xv.

<sup>20</sup> *Ibid.*, IV-17.

<sup>21</sup> *Ibid.*, II-11.

<sup>22</sup> JP 1-02, *Department of Defense Dictionary of Military and Associated Terms* (Washington, DC: The Joint Staff, November 8, 2010, as amended through February 15, 2016). The DOD dictionary defines the *base boundary* as "a line that delineates the surface area of a base for the purpose of facilitating coordination and deconfliction of operations between adjacent units, formations, or areas."

<sup>23</sup> JP 3-10, II-12.

<sup>24</sup> AR 15-6, 26.

<sup>25</sup> Air Force Manual 31-201, *Security Forces History*, vol. 1 (Washington, DC: Department of the Air Force, June 1, 2015), 16-17.

<sup>26</sup> *Ibid.*, 17.

<sup>27</sup> *Ibid.*

<sup>28</sup> Amir Shah et al., "Taliban Attack Key U.S. Base in Afghanistan, Killing 1 U.S. Contractor, Wounding 9 Troops," Associated Press, May 18, 2010, available at <[www.foxnews.com/world/2010/05/18/insurgents-launch-complex-attack-bagram-air-field.html](http://www.foxnews.com/world/2010/05/18/insurgents-launch-complex-attack-bagram-air-field.html)>.

<sup>29</sup> Joint Training Counter IED Operations Integration Center, Sims Directorate Video, "Airfield Complex Attack, Bagram Airfield Afghanistan," December 5, 2011.

<sup>30</sup> *Ibid.*

<sup>31</sup> Christopher J. Willis, "Bagram Security Forces Group Stands-Up," Defense Video Imagery Distribution System, January 1, 2013, available at <[www.dvidshub.net/news/104996/bagram-security-forces-group-stands-up](http://www.dvidshub.net/news/104996/bagram-security-forces-group-stands-up)>.

Sailor in hangar bay of aircraft carrier USS Dwight D. Eisenhower maintains E2-C Hawkeye assigned to the Screwtops of Airborne Early Warning Squadron 123, October 10, 2016 (U.S. Navy/Joshua Murray)

# Joint Publication 3-20, *Security Cooperation* Adapting Enduring Lessons

By Keith D. Smith, Mark H. Lauber, and Matthew B. Robbins

---

Keith D. Smith is a Senior Analyst in the Joint Center for International Security Force Assistance at Joint Staff J7 Joint Force Development. Mark H. Lauber is a Senior Special Operating Forces Analyst in the Joint Center for International Security Force Assistance. Lieutenant Colonel Matthew B. Robbins, USMC, is a Joint Doctrine Development Officer in the Joint Doctrine Analysis Division at the Joint Staff J7 Joint Education and Doctrine Division.

Today's security environment demands that the Department of Defense (DOD) employ a robust strategy and assortment of capabilities across the entire range of military operations and in support of America's national security interests. A preponderance of these activities falls under the umbrella of security cooperation (SC) in which few, if any, U.S. forces participate directly in combat operations. As DOD

continues to develop the "four plus one" threat baseline described by the Chairman of the Joint Chiefs of Staff, the Joint Force Development Directorate has taken steps to better align joint doctrine with the National Military Strategy as part of an approach that emphasizes the need for adaptive doctrine.<sup>1</sup> Within this effort, the need to synergize U.S. capacity and capabilities with those of its partners remains paramount.<sup>2</sup>



To this end, ongoing efforts to adapt the disparate entities and authorities associated with SC into a unified strategy serve as an important next step. In 2008, DOD published a directive that elevated the requirement for DOD expertise for SC activities to the same level as other “integral [conventional] DOD activities.”<sup>3</sup> To achieve parity, the Joint Doctrine Development Community (JDDC) identified the need to incorporate the topic of SC into the joint publication library as Joint Publication (JP) 3-20, *Security Cooperation*. The approval of JP 3-20 is a major step toward the joint force recognizing SC as a way to apply the military instrument of national power in support of partner nations (PNs) around the globe to achieve strategic objectives and to help shape the operational environment for current and future operations. This article outlines the continued adaptation of SC and the inextricable doctrinal security force assistance (SFA) principles discussed in JP 3-20 that are applicable to the joint force.

JP 3-20 defines *security cooperation* as “all DOD interactions with foreign security establishments to build security relationships that promote specific U.S. security interests, develop allied and friendly military capabilities for self-defense and multinational operations, and provide U.S. forces with peacetime and contingency access to a partner nation.”<sup>4</sup> These three categories, however, only hint at the true breadth and complexity of activities that make up the universe of security cooperation. Some SC activities are simple engagements between U.S. and PN defense officials, while others are complex and may include multibillion-dollar arms negotiations brokered at the highest levels of government through DOD-administered and Department of State-led security assistance (SA) programs under U.S. Code Title 22 authority. These examples bracket the more common theater security cooperation exercises routinely conducted within each geographic combatant command’s area of responsibility. While the recent and formal incorporation of SC into joint doctrine may appear new, the United States has used various adaptations of SC to protect and advance its vital interests abroad for decades.

## Historical Overview

In 1971, the Secretary of Defense established the Defense Security Assistance Agency (DSAA) to direct, administer, and supervise the execution of approved SA plans and programs, such as military assistance, international military education and training, and foreign military sales.<sup>5</sup> In November 1997, the Defense Reform Initiative transferred additional responsibility for program management of humanitarian assistance and demining, armaments cooperation, export loan guarantees, and foreign comparative testing functions, along with their associated personnel and resources, to DSAA. In October 1998, SC officially entered the DOD lexicon, accommodating the scope of these additional functions beyond DSAA’s traditional SA missions. This expansion of mission necessitated a name change, hence DSAA’s redesignation as the Defense Security Cooperation Agency.<sup>6</sup> This consolidation of similar programs from five dissonant agencies into one stand-alone entity reflected efforts to improve efficiency and reduce administrative redundancy.

However, SC did not appear in mainstream joint doctrine until manifested in a 2004 revision of JP 3-07.1, *Joint Tactics, Techniques and Procedures for Foreign Internal Defense (FID)*. As the JDDC struggled to refine doctrinal treatment of SC, amended versions of then-JP 1-02, *Department of Defense Dictionary of Military and Associated Terms*, revealed continuing efforts to clarify myriad SC activities. Though not retained in the current JP 1-02, the meaning behind the original definition of SC activity prevails:

*Military activity that involves other nations and is intended to shape the operational environment in peacetime. Activities include programs and exercises that the U.S. military conducts with other nations to improve mutual understanding and improve interoperability with treaty partners. They are designed to support a combatant commander’s theater strategy as articulated in the theater security cooperation plan.*<sup>7</sup>

Today, SC more broadly supports the combatant command’s entire theater campaign plan.

Subsequent developments in SC further expanded its scope by adding authorities from U.S. Code Title 10 for programs such as multinational exercises—a move designed to gain synergy by coordinating peacetime Title 10 activities with Title 22 activities. Amended in the reformative aftermath of the Vietnam War, these Title 22 programs specifically precluded the United States from employing its forces in harm’s way using SA funds. This contributed to a misunderstanding of both SA and SC as exclusively peacetime activities. This inaccurate conclusion led to confusion regarding *when* and *how* SA and SC authorities and programs could and should be used. Originally designed to limit American participation in conflict, modern versions of the vintage U.S. Lend-Lease program, as the precursor to what we now know as SA, continue to evolve, but still contribute to the development of our foreign partners’ security force capacities and capabilities across the entire range of military operations.

The term *security force assistance* entered the DOD lexicon to provide greater depth to the SC pillar of developing PN capabilities. SFA was coined (after early efforts in Iraq failed to create a viable security force) to provide U.S. forces with applicable means for developing the capacity and capabilities of PN forces and their supporting institutions. The training of foreign security forces is a primary role of U.S. special operations forces. However, special operations forces were stretched to their limits conducting counterterrorism and counterinsurgency operations throughout the Iraq and Afghanistan theaters of operation and elsewhere. In response, significant numbers of conventional forces were indoctrinated to conduct SFA activities and further doctrine was developed. The initial incorporation of SFA into the 2010 replacement for JP 3-07.1, known after as JP 3-22, *Foreign Internal Defense*, defined it as DOD “activities that contribute to unified action by the U.S. Government to support the development

of the capacity and capability of foreign security forces and their supporting institutions.” Essential to SC, this streamlined definition established the enduring relevance of SFA, and subsequently SC, in all circumstances where U.S. military forces must develop foreign security force (FSF) capabilities.

### SC and SFA in the Current and Future Operating Environment

While SC and SFA remain important to steady-state operations, they are equally valuable in support of major combat operations because they can facilitate operational access and improved military relations and interoperability. Whether considering their preemptive use to shape the operational environment, provide trained and ready forces to participate in operations, or create a postconflict application to lay the foundations for lasting peace and regional stability, SC and SFA present irreplaceable mechanisms for achieving conditions conducive to U.S. national interests.

As history shows, improving the security capacity and capabilities of U.S. allies and partners contributes significantly to both the PN security strategies as well as U.S. national interests. Repeatedly, U.S. Presidents have illustrated the connection between the two. In March 1959, President Dwight D. Eisenhower conveyed to Congress that “we cannot safely confine government programs to our own domestic progress and our own military power. We could be the wealthiest and the most mighty nation and still lose the battle of the world if we do not help our world neighbors protect their freedom.”<sup>8</sup>

Decades later, a White House fact sheet detailing the U.S. Security Sector Assistance Policy from 2013, known as Presidential Policy Directive–23 (PPD-23), read as follows:

*The United States has long recognized that the diversity and complexity of the threats to our national interest require a collaborative approach, both within the United States Government and among allies, partners, and multilateral organizations.*

*U.S. assistance to build capabilities to meet these challenges can yield critical benefits, including reducing the possibility that the United States or partner nations may be required to intervene abroad in response to instability.*<sup>9</sup>

Implied in these statements from two different Presidents—who were separated by generations—is the fact that the United States faces a unique set of security challenges. Today, they are budgetary constraints and threats that are increasingly complex, transregional, multidomain, and multifunctional. Management of these challenges and associated threats demands greater innovation and a higher degree of efficiency in mastering SFA activities and SC as force multipliers, shapers, and stabilizers.

SC and SFA will continue to be necessary in the future operating environment, as characterized by persistent disorder and contested norms.<sup>10</sup>

**Persistent Disorder.** Within the context of violent ideological competition, the *Joint Operating Environment 2035* highlights identity networks as key actors. Much like nonstate actors, identity networks may be activated, guided, and directed by states to perpetuate chaos and disorder. These networks, and the individuals identifying with them, cross geographical boundaries and exploit the information environment, requiring more robust allied and PN security institutions to thwart their attacks and facilitate a more enduring peace and stability. Well-trained and properly equipped internal security forces, supported by the appropriate institutional backbone, help to reduce these types of threats. JP 3-20 enables the joint force to tailor SC and SFA activities to develop just such PN capacity and capabilities to defeat these increasingly advanced threats.

**Contested Norms.** State and nonstate actors will continue to threaten U.S. territory and sovereignty, thus necessitating increased efficiency and tempo in SC and SFA activities. The permeability of U.S. borders may lead the joint force to enhance cooperation with its neighbors and partners in Central, South, and North America. Continued Russian and

Chinese activity in the Arctic may lead to increased collaboration with Canada. Transregionally, hybrid attacks conducted against global trade and logistics nodes, but below the traditional U.S. threshold for military involvement, may warrant further development of partner capacity and capabilities to secure and defend these assets. JP 3-20 provides doctrinal guidance upon which combatant command planners can build an operational framework to support U.S. defenses against such threats.

Foreseeable manifestations of these distinctive challenges will require more than raw U.S. military capability and will demand a more comprehensive solution. As the draft copy of the *Capstone Concept for Joint Operations* notes, “The contexts of conflict represent a complex mix of diplomatic, informational, economic, and social problems. . . . The military can enable stable conditions in which to address these problems, but whole of government efforts are better suited to solve them.”<sup>11</sup> One shortcoming in the creation of a truly whole-of-government effect has been lexicon. Interagency coordination faces great obstacles when even understanding the multitude of DOD terms associated with SC tends to cause more than a little confusion. The 2011 *DOD Security Force Assistance Lexicon Framework*, written in response to an SFA doctrine, organization, training, materiel, leadership and education, personnel, and facilities (DOTMLPF) change recommendation and Joint Requirements Oversight Council memorandum, should have provided just such an approach given its intent to “develop a framework that reconciles/clarifies SFA with overlapping and related terms.”<sup>12</sup> As early as 2012, the U.S. Government Accountability Office highlighted “the value of distinguishing security force assistance from other security cooperation activities.”<sup>13</sup> Soon after, the Joint Staff J7, Joint and Coalition Warfighting Directorate, conducted a front-end analysis that prompted a 2012 special study titled *Security Force Assistance in Joint Doctrine* “to determine the proper place and amount of doctrinal guidance



MH-60R Sea Hawk helicopter assigned to Vipers of Helicopter Maritime Strike Squadron 48 conducts vertical replenishment training aboard guided-missile cruiser USS *Monterey*, Gulf of Oman, November 21, 2016 (U.S. Navy/William Jenkins)

on security cooperation, SSR [security sector reform], SFA, and FID.”<sup>14</sup> Despite the eventual decision within the JDDC to develop JP 3-20, many of the deliberations captured in this special study persist.

Because of its continued adaptation in policy and practice without a doctrinal anchor point, various interpretations of SC and its application have developed over time and still complicate understanding of the many terms related to its policies, programs, and authorities. Such contention explains the conspicuous omission and intentional exclusion of much of the content of that original lexicon discussion. Despite assuming the doctrinal responsibility for SFA and promoting an articulation of the functional relationships among SC, foreign assistance, security assistance, SFA, and FID, JP 3-20 relegated the opportunity

to clarify the joint force’s understanding of these relationships to JP 3-22, *Foreign Internal Defense*. Complete resolution of these complex relationships is tied to current and future policy. The introduction of any subsequent terms or broader doctrinal content should reflect a common understanding between multiple departments, as illustrated in PPD-23. However, facilitating that common understanding is traditionally beyond the scope of an operational-level publication.

With that in mind, JP 3-20 cursorily describes the sometimes hierarchical, sometimes conditional, and sometimes functional relationships among the SC- and SFA-related programs and authorities applicable to them. It does, however, include appendix B, which explains two particular SFA models relevant to developing a viable and lasting security force. The first of these models represents the

executive, generating, and operating (EGO) functions that must be performed by any effective security force, while the latter addresses the organize, train, equip, rebuild/build, and advise (OTERA) tasks associated with the conduct of SFA. EGO depends upon the delineation of responsibilities for DOD as written in U.S. Code Title 10. While many nations may not want their defense apparatus to mimic DOD, nor even possess the resources to build similar organizations, they will need to perform these basic functions effectively in some way or fashion. When the United States has determined that it will help a PN build capabilities, it must consider which EGO function(s) require assistance. Crafted to leverage expertise not available within U.S. operating forces, defense institution building specifically addresses the development of capacity and capabilities at the ministerial level.



U.S. and Royal Thai marines participate in Indo-Asia-Pacific region exercise Cobra Gold, February 14, 2017, Ban Chan Krem, Thailand (U.S. Marine Corps/Tiffany Edwards)

At this point, a second doctrinal SFA model enables the United States to apply personnel and other resources as the means to conduct SFA activities through one or more of the OTERA tasks. These tasks roughly align with the DOTMLPF and policy mechanisms of change used for U.S. joint force development, though formatted as tasks for execution. Not yet recognized for inclusion in JP 3-20, another SFA model offers a potential solution to synchronizing U.S. activities according to the level of development of the FSF. The development of additional capacity and capabilities follows a distinctive pattern involving five concurrent stages with common activities: Plan, Generate, Employ, Transition, and Sustain (PGETS).

During the Plan stage, an assessment with the PN is conducted to help determine what the FSF must do to fulfill its role as a security force. Though planning and resourcing activities comprise the bulk of the activities during this stage, they span all five stages. The majority of the activities accomplished during the “Generate” stage contribute to building the required capacity and capabilities for

the PN. The “Employ” stage results in application of generated capacity or capabilities toward their intended purpose. The “Transition” stage shifts responsibility for the generating and operational functions to the PN. The “Sustain” stage recognizes PN achievement of self-sustaining capacity and capabilities across the EGO functions. This PGETS model applies to the development of an individual capability or an entirely new security force (see figure).

In form, the PGETS model evokes the familiar joint operation phasing model as discussed in both JP 3-0, *Joint Operations*, and JP 5-0, *Joint Planning*, but transcends the doctrinal limitations of its designed application at the operational and tactical levels of joint operations. It also complements the JP 3-22 efforts to encapsulate an updated and viable framework or lexicon for SC and SFA at this same level. By bridging the political and strategic levels where the preponderance of SC guidance originates with operational- and tactical-level details, the PGETS model facilitates a linkage not fully reflected in JP 3-20, whereby the *Department of Defense Guidance for*

*Security Cooperation* establishes policy that “prioritizes the outcomes that security cooperation efforts should seek to achieve and provides additional guidance to the security cooperation enterprise on Department-wide expectations for planning, assessing, monitoring, and evaluating (AME) security cooperation.”<sup>15</sup>

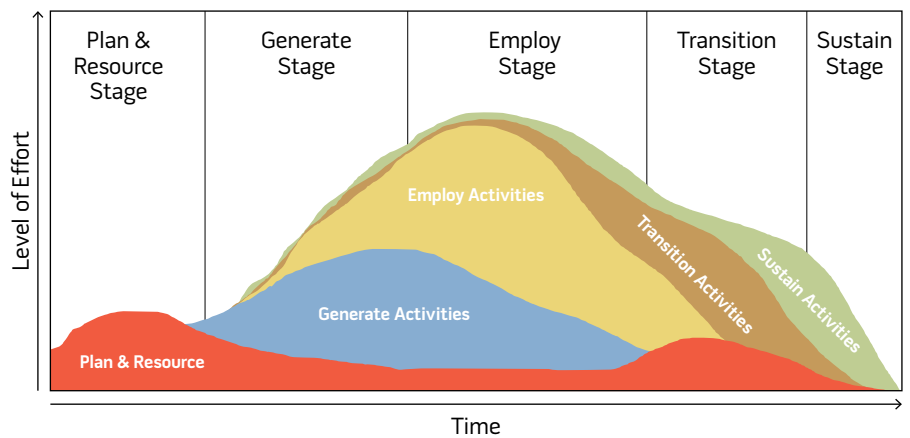
This guidance clearly describes the need for initial and follow-on assessment, systematic monitoring to track implementation and output, and evaluations that analyze the relevance, effectiveness, and sustainability of SC activities not well-detailed in JP 3-20, which enables it to distinguish these efforts from doctrinal operation assessment. It actually offers a broader mechanism that complements operation assessment by incorporating appropriate data from the measures of performance and measures of effectiveness used to assess individual SFA activities. Though contextualized for SC, this AME guidance may in fact warrant consideration for inclusion in the keystone JP 5-0, as the need for feedback and accountability far exceeds the scope of Joint Doctrine Note 1-15, *Operation Assessment*. However, it is not without its

own complications, as that same DOD policy portrays AME as a part of yet another competing SC framework.

On a much broader scale, the fiscal year 2017 National Defense Authorization Act promises even more comprehensive whole-of-government reform. In addition to enforcing standards for AME, “the statutes will enhance the flexibility, transparency, and oversight of SC authorities and resources; professionalize the workforce; and improve alignment of security cooperation activities to defense strategy.”<sup>16</sup> The ensuing consolidation of train-and-equip authority, SC programming, budgeting, and management responsibilities will clearly impact future developments of SC and SFA within joint doctrine.

Current and future manifestations of the four-plus-one threat will continue to necessitate transregional, multifunctional, and multidomain solutions that involve much more than the military instrument of national power. JP 3-20 offers the joint force guidance to protect U.S. security interests in this increasingly complex world, harmonized with the development of PN capacity and capabilities. While JP 3-20 might be new, the notion of enabling partners and allies to thwart threats and facilitate enduring peace and stability around the globe comprises a long and storied history. The dynamic complexities of the current and future operating environment associated with persistent disorder and contested norms demand that the joint force array itself to address not only the conventional threats presented by state actors, but also those represented by identity networks and other nonstate entities. This disposition must also reflect current fiscal realities amid the various legal ramifications of national sovereignty that further strain multinational relationships. The doctrinal planning constructs of EGO and OTERA, as well as other relevant but not yet extant or validated practices such as PGETS and AME, present planners from across the joint force with an organized approach to enhancing the operational effectiveness of U.S. joint forces and optimizing the application of U.S. military

**Figure. Notional Level of Effort by Stage (PGETS) Over Time**



power while addressing these challenges. JP 3-20 fills a persistent doctrinal gap by codifying SC and SFA doctrine into the changing character of warfare as essential to shaping the operational environment and, protecting U.S. and PN security interests now and into the future. JFQ

### Notes

<sup>1</sup> In order to address one of the priorities of the Chairman of the Joint Chiefs of Staff (CJCS), the director of the Joint Staff J7 Joint Force Development Directorate created the Campaign Plan for Joint Force Development Next. This campaign plan involves four lines of effort, one of which includes a task that ensures joint doctrine remains adaptive to operational priorities by using adaptive processes and adaptive products.

<sup>2</sup> See CJCS commencement remarks to the National Defense University’s Class of 2017, titled “Dunford Details Implications of Today’s Threats on Tomorrow’s Strategy,” August 23, 2016, available at <[www.defense.gov/News/Article/Article/923685/dunford-details-implications-of-todays-threats-on-tomorrows-strategy](http://www.defense.gov/News/Article/Article/923685/dunford-details-implications-of-todays-threats-on-tomorrows-strategy)>.

<sup>3</sup> Department of Defense Directive (DODD) 5132.03, “DOD Policy and Responsibilities Relating to Security Cooperation,” October 24, 2008, available at <[www.dtic.mil/whs/directives/corres/pdf/513203\\_dodd\\_2016.pdf](http://www.dtic.mil/whs/directives/corres/pdf/513203_dodd_2016.pdf)>.

<sup>4</sup> JP 3-20, *Security Cooperation* (Washington, DC: The Joint Staff, September 2016, Signature draft).

<sup>5</sup> DODD 5105.38, “Defense Security Assistance Agency,” August 11, 1971.

<sup>6</sup> DODD 5105.65, “Defense Security Cooperation Agency,” October 26, 2012, avail-

able at <[www.dtic.mil/whs/directives/corres/pdf/510565p.pdf](http://www.dtic.mil/whs/directives/corres/pdf/510565p.pdf)>.

<sup>7</sup> Introduced into Joint Doctrine in the 2006 revision of JP 3-0, *Joint Operations*, the term *security cooperation activity* was removed in the 2011 revision of JP 3-0 and thus from JP 1-02, *Department of Defense Dictionary of Military and Associated Terms* (Washington, DC: The Joint Staff, November 8, 2010, as amended through February 15, 2016).

<sup>8</sup> See “Special Message to the Congress on the Mutual Security Program,” March 13, 1959, available at <[www.eisenhower.archives.gov/all\\_about\\_ike/quotes.html](http://www.eisenhower.archives.gov/all_about_ike/quotes.html)>.

<sup>9</sup> “Fact Sheet: U.S. Security Sector Assistance Policy,” April 5, 2013, The White House, available at <[www.whitehouse.gov/the-press-office/2013/04/05/fact-sheet-us-security-sector-assistance-policy](http://www.whitehouse.gov/the-press-office/2013/04/05/fact-sheet-us-security-sector-assistance-policy)>.

<sup>10</sup> *Joint Operating Environment JOE 2035: The Joint Force in a Contested and Disordered World* (Washington, DC: The Joint Staff, July 14, 2016).

<sup>11</sup> “Capstone Concept for Joint Operations: Joint Force 2030,” draft, June 28, 2016.

<sup>12</sup> *DOD Security Force Assistance Lexicon Framework*, November 1, 2011 (incorporating Change 1, April 27, 2012).

<sup>13</sup> U.S. Government Accountability Office (GAO) Report to Congressional Committees, *Security Force Assistance: Additional Actions Needed to Guide Geographic Combatant Command and Service Efforts* (Washington, DC: GAO, May 2012), 14.

<sup>14</sup> Joint and Coalition Warfighting Study on Security Force Assistance in Joint Doctrine, November 2012.

<sup>15</sup> “DOD Guidance for Security Cooperation,” memo from the Deputy Secretary of Defense, August 29, 2016.

<sup>16</sup> Fiscal Year 2017 National Defense Authorization Act, Title XII, Subtitle E, Summary of Key Reforms, December 5, 2016.

## New from NDU Press

for the Center for Strategic Research

Strategic Forum 295  
*Reflections on U.S.-Cuba  
Military-to-Military Contacts*  
by Hal Klepak



President Barack Obama's visit to Cuba in March 2016 opened up the possibility of strategic benefits for

both nations. Well after over 50 years of hostility, however, it will not be easy to keep this nascent relationship on track. Avoiding missteps requires a deep knowledge of Cuba and particularly its Revolutionary Armed Forces (Fuerzas Armadas Revolucionarias, or FAR). The FAR are a complex and powerful institution that enjoys great public respect—more so than Cuba's Communist Party—and remain central to the functioning of the Cuban economy and state. Broadening rapprochement without the support of the FAR is inconceivable.

This paper offers insights concerning the FAR. It argues that it will be important to expand cooperation in the right areas and that it will be important to start small, go slow, build trust, consult early and often, let Cuba take the lead, and avoid imposing or reflecting a U.S.-centric view of civil-military relations.



Visit the NDU Press Web site for more information on publications at [ndupress.ndu.edu](http://ndupress.ndu.edu)

### Joint Publications (JPs) Under Revision (to be signed within 6 months)

JP 1, *Doctrine for the Armed Forces of the United States*  
JP 3-12, *Cyberspace Operations*  
JP 3-27, *Homeland Defense*  
JP 3-35, *Deployment and Redeployment Operations*  
JP 3-57, *Civil-Military Operations*  
JP 3-59, *Meteorological and Oceanographic Operations*  
JP 4-02, *Joint Health Services*  
JP 4-06, *Mortuary Affairs*

### JPs Revised (signed within last 6 months)

JP 2-01, *Joint and National Intelligence Support to Military Operations*  
JP 2-03, *Geospatial Intelligence in Joint Operations*  
JP 3-0, *Joint Operations*  
JP 3-01, *Countering Air and Missile Threats*  
JP 3-04, *Joint Shipboard Helicopter and Tiltrotor Operations*  
JP 3-08, *Interorganizational Cooperation*  
JP 3-13.4, *Military Deception*  
JP 3-14, *Space Operations*  
JP 3-15.1, *Counter-Improvised Explosive Device Operations*  
JP 3-18, *Joint Forcible Entry Operations*  
JP 3-20, *Security Cooperation*  
JP 3-25, *Countering Threat Networks*  
JP 3-33, *Joint Task Force Headquarters*  
JP 4-01, *Defense Transportation System*  
JP 4-01.6, *Joint Logistics Over-the-Shore*  
JP 4-08, *Logistic Support of Multinational Operations*  
JP 5-0, *Joint Planning*

# LESSONS ENCOUNTERED

LEARNING FROM THE LONG WAR

*Edited by Richard D. Hooker, Jr., and Joseph J. Collins*

## From NDU Press

**Lessons Encountered:**

**Learning from the Long War**

NDU Press, 2015 • 488 pp.

This volume began as two questions from General Martin E. Dempsey, 18<sup>th</sup> Chairman of the Joint Chiefs of Staff: What were the costs and benefits of the campaigns in Iraq and Afghanistan, and what were the strategic lessons of these campaigns? The Institute for National Strategic Studies at the National Defense University was tasked to answer these questions. The editors composed a volume that assesses the war and analyzes the costs, using the Institute's considerable in-house talent and the dedication of the NDU Press team. The audience for this volume is senior officers, their staffs, and the students in joint professional military education courses—the future leaders of the Armed Forces. Other national security professionals should find it of great value as well.

The volume begins with an introduction that addresses the difficulty of learning strategic lessons and a preview of the major lessons identified in the study. It then moves on to an analysis of the campaigns in Afghanistan and Iraq from their initiation to the onset of the U.S. Surges. The study then turns to the Surges themselves as tests of assessment and adaptation. The next part focuses on decision-making, implementation, and unity of effort. The volume then turns to the all-important issue of raising and mentoring indigenous

security forces, the basis for the U.S. exit strategy in both campaigns. Capping the study is a chapter on legal issues that range from detention to the use of unmanned aerial vehicles. The final chapter analyzes costs and benefits, dissects decisionmaking in both campaigns, and summarizes the lessons encountered. Supporting the volume are three annexes: one on the human and financial costs of the Long War and two detailed timelines for histories of Afghanistan and Iraq and the U.S. campaigns in those countries.

The lessons encountered in Afghanistan and Iraq at the strategic level inform our understanding of national security decisionmaking, intelligence, the character of contemporary conflict, and unity of effort and command. They stand alongside the lessons of other wars and remind future senior officers that those who fail to learn from past mistakes are bound to repeat them.

Available at [ndupress.ndu.edu/Books/LessonsEncountered.aspx](http://ndupress.ndu.edu/Books/LessonsEncountered.aspx)

## Women on the Frontlines of Peace and Security

Foreword by Hillary Rodham Clinton and Leon Panetta

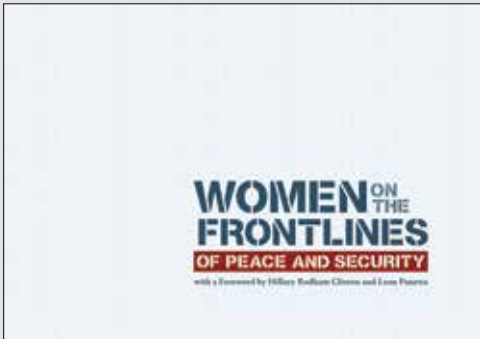
NDU Press, 2015 • 218 pp.

This book reflects President Barack Obama's commitment to advancing women's participation in preventing conflict and keeping peace. It is inspired by the countless women and girls on the frontlines who make a difference every day in their communities and societies by creating opportunities and building peace.

Around the globe, policymakers and activists are working to empower women as agents of peace and to help address the challenges they face as survivors of conflict. When women are involved in peace negotiations, they raise important issues that might be otherwise overlooked. When women are educated and enabled to participate in every aspect of their societies—from growing the economy to strengthening the security sector—communities are more stable and less prone to conflict.

Our understanding of the importance of women in building and keeping peace is informed by a wide range of experts, from diplomats to military officials and from human rights activists to development professionals. The goal of this book is to bring together these diverse voices. As leaders in every region of the world recognize, no country can reach its full potential without the participation of all its citizens. This book seeks to add to the chorus of voices working to ensure that women and girls take their rightful place in building a stronger, safer, more prosperous world.

Available at [ndupress.ndu.edu/Books/WomenontheFrontlinesofPeaceandSecurity.aspx](http://ndupress.ndu.edu/Books/WomenontheFrontlinesofPeaceandSecurity.aspx)



## 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](http://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

