JFQ | Joint Force Quarterly

Issue 79, 4th Quarter 2015

Trends in Defense Analysis

Integrity in Military Writing

2015 Essay Competition Winners

Joint Force Quarterly

Founded in 1993 • Vol. 79, 4th Quarter 2015

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

Copyeditor
Erin L. Sindle

Art Director
Marco Marchegiani, *U.S. Government Printing Office*

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

Cover 2 images (top to bottom): Airman with Paktika Provincial Reconstruction Team, in coordination with Afghan government, provincial government, and Ministry of Youth Affairs, interviews 14-year-old Afghan boy attending large Paktika youth shura (U.S. Air Force/William Greer); Marine with Marine Rotational Force–Darwin handles black-headed python during orientation brief aboard Robertson Barracks, Northern Territory, Australia, in preparation for training "out bush" with Australian Defence Force during 6-month rotation (U.S. Marine Corps/James Gulliver); As part of conducting carrier qualifications for its upcoming deployment, Sailors pull arresting-gear wire across flight deck of aircraft carrier USS *Harry S. Truman* (CVN 75) (U.S. Navy/A.A. Cruz).

In this Issue

About the Cover
U.S. Army Rangers, assigned to 2nd Battalion, 75th Ranger Regiment, advance toward their objective during Task Force Training on Fort Hunter Liggett, California, as part of rigorous training to maintain their tactical proficiency (U.S. Army/ Steven Hitchcock)

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.

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

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

Telephone: (202) 685-4220/DSN 325
Email: JFQ1@ndu.edu
JFQ online: www.dtic.mil/doctrine/jfq/jfq.htm

4th Quarter, October 2015
ISSN 1070-0692

Rangers from 1st Battalion, 75th Ranger Regiment, as part of a combined Afghan and coalition security force operating in Ghazni Province, Afghanistan, await CH-47 for extraction (DOD/Pedro Amador)

Executive Summary

As this column is written, a number of significant events are occurring that will shape the future joint force. The barriers to women engaging in ground combat are being reassessed and, in all likelihood, most if not all will be removed. At the same time, the U.S. Army's end-strength is expected to be reduced significantly (to below pre-9/11 levels), while other Services are already there. The price of oil has hit historic lows and global stock markets have fallen significantly. The situation would seem to put pressure on some states that depend on high oil prices for revenue. The combat and growing refugee crises in Syria and Iraq (and now Europe) continue without end. Afghanistan is still dealing with a difficult transition. The area around the demilitarized zone on the Korean Peninsula once again has both sides on high alert but talking to each other at Panmunjom. On the home front, another Presidential and congressional election campaign has begun while the sequestration shadow looms over the Federal Government and especially the Department of Defense. What does this all mean?

The easy answer is that a great deal of unsettled business from the past is likely to remain while some new work is added to our collective "inboxes." Inside the military, as I have said in previous columns, the need for smart leaders who can figure out a way to lead their organizations to success will continue. Constrained budgets are nothing new for many of us, so adapting to these circumstances should be almost standard operating procedure. The hard part, I suspect, will be figuring out how to keep the best people in the force even though the tempo of operations may not get slower, despite the drawdowns in Iraq and Afghanistan. Some of the force continues at a high operational tempo in part because of unfolding events around the globe. The good news is that we will always find we have great people among us who know what to do even when the circumstances unfold in unexpected ways, as we saw recently on a high-speed train from Brussels to Paris. Five people took action to stop a man with weapons and the intent to do harm, and each was rightly awarded France's highest honor—the Legion of Honor—for taking swift and effective action. As we now know, four were Americans, including two Servicemembers, and the other hero was a British businessman. While few of

us will ever find ourselves in such a situation, being able to respond to a threat by doing what you think is best—especially for the common good of others around you—is often the difference between success and failure, and these times call for people doing what they think is best for the common good. Those who serve their nation honorably are just such people. Some even try to share their good ideas for how to do what is best through journals like this one. If you are looking for good ideas to help you deal with increasingly difficult events, I think you will benefit by reading *Joint Force Quarterly*.

This issue's Forum begins with an article by Paul B. Symon and Arzan Tarapore, who see both the great potential and the inherent risks in harnessing big data to our intelligence processes. Seeking to improve another key strategic process, Catherine Johnston and her co-authors from the Intelligence Community offer insight into how intelligence analysis is adapting to the disorganized world we work in. Alexander L. Carter next provides some important ideas regarding improving joint interagency coordination. As we continue to assess the last several years of war and its aftermath, Jeffrey M. Shanahan provides a new look at stability operations as seen through the lens of mission command.

JFQ next presents the winning essays from the 9th annual Secretary of Defense and 34th annual Chairman of the Joint Chiefs of Staff Essay Competitions. In May, 24 judges from across the joint professional military education (JPME) community met to determine the best JPME student entries among the three categories. This year's winners provide a diverse set of issues and recommendations to consider. In his winning Secretary of Defense National Security Essay, Lieutenant Colonel Wallace R. Turnbull III, USAF, argues that the nuclear force structure planned for 2040 lacks key elements in the air-delivered elements of the triad that must be considered for our deterrent to be credible in 25 years. Winning the Chairman of the Joint Chiefs of Staff Strategic Research Paper competition, Lieutenant Colonel (P) Patrick Michael Duggan, USA, discusses the role for special warfare operations in cyberspace. In the Chairman's Strategy Article, Lieutenant Colonel Robert William Schultz, USA, discusses how to deal with extremist groups in cyberspace.

In JPME Today, the discussion of two important and ever-present issues for graduate studies, and PME in particular, are brought into focus in two excellent articles from teams within the U.S. Army's PME institutions. If you missed the class on what plagiarism is and how to avoid it, you will want to read and share Larry D. Miller and Laura A. Wackwitz's engaging article on the nexus between an author's expression of thought and ethical behavior, especially how it affects national security. William G. Pierce, James E. Gordon, and Paul C. Jussel, a team from the U.S. Army War College, next offer suggestions on how to help PME instructors possessing advanced but dated operational experience remain relevant in the classroom.

In Commentary you will find Robert A. Gleckler's important analysis of war planning. His article should help those who are not planners understand the strengths and limitations of our most important military efforts prior to the start of operations. As a former operational and strategic planner myself, looking at what the plans can mean for strategic decisionmakers is a unique interpretation, at least in the pages of military journals.

Our Features section takes on three distinct but central issues for the joint force: the effect of military pay and compensation on the force we can field, how best to manage theater air and missile defense at the operational level, and how cyber has an impact on conventional combat power. Anyone who has served or been aware of the pace of compensation in recent years for military members, especially those approaching or at retirement age, knows that the benefits currently provided have been steadily increasing. Mark F. Cancian shows us what he believes is the consequence of that part of the Defense Department budget growing as the total budget is affected by legislated cuts: the military's force structure. Edward Boxx and Jason Schuyler suggest a better way to organize decisionmaking at the operational level of air and space warfare through the Joint Theater Air and Missile Defense Board. As military leaders at all levels search for ways to get more while dealing with less resources, Sean Kern sees the development of military cyber power theory as crucial to adding punch to our combat power.

Continuing our Recall offerings on World War I during this 100th anniversary period of the "war to end all wars," Raymond Adams takes us to the Gallipoli Campaign, the last great battle of the Ottoman Empire, and shows us how things went wrong for the Allies far from the fields of France. As the title suggests, strategy only works when ends and means are matched. The hard part is getting them to do so when the fighting starts.

Joint Doctrine provides two interesting and important articles. A team of experts, led by the Joint Staff J7's James C. McArthur, provides us with the first in a series of articles on interagency organization. Jon T. Thomas and Douglas L. Schultz then offer an excellent recap on the history and status of the 30-year-long effort to achieve success in providing the joint force with the effective lessons learned capability now known as the Chairman's Joint Lessons Learned Program. Of course, we also bring you the latest Joint Doctrine Update as well as three book reviews on Russia, PTSD, and corruption in Afghanistan to help you in your professional reading.

No matter what new challenges the world brings us, *JFQ* will endeavor to provide what you have come to expect from us: high-quality thinking and writing that is useful as you work your way forward. Let us know what you think. **JFQ**

William T. Eliason
Editor in Chief

Crew chief with 36th Aircraft Maintenance Unit, Osan Air Base, South Korea, checks computer data during Red Flag-Alaska 14-2, ensuring F-16 Fighting Falcon readiness (U.S. Air Force/Peter Reft)

Defense Intelligence Analysis in the Age of Big Data

By Paul B. Symon and Arzan Tarapore

Over the past decade, the U.S. and Australian intelligence communities have evolved rapidly to perform new missions. They have developed new capabilities and adapted their business processes, especially in support of joint and complex military operations. But in the coming decade, their greatest challenge will be to develop new capabilities to manage and exploit big data.[1] We use the term *big data* to mean the exponentially increasing amount of digital information being created by new information technologies (IT)—such as mobile Internet, cloud storage, social networking, and the "Internet of things"—and the advanced analytics used to process that data. Big data yields not simply a quantitative increase in information, but a qualitative change in how we create new knowledge and understand the world. These data-related information technologies have already begun to revolutionize commerce and science, transforming the economy and acting as enablers for other game-changing technology trends, from next-generation genomics to energy exploration.[2] In defense intelligence communities,

Major General Paul B. Symon, Australian Army, served as Director of the Defence Intelligence Organisation from 2011 to 2014. Arzan Tarapore is a Doctoral Student in the War Studies Department at King's College London. The authors thank Josh Kerbel and Peter Mattis for comments on an earlier version of this article.

some of these technologies have been adopted for tasks, including technical collection and operational intelligence fusion—but big data's impact on all-source intelligence analysis has scarcely been examined.

This article offers a view on how these disruptive information technologies could transform defense intelligence analysis and the functions of the all-source enterprise. It is not a comprehensive study on trends in technology or in the intelligence profession, nor is it a deterministic scenario of a high-tech future. Rather, here we seek to identify some opportunities and risks of the disruptive technologies at hand. First, we sketch a background of the most important IT trends that are shaping today's economy and society. Second, we outline how big data could transform intelligence analysis; it has the potential to unlock enormous productivity gains and effectiveness by automating some currently labor-intensive tasks, enabling new forms of analysis and creating new forms of presentation. Third, we argue big data cannot do it all; its utility in making sense of complex systems and addressing knowledge gaps is limited. Finally, we outline how big data could transform the wider assessment agency enterprise. We argue that the explosion in data supply and demand will incentivize assessment agencies to reposition their roles more toward service-delivery functions and to rebalance their workforces.

None of this is inevitable. In both analytic operations and enterprise management, much of how the scenario actually unfolds will be determined by the vision and agility of our leadership, our partners, and our adversaries. Defense and intelligence community (IC) leaders must play an active but balanced role, exploiting big data's potential, but understanding its limitations.

Today's Tech Trends

The big data phenomenon presents defense intelligence with a range of opportunities, from off-the-shelf tools to complex business-process reforms. Some tools can be absorbed wholesale by the IC; for example, social networking tools such as Wikis and Chat are already being used to facilitate better collaboration between analysts. Beyond simple software acquisitions, however, disruptive information technologies have birthed a number of trends in how data are collected, moved, stored, and organized. Four of the most salient prevailing concepts, which are already transforming the economy and society, could reshape all-source intelligence.

Everything Is Social, Mobile, and Local. Much of the explosion of big data has been driven by the fact that information is increasingly social (generated and transmitted by many users, rather than a few big producers), mobile (collected by sensors on ubiquitous Internet-connected mobile devices), and local (geospatially tagged). These trends have irreversibly transformed IT; mobile devices in particular have become the primary means of connecting to the Internet and have thus become the primary market for much IT innovation. This has already created new opportunities not only for collection, but also for intelligence processing, exploitation, and dissemination (PED), and analysis.

Data Are Useless Without Data Science. The exponential creation of digital data holds enormous potential for creating insight and knowledge through PED and data analytics. The burgeoning field of data science—at the intersection of statistics, computer science, and other related fields—is increasingly being used by the private sector to realize the commercial potential of big data, often for prosaic tasks such as tracking a person's consumption patterns to better target advertising campaigns. The IC's routine work of collection, PED, and analysis is still largely organized on the Cold War model of seeking out sparse and secret information. Now, however, it must cope with the inverse challenge (and exploit the opportunities) of managing and analyzing massive quantities of data and, in the process, compete with the lucrative private sector to attract the highly specialized skills of data scientists.[3]

IT Solutions Are Customized and Intuitive. The accelerating pace of innovation and the need to best harness big data are both enabling and driving the creation of IT solutions that are customized and intuitive for the user. Gone are the days of hefty user manuals or obscure text-based user interfaces. Specific applications perform specific functions. Even major platforms such as Palantir are delivered with bespoke service support, both in tailoring the product to customer requirements and in providing ongoing software development support. Complex data-driven analysis demands a menu of apps or even dedicated software developers integrated into analyst teams—as they already are in some parts of the IC.

The Internet Is Everywhere. The rate of increase in big data will only grow as more devices join the Internet. These devices not only provide an interface for users, but are also creating a growing "Internet of things"—everything from household appliances to industrial robots—that generate and use more data, in turn creating more potential knowledge and vulnerabilities. At the same time, emerging technologies (such as free-space optical communications, which use lasers to transmit data through the atmosphere) are allowing users to bring the Internet into austere communications environments in order to enable the wider military use of Internet-connected IT and greater resilience to network failures.

These technology trends have been driven by the commercial and scientific sectors, but they also have powerful implications for the IC; they are rapidly challenging long-held conceptions of intelligence collection targets, business processes, required IT tools, and workforce skill sets. But the IC's capacity to adopt these technologies remains inadequate; fully exploiting these trends would require a deep revision of innovation policy and IT-acquisition business models. To adequately exploit these opportunities, the IC would need to incorporate a "technology push" acquisition model alongside the customary "demand pull" model. In today's IT environment of faster innovation and more disruptive and unpredictable technologies, where government lacks the speed or vision to lead innovation, the IC's best option may be to monitor

and leverage incipient innovation instead of attempting to drive it. Rather than dictating requirements to firms through a byzantine acquisitions process (as in most defense procurement programs), the IC's greatest potential for IT adoption may lie in injecting its "use cases" (and resources) in the start-up or development phases of future technologies. And in a data-intensive information environment, assessment agency leaders would need to recognize that adaptive IT is integral to analytic operations and no longer an ancillary support function toiling in the basement. The analysis mission-owner should therefore be responsible for shaping the agency's IT architecture as never before.

Even if imperfectly realized, today's technology trends hold enormous potential to transform all-source intelligence.

Transforming Analysis

Across intelligence problems, big data's greatest promise is its potential to integrate and organize information. New technologies for collecting, moving, storing, and organizing data could give all-source analysts access to vastly more information with more automation and productivity, thereby allowing them to concentrate their finite cognitive capacity on the hardest, highest-priority problems. But rather than simply bolting new technologies onto current processes, assessment agencies now have an opportunity to incorporate new technological trends in ways that fundamentally reshape how data are used for all-source analysis. The new technologies could be usefully applied to a range of defense intelligence problems, including social network analysis, weapons systems modeling, trend analysis for tactical military intelligence or nontraditional warning problems, and nascent analytic constructs such as "object-based production" and "activity-based intelligence."[4] Thus, they not only improve our capacity to execute existing intelligence missions, but they also create entirely new data-intensive types of analysis.

More Information with Less Effort. Big data and data analytics rely heavily on automation. Once the architecture and algorithms are set, the data could be managed—collected, moved, stored, and organized—with relatively little additional effort. Applied to all-source intelligence, the exponential increase in data and analytics would render manual information retrieval impractical and unnecessary; the heavy lifting of data management could be largely automated. Already-existing tools can create an automatic and persistent push of data to analysts, obviating the labor-intensive requirement to manually pull data from various sources. That push of data could be more processed and valuable—for example, collated across different sources or formats—before it even reaches the analyst.

Automated data collation and analytics would both save analyst effort and enable powerful new capabilities. Data analytics could, with varying levels of human supervision, characterize data into meaningful clusters or categories, categorize and file new data into existing clusters, and detect outliers or new data that do not fit into existing clusters.[5] For all-source analysis, new methods such as object-based production could enable seamless integration of data from multiple sources and in multiple formats, thereby building comprehensive libraries of data on given targets. Analysts could use that mass of data and associated analytics to more quickly identify intelligence gaps, unexpected correlations and associations, or anomalies or irregular behavior. This range of capabilities could be profitably used, for example, for everything from finding patterns or anomalies in a terrorist target's pattern of life, to tracking military targets automatically in wide-area surveillance, to tipping and cueing for humanitarian assistance and disaster recovery support. In such cases, human intervention—especially expert analysis of the target—is still critical, but big data could empower those analysts to know more and to know it more quickly and with less effort.

Big data technologies allow intelligence to move quickly, be stored indefinitely, and yield more valuable insights over time. Much of the newly collected data would arrive at or near real-time, compressing the latency of collection, PED, and analysis, and cueing further collection. Vast quantities of data—unprocessed and unseen by any analyst—would be stored, available to be mined later in the context of future data or requirements or to discover or recognize associations or trends. Machine learning would allow this entire process to improve with time. The accumulation of data and the refinement of algorithms would allow for dynamic and progressively more accurate models or more robust and adaptive normalcy patterns, and would enable the detection of finer or more meaningful anomalies accordingly.

There are significant challenges to fielding these new capabilities. Some of these challenges are technical—for example, optimizing ways to ingest and collate data from different sources and in different formats, especially unstructured data from text and media. The thorniest challenges, however, are associated with policy settings and governance frameworks. For example, intelligence agencies will need to set standards for the vetting and quality assurance of data they source from interagency or other partners; establish security and legal compliance protocols for sharing data across organizations; establish robust security measures to protect data from spoofing, cyber exploitation, or insider leaks; and standardize the tagging and coding of data for use in analytics. Once mission-owners set these frameworks to govern the effective and secure use of big data, all-source analysis should yield unprecedented gains in productivity and capability.

Presentation Is Everything. Once collated, managed, and applied to gain new insights, data must be presented effectively to the customer. Here, too, big data carry risks and opportunities. Customers will never lose the temptation to acquire and interpret their own data, and big data, plentiful and apparently authoritative, will exacerbate that problem. The IC faces the risk that these quantities and varieties of data will create the appearance of veracity—and customers' easy access to raw data streams or intelligence reporting could become even more hazardous. In an environment where data are

Airman checks diagnostic information after applying three different upgrades that give pilots more situational awareness data in user-friendly formats (U.S. Air Force/Alexander Guerrero)

ubiquitous, customers will expect immediate and authoritative answers and will sideline IC producers that cannot quickly deliver user-friendly products.

Fortunately, big data and data analytics also present opportunities to create compelling and effective outputs for the customer. Data-intensive solutions to intelligence problems demand appropriate forms of presentation; just as in science and commerce, these solutions would be best presented as graphics or visuals, not text-heavy assessments. Assessment agencies could profitably use one or a few main data-agnostic platforms (such as Google Earth), connected to relevant intelligence databases and easily overlaid with various customized data layers, to electronically deliver finished intelligence to the customer. With the concomitant improvement in IT, these outputs could be easily pushed to the customer, just as data are pushed to the analyst. Presented in multimedia, they could incorporate multi–collection platform reporting and data streams and use "recommendation engines" of the type used by Amazon and Netflix to suggest other relevant outputs tailored to the customer's requirements.

The most effective finished intelligence outputs, exploiting the full potential of data analytics, would incorporate the following features. First, they would use a visualization platform, and for strategic analysis, the most common platforms would most likely be geospatial. Much digital data are already geospatially tagged, and geospatial presentation often yields powerful insights that are not otherwise apparent. Second, they would be dynamic—using automated feeds, the product would be constantly updated with data collated in real time. Outputs would offer more than just a recent snapshot of intelligence, as the IC typically provides now with written assessments, and they would render obsolete terms such as "Latest Date of Intelligence" or "Information Cut-Off Date." Third, they would be interactive; the customer could interrogate the product, using hyperlinks or some other intuitive interface, to pursue additional layers of data.

These attributes of data-intensive presentation are clearly better suited to some outputs, and some customers, than others. Already, strategic assessments for national policymakers can profit from visual and interactive outputs—even the President's Daily Brief, the pinnacle of national-level intelligence, has been delivered on an iPad. With time, big data and data analytics could transform all phases of analytic operations, culminating with quicker, more accurate, and more tailored intelligence for customers.

Limits to Transformation

The promises of big data are tantalizing, but they are limited. The greatest impact will be felt in the analysis of who, what, where, and when ques-

Intelligence analyst gives commander of 21st Theater Sustainment Command terrain brief of Hohenfels Training Area on enemy activity (U.S. Army/Henry Chan)

tions, using single– or multi–collection platform structured data to address discrete, bounded questions. It plays a smaller role in analysis of why or how questions, which are salient not only for strategic intelligence supporting the policymaker, but also for every level down to tactical intelligence supporting subunit commanders.

Analysis Needs More Than Data. Data-intensive forms of analysis promise new efficiencies and insights, but at its heart, all-source analysis needs more than just data. First and foremost, analysis needs expert leadership. Faced with the allure of compelling data, the IC faces a risk that available data will drive the analytic agenda rather than the other way around. The sheer availability of certain types of data could skew the analytic enterprise to prioritize its efforts or distort its assessments by placing undue importance on the most data-intensive activities or by emphasizing the most visible and trackable targets or issues. Instead, expert leadership must still determine which data are collected and in the service of which analytic priorities; these tasks demand judgment and knowledge of customer requirements. The analysis mission-owners must be careful to redouble their emphasis on directing the intelligence cycle and to ensure the enterprise is serving customer requirements—asking the right questions and directing collection and analysis accordingly—rather than being slaves to the data.

Second, analysis needs expert analysts. Data-intensive fusion, PED, and analysis are better suited to some types of intelligence problems than others, but they always require expert analysts to make sense of outputs. Data-intensive analysis can more profitably be applied against "puzzles," with bounded, empirically discoverable answers, rather than "mysteries" that deal with a contingent, imponderable future.[6] Puzzles typically relate to discrete objects—places and things—whereas mysteries are tied to complex phenomena.[7] Mysteries or complex phenomena are the product of inscrutably complex human interactions and, like any complex system, are sensitive to countless variables and therefore inherently unpredictable. Defense intelligence must be postured to tackle both.

Even puzzles require expert analysts—to frame the puzzles in the first place, solve them, and then to make them relevant. Analysts need to verify collected data that may be flawed or spoofed by denial and deception, which requires expert analytic tradecraft. They then need to provide the necessary context or value-added interpretation of the data analytics—the "so what?"—which requires not only subject matter expertise but also sensitivity to customer requirements.

Consider the conflicts that flared in Ukraine and Iraq in 2014. In both cases, irregular forces—Russian-backed separatists and Islamic State militants, respectively—made rapid advances against their adversaries, not only deploying effective military force but also documenting their campaigns in social media platforms such as Twitter and YouTube. Exploiting the content and metadata of these sources, fused with data from traditional intelligence, surveillance, and reconnaissance (ISR), could yield significant data about those forces' tactics, social networks, and geolocation at particular times. Those data-intensive streams would allow Western defense intelligence to build a high-fidelity picture of these forces' composition, materiel, and disposition. They could thus provide useful context and cueing for tactical intelligence support. But they would add little to the customers' understanding of the militants' intent—their operational plans and political agenda—or even some elements of their capability, such as their level of unit cohesion. Framing, solving, and interpreting these puzzles, even for tactical military intelligence problems, require analytic judgment, attuned to customer needs.

For mysteries, data may offer valuable piecemeal insights, but expert analysts need to do even more heavy lifting to translate those insights into meaningful assessments for customers. Expertise is critical for inferring a target commander's intent (as in the Ukraine and Iraq irregular warfare examples above) and even more so for assessments of complex phenomena, such as political unrest. For instance, a more perfect data-intensive coverage of the Arab Spring unrest could have provided better insights into the depth of popular opposition to Arab regimes or tactical warnings of intensifying protests, but simply a better coverage of social-networking or other data-intensive tools would not have prepared Western intelligence agencies to anticipate the

revolutions. Twitter feeds alone could not explain why revolutions swiftly consumed regimes in Tunisia and Egypt, or explain the difference in political trajectories in Libya, Bahrain, and Syria. An actionable intelligence response to Arab unrest would have required marrying that data-intensive coverage with subject matter expertise, comprehensive analyses of state stability, and a receptive and agile policy customer; big data without those factors would have provided tactical tipping of protests, not strategic warning of regime collapse or civil war. For complex problems, big data can provide a more granular picture of the target, quickly and with little effort, but the mystery can only be anticipated or managed (if at all) by the enterprise's expert leaders and analysts, working closely with the customer.

Addressing Knowledge Gaps. Some big data proponents argue that new storage and processing technologies should allow users to collect and manage virtually all relevant data about a given object. By examining the entire population of data rather than a sample (that is, where n = all), users could make direct observations rather than relying on inferences based on partial data. Induction and modeling would be unnecessary, replaced by the volume and fidelity of a virtually complete data set, manipulated by well-tested algorithms. In this view, better understanding only needs better data.

The quest for more data is all too familiar for the Intelligence Community. Built in the Cold War, when clandestine collection was key to uncovering scarce information, and reinforced in the past decade of ballooning technical ISR collection to support warfighters, the community has developed as a collection-centric system geared toward plugging intelligence gaps or arithmetically connecting the dots, and any missteps or intelligence failures are most commonly met with demands for more or better data.[8] For some problems, addressing intelligence gaps is vital, and big data will help—with both open source and intelligence collection.

Complex phenomena, on the other hand, are not so easily conquered by data. For these, assessment agencies need to address enduring *knowledge gaps*. Unlike intelligence gaps, knowledge gaps have no single, durable answer and may not be required to directly support specific decisions or actions. Rather, they are an ongoing requirement, a framework to guide collection and to improve decisionmakers' understanding as they seek to execute a plan. These gaps would only be satisfied—or, more likely, de-prioritized—when they are no longer essential for decision advantage. More data cannot close a knowledge gap. As a result, knowledge gaps involve an inescapable degree of uncertainty and limit analytic confidence. They remain extremely useful constructs to structure and prioritize intelligence collection and analysis, but they also highlight the limitations of big data's utility to strategic analysis.

Knowledge gaps may be comprised of multiple intelligence gaps, but critically, they also require analytic interpretation and judgment. For example, cataloging the signatures of China's new aircraft carrier, charting the performance of its aircraft and weapons systems, or tracking its position on a patrol all represent intelligence gaps with discoverable answers. But understanding how that vessel might be used by Beijing, in concert with other capabilities in a crisis or as part of a coercive strategy, would represent a complex knowledge gap comprised of many constituent intelligence gaps and unknowable future courses of action that are contingent, complex, and unpredictable. Data cannot reveal what does not yet exist, such as adversary decisionmaking in a crisis. For such knowledge gaps, collecting and collating all relevant data would not be sufficient; better data may provide richer evidence for interpretation and anticipation, but it would only be a supplement to subject matter expertise and rigorous tradecraft.

In defense intelligence, creating knowledge requires more analyst effort than closing intelligence gaps, but it is also more important, at least to strategic policy customers. Making sense of complex systems and phenomena—creating knowledge—is central to sound decisionmaking. Some big data optimists suggest that uncovering all relevant data for a problem (or achieving n = all) should allow users to draw reliable empirical correlations without needing to understand causality; indeed, in some fields, that may be sufficient. But in intelligence analysis, understanding causality is indispensible because customers seek to take action

A Modest Time Horizon

The pace of technological innovation is extremely high and increasing. Many of the consumer products and underlying technologies that have revolutionized the high-tech sector have gone from prototype to ubiquity in a few short years. The iPhone—the device that made mobile Internet routine—was launched only in 2007. By 2008, the number of mobile (WiFi) broadband users overtook the number of fixed (wired) users. The two giants of social networking, Facebook and Twitter, were both opened to public use in 2006; by 2011 Twitter was being credited with facilitating political organization in the Arab Spring, and by 2012 Facebook boasted more than a billion members.

These technology applications all had a widespread disruptive effect in less than 5 years; other technologies such as the "Internet of things" are yet to mature, and their impact can scarcely be predicted. Big data technologies present a complex set of challenges that the Intelligence Community (IC) will grapple with for years, but the extreme pace of technological change will continue. Within another 5 to 10 years, the high-tech ecosystem will probably be unrecognizable, and the IC will be faced with a radically different set of risks and opportunities. Thus we can only meaningfully project the impact of existing disruptive technologies with a maximum time horizon of about 5 years—a period that will be dominated by adoption of big data technologies. Anything beyond that is science fiction.

to influence outcomes, and actionable intelligence support should accordingly highlight causality, enable the customer to understand their points of leverage, be alert to key decision points, and act effectively against threats or opportunities. Understanding causality in the context of customer requirements—in other words, creating and applying knowledge—is thus central to the IC mission.

Transforming the Enterprise

Simply passing the deluge of data on to customers would be counterproductive; even neatly presented fused data, absent expert assessment and advice, would only decrease the signal-to-noise ratio of useful, actionable intelligence. Big data are exacerbating that problem by sharply increasing both the *supply* of data available to the IC and the *demand* for it from senior customers. Caught in the middle, IC leaders will need to adapt not only to the transformation of analytic operations, but also to the functions and staffing of the enterprise.

From Production to Service Delivery. In an environment of ballooning data inputs and expected outputs, the IC cadre of all-source analysts will find it increasingly difficult to remain the original producers of all finished intelligence for their customers. Even with the anticipated productivity dividends, the enterprise in its current form will not be able to cope with the pace or scale of the big data challenge, for at least four reasons.

First, customer expectations are already growing and outstripping the IC capacity to adapt. As their decision cycles continue to be compressed, customers will demand immediate and data-rich answers rather than lengthy deliberations or vague and unverifiable "gut calls."

Second, in the face of these increasingly unforgiving expectations, the current production process—tasking collectors, collating and analyzing data, and producing finished intelligence reports—is too cumbersome and time-consuming. If the IC rigidly sticks to that process, dissatisfied customers will seek their information elsewhere.

Third, these dissatisfied customers will find data-intensive information support from a proliferating array of competing suppliers, from established and nontraditional media to commercial intelligence services, which can provide quicker and more user-friendly answers—at a tiny fraction of the IC enterprise's operating budget.

Fourth, the proportion of useful information that is classified, the unique province of the IC, is rapidly declining. Increasingly, decision advantage hinges on speedily integrating multiple streams of data rather than on a well-placed spy—and big data provide a wealth of open source or gray information that can more cheaply and automatically be deployed for intelligence solutions. Classified collection will remain indispensible, but IC leaders will be incentivized to more judiciously deploy those relatively expensive and risky means against their toughest hard targets.

With these clunky production processes, tough competitors, and less unique information, an unchanging IC enterprise will face an urgent threat of irrelevance. This threat sharpens already existing incentives for assessment agencies to reimagine their function, from the current industrial-age model of linear *finished intelligence production* to an information-age model of integrated and adaptive *assessment service delivery.* Even without the advent of big data, a growing body of literature on the state of the art of all-source analysis argues that intelligence agencies should cultivate a more intimate relationship with their customers—to better understand their requirements and more effectively deliver influential support—and to reconceptualize their role from sole producers to service providers.[9] Much of this literature points to the importance of timely and tailored on-call expertise (as distinct from discrete written products) as a key service for customers. The J2 briefing the commander or the analyst briefing the policymaker is an indispensable face-time moment for both the customer and the intelligence provider. The customers' abiding preference for agile and responsive in-person expertise will ensure such services remain a prized feature of assessment services.

Another key service the enterprise could deliver is access to a much wider network of expertise from across, and from outside of, the IC. In this view, assessment agencies would retain their core analysis and production mission, but to meet customers' demand with the best possible intelligence support, they would also leverage networks of other agencies, allied partners, commercial sources, and cleared outside experts. In a world awash in data, assessment agencies' prime advantage will lie in the privileged access to their customers; while they will not be able to internally produce all the answers, they should be able to tailor and fine-tune intelligence solutions sourced from intelligence collectors and from elsewhere. This service then amounts to enterprise management: using networks of experts and data sources and collaborative mechanisms including social-networking tools to quickly address priority knowledge gaps. Effective enterprise management hinges on robust integration with both those networks and with the customer.

Renewed Importance of Staff Functions. All-source analysts have traditionally been the core skill set of assessment agencies, and as we have argued, big data create powerful reasons to integrate data scientists and software engineers into analytic teams. Additionally, intelligence staff functions—a greatly enabled version of today's collection managers as distinct from all-source analysts—would be a critical force multiplier by facilitating the agency's enterprise management roles. In an enterprise transformed to provide assessment services rather than simply production, effective staff work would form the vital connective tissue between the assessment agency and its network of collectors and partners.

The force-multiplying quality of these staff functions will prove particularly valuable as agencies seek to manage both the demands of big data analytics and resource constraints. Assuming the U.S., Australian, and other ICs will continue to face tough budget and staffing pressures, any future investment in data analytics–related functions will likely come at the

expense of all-source analyst capacity, as analyst billets are retasked for new data-related missions. Investing more in staff functions would provide a scalable solution for the agency to leverage more external capacity to meet rising customer demands—and a scalable solution to maximize service delivery will become particularly salient in case of future budget or staffing cuts.

Thus, the future assessment agency should have a more diverse ecology of personnel. Rather than treating all-source analysts as the sole core competency and all other functions as ancillary support, an effective assessment agency that has adapted well to big data–related disruptive technologies will rely critically on the interaction of three core job types, none of which can be fully effective without the others: *data analytics disciplines*, including data scientists and software engineers, to process and manipulate big data inputs; *all-source analysts*, to provide expert and customized assessment advice; and *intelligence staff functions*, to manage and enable the assessment agency's key advantage: its connections to the customer and the rest of the enterprise.

Conclusion

Disruptive technologies carry implications not only for the work of the future analyst, but also for the future assessment agency. In particular, big data and its associated trends should yield enormous productivity and capability gains. But these technologies will also put pressure on the assessment agency as a whole to move away from internally producing all their intelligence and toward a service-provider model in which it tailors intelligence solutions sourced from across the IC and elsewhere. Many of these implications apply particularly to foundational military intelligence, so they will not be felt equally across the IC, and they will also extend to deployed warfighter support and collaboration with other government agencies and allied partners.

Like no change since the end of the Cold War, the advent of big data and data analytics will compel abiding changes in the IC. The risks and opportunities we have outlined are foreseeable in the next 5 to 10 years; other disruptive technologies not yet conceptualized (let alone fielded) will have other, unknowable effects in coming decades. The unknowable nature of future disruptive technologies, however, should not prevent IC leaders from executing a big data strategy immediately to transform both analysis and the enterprise.

None of these changes is inevitable; exploiting big data's remarkable opportunities and mitigating its risks demand strategic vision. An adaptive and effective defense intelligence enterprise will need new IT tools, new skill sets, and new business processes to embrace innovative technologies, and these will be costly. It will also entail a formidable recruitment and training challenge not only to cultivate a cadre of skilled data scientists but also to train all-source analysts on the uses and limits of data analytics. Meeting the challenge of big data will require investments of money and resources, and some risk-taking on new technologies and protocols—precisely at the moment of tightening budget constraints and post–Edward Snowden security sensitivities. These investments will have to compete with continued investments in the IC's treasured but exorbitant clandestine collection platforms, and IC leaders will need to make increasingly tough decisions on allocating those resources. As resources for traditional clandestine collection shrink, the obvious solution would be to reduce unnecessary duplication and dedicate those rare collection means to priority hard targets.

Most importantly, meeting the challenge of big data requires disciplined leadership to judge and maintain the right balance between data-intensive analytic functions, such as foundational defense intelligence, and making sense of complex phenomena for strategic intelligence advice. Absent strong direction, big data could easily become fetishized, where the quantity of data collected, collated, and processed becomes the measure of the community's effectiveness and distorts the analytic agenda. Instead, IC leadership must ensure that expertise and tradecraft are at the center of analytic operations and that knowledge creation and assessment services are at the center of enterprise management—all in the service, ultimately, of decision advantage for the customer. JFQ

Notes

[1] *Big data* is now a hackneyed, almost passé, term, but in the absence of a widely accepted substitute, it remains useful. For a non-scientific introduction to big data and its transformative potential, see Kenneth Neil Cukier and Viktor Mayer-Schoenberger, "The Rise of Big Data: How It's Changing the Way We Think about the World," *Foreign Affairs* (May–June 2013).

[2] James Manyika et al., *Disruptive Technologies: Advances that Will Transform Life, Business, and the Global Economy* (San Francisco: McKinsey Global Institute, May 2013), available at <www.mckinsey.com/insights/business_technology/disruptive_technologies>.

[3] On the skills required for data science, see Drew Conway, "Data Science in the U.S. Intelligence Community," *IQT Quarterly* 2, no. 4 (Spring 2011), 24–27. McKinsey estimates that by 2018 the demand for data-science talent will exceed its projected supply by about 50–60 percent (see Manyika et al.). The Intelligence Community will need to compete with the more lucrative private sector for those scarce talents.

[4] On object-based production and activity-based intelligence, see Catherine Johnston, "Modernizing Defense Intelligence: Object-Based Production and Activity-Based Intelligence," briefing, Defense Intelligence Agency, June 27, 2013, available at <www.ncsi.com/diaid/2013/presentations/johnston.pdf>.

[5] Kirk Borne, "Knowledge Discovery from Mining Big Data," briefing, March 12, 2013, available at <http://realserver4v.stsci.edu/t/data/2013/03/3194/KborneStsci2013.pdf>.

[6] On puzzles and mysteries, see Gregory F. Treverton, "Risks and Riddles," *Smithsonian Magazine* (June 2007).

[7] We are grateful to Josh Kerbel for coining this distinction between objects and phenomena.

[8] Josh Kerbel and Anthony Olcott, "The Intelligence-Policy Nexus: Synthesizing with Clients, Not Analyzing for Customers," *Studies in Intelligence* 54, no. 4 (December 2010).

[9] See, especially, Kerbell and Olcott; interview with Robert Blackwill, "A Policymaker's Perspective on Intelligence Analysis," *Studies in Intelligence* 38, no. 5 (1995); and Thomas Fingar, "Intelligence as a Service Industry," *The American Interest* 7, no. 4 (March–April 2012).

Lieutenant General Vincent Stewart, USMC, delivers inaugural address as director of Defense Intelligence Agency and commander of Joint Functional Component Command for Intelligence, Surveillance, and Reconnaissance, January 23, 2015 (Defense Intelligence Agency)

Transforming Defense Analysis

By Catherine Johnston, Elmo C. Wright, Jr., Jessica Bice, Jennifer Almendarez, and Linwood Creekmore

The Defense Intelligence Enterprise is on the precipice of tremendous change. The global environment is experiencing a mind-numbing quantity and diversity of challenging crises. Perhaps not since the end of World War II have so many pockets of instability and change confronted the Intelligence Community (IC). These traditional security crises are compounded by global demographic, economic, and climate challenges that need to be viewed through the prisms of nontraditional disciplines.

Against the backdrop of this complex operational environment, the volume, velocity, and variety of data continue to grow at a dramatic pace.[1] The early 21st century has seen groundbreaking disruptive technologies adopted on a global scale, and the pace of technology innovation and further disruptive developments looks to increase exponentially. Drivers of technology innovation are no longer simply government-funded initiatives; commercial and private industries are also involved. Individuals are increasingly empowered with a low barrier of entry for truly sophisticated technological fields. The IC must take advantage of this seemingly boundless information age by leveraging large volumes of data, using

Catherine Johnston is Director for Analysis at the Defense Intelligence Agency (DIA). Elmo C. Wright, Jr., is the Senior Expert for Analytic Modernization and Innovation at DIA. Jessica Bice is an Intelligence Officer in the Defense Counter Terrorism Center at DIA. Jennifer Almendarez is a Strategic Communications Officer at DIA. Linwood Creekmore is an Analyst at DIA.

innovative technology, and employing common analytic strategies and tradecraft to provide the United States and its allies with critical information when and where it is needed.

The Defense Intelligence Agency (DIA) recognizes that the collective response of these defense all-source enterprises to such challenges will be significantly limited by the stark realities of fiscal austerity. The intelligence budget is unsustainable given fiscal pressures, and yet it is inadequate considering the scope and scale of current and future operational requirements. The solution will not be in lobbying for additional funds—mandated reductions and decreased budget authorizations must be adhered to—but rather in effectively transforming our tradecraft and technology. We are addressing the threat environment by aligning our priorities with the 2014 National Intelligence Strategy objectives: innovating the way we share data while safeguarding it, managing the defense intelligence analytic enterprise, investing in our people, and working with our partners.[2] In this article, we examine in turn how we are doing in each of these four areas. The article then concludes with what the future of defense all-source analysis might look like.

Innovating Information-Sharing While Safeguarding Data

The defense intelligence ecosystem has evolved rapidly over the past 10 years, but our analytic methodologies have only incrementally adapted to the changing environment. As of 2012, more than 90 percent of the stored data in the world had been created in the previous 2 years.[3] Historically, information in the IC was disseminated through single intelligence discipline stovepipes according to the specific sensor that detected it. This method of receiving data forced the all-source analyst to hunt for and gather information in these stovepipes—basically finding all of the disparate pieces of information and acting as the manual fusion engine for single-source reporting. Given the manual method of collecting information, we estimate that at least 70 to 80 percent of an all-source analyst's work hours is spent searching and compiling information, and less than 20 percent is actually spent performing higher order analytics of the assembled data.[4]

The crux of this inefficiency is the onset of large electronic data sets that have created challenges for analysts in how they retrieve, mine, and amalgamate information to glean key insights. As automated data expand, analysts are overwhelmed, with no reasonable chance to find all the relevant information, much less analyze it. Instead, analysts spot-check roughly 1,400 data sources for information they believe will be most relevant.[5] This introduces hidden biases, as analysts are more likely to seek data sources that reinforce their preconceived opinions. Unfortunately, data can become operationally useful only if we can make sense of it at the right time and in the right context. The intelligence analytic enterprise must find a way to ensure analysts can access data from areas, tools, and platforms not previously discoverable. This challenge is the driving force behind DIA's analytic modernization initiative.

Working in conjunction with the Director of National Intelligence's information technology strategy, the IC Information Technology Enterprise (IC ITE, or "I sight"), and the Mission User Group, DIA is facilitating this fundamental shift in the analytic environment. The IC ITE architecture will enable the Intelligence Community to become more transparent, efficient, and effective, moving us from an individual, agency-centric model to an enterprise model that shares resources and data. The common cloud-based data architecture will reconcile single-source, multi-source, and all-source collection and analysis in near real time. This new IT architecture provides a tremendous opportunity to reimagine our intelligence process in ways that eliminate dissemination stovepipes, increase multi-intelligence data-sharing, and integrate knowledge at the data layer, thus eliminating, or at least reducing, the existing linear and labor-intensive tasking, collecting, processing, exploiting, and disseminating process. IC ITE will significantly enable and make easier a number of cross-agency analytic modernization efforts, such as object-based production (OBP).

Object-based production is a concept being implemented as a whole-of-community initiative that fundamentally changes the way the IC organizes information and intelligence. Reduced to its simplest terms, OBP creates a conceptual "object" for people, places, and things and then uses that object as a "bucket" to store all information and intelligence produced about those people, places, and things. The object becomes the single point of convergence for all information and intelligence produced about a topic of interest to intelligence professionals. By extension, the objects also become the launching point to discover information and intelligence. Hence, OBP is not a tool or a technology, but a deliberate way of doing business.

While simple, OBP constitutes a revolutionary change in how the IC and the Department of Defense (DOD) organize information, particularly as it relates to discovery and analysis of information and intelligence. Historically, the IC and DOD organized and disseminated information and intelligence based on the organization that produced it. So retrieving *all* available information about a person, place, or thing was primarily performed by going to the individual repository of each data producer and/or understanding the sometimes unique naming conventions used by the different data producers to retrieve that organization's information or intelligence about the same person, place, or thing. Consequently, analysts could conceivably omit or miss important information or erroneously assume gaps existed.

OBP aims to remedy this problem and increase information integration across the IC and DOD by creating a common landing zone for data that cross organizational and functional boundaries. Furthermore, this business model introduces analytic efficiency; it reduces the amount of time analysts spend organizing, structuring, and discovering information and intelligence across the enterprise. By extension, OBP can afford

analysts more time for higher orders of analysis while reducing how long it takes to understand how new data relate to existing knowledge. A central premise of OBP is that when information is organized, its usefulness increases.

A concrete example best illustrates the organizing principle of OBP and how it would apply to the IC and DOD. Consider a professional baseball team and how OBP would create objects and organize information for all known people, places, and things associated with the team. At a minimum, "person" objects would be created for each individual directly associated with the team, including coaches, players, the general manager, executives, and so forth. As an example of person-object data, these objects would include characteristics such as a picture, height, weight, sex, position played, college attended, and so forth. The purpose is to create, whenever possible, objects distinguishable from other objects. This list of person-objects can be enduring over time and include current and/or past people objects or family or previous team relationships.

In a similar fashion, objects could be created for the physical locations associated with the team, including the stadium, training facility, parking lots, and players' homes. The same could be done for "thing" objects associated with the team, such as baseballs, bats, uniforms, training equipment, team cars/buses/planes, and so forth.

With the baseball team's objects established, producers could report information to the objects (for example, games, statistics, news for players, or stadium upgrades), which would serve as a centralized location to learn about activity or information related to the team. Also, relationships could be established between the objects to create groupings of objects that represent issues or topics. For example, a grouping of people-objects could be created to stand for the infield or outfield, coaching staff, or team executives. Tangential topics/issues such as "professional baseball players involved in charity" could be established as well. Events or activities (such as games) and the objects associated with them could also be described in this object-centric data construct. Moreover, the concept could expand to cover all teams in a professional baseball league or other professional sports or abstract concepts that include people, places, or things.

Similar to the example above, the IC and DOD will create objects for the people, places, things, and concepts that are the focus of intelligence and military operations. Topics could include South China Sea territorial disputes, transnational criminal organizations, Afghan elections, and illicit trade. Much like the sports example, IC and DOD issues have associated people, places, and concepts that could be objects for knowledge management.

OBP is dependent on implementation, evolution, and maturation of policies and technologies to set the conditions for IC and DOD transition to OBP as a core production process. OBP services—as they relate to object management, data storage and availability, access control, and security—will largely depend on the infrastructure, policies, and capabilities that come with IC ITE.

OBP services will be delivered as a back-end cloud-based platform service within IC ITE and take full advantage of enterprise security capabilities related to access control and auditing.[6] IC ITE will establish and recognize the electronic identity for all users across the IC and DOD enterprises, with a computer-recognizable understanding of the types of data that each user is allowed to access, regardless of agency affiliation.[7]

This IC ITE capability perfectly complements OBP's data-conditioning standards to "atomize" data. Within the OBP framework, as data are objectified, individual data fragments (such as individual facts about the object) will be tagged with a classification. This is effectively called *atomization* of data.[8] Combining OBP's data atomization and IC ITE's enterprise capability to recognize user access privileges, object views will be assembled dynamically based on the role, authorities, and access of the individual user at machine speeds on enterprise IC and DOD data, regardless of agency affiliation.[9] This is important not only for data access control measures but also for data-auditing purposes. Enterprise managers will have a retrievable history of the types of data each user accessed, potentially at the specificity of knowing which individual object facts were retrieved.

The path forward faces significant challenges. Existing stovepiped processes are well entrenched in DOD. Even in its early stages, IC ITE will change both analytic behavior and intelligence processes, though current pilot programs are not fully operational because the architecture is still stabilizing. Until we have a stable architecture, we must maintain the legacy system, data, and associated processes. IC ITE–enabled analytic integration and exposure to sources of data at the point of system ingestion will provide a much richer knowledge pool; however, this integration will require a concerted change-management program to standardize changes across the Defense Intelligence Enterprise and the IC.

Analytic efficiency, increased productivity, and a stronger, more robust intelligence enterprise are the promises of analytic modernization. These big data–enabled gains across the IC are particularly critical in a time of fiscal austerity and an increasingly complex operational environment. Austerity and complexity will compel the community to function as a cohesive, integrated, and responsive unit. The pilot programs are already driving cultural and behavioral changes for both collectors and analysts. Continued community innovation in data-handling methods will increase collection efficiency and analytical accuracy. Ultimately, these efficiencies will translate into heightened responsiveness and accuracy when meeting the demands of warfighters, policymakers, and national leaders.

In the future, an analyst will begin the day at both the operational and strategic levels by reviewing automated aggregated data and deciphering anomalies to instantaneously begin interacting with key strategic, operational, and tactical colleagues. Collectors and analysts working together in a networked, nonstovepiped environment will leverage collaboration to focus collection and

analytic assessments when informing decisionmakers. Though these pilot programs are in their nascent stages, DIA is committing time and resources to ensure successful, full-operating capability. These pilot programs are the basic building blocks that will enable the true transformation of defense all-source analysis.

Managing the Defense Intelligence Enterprise

Leveraging the Defense Intelligence Analysis Program. A centralized management structure of the Defense Intelligence Enterprise is necessary to drive down duplication and create efficiencies across the enterprise to meet the mission in an era of declining resources and growing requirements. The Defense Intelligence Analytic Program (DIAP) Enterprise includes DIA, nine combatant commands, five Service intelligence centers, two subunified commands, and the Commonwealth partners. Functionally managed by DIA's Directorate for Analysis, DIAP ensures resources are properly aligning to each enterprise member's core mission areas as defined by the National Intelligence Priorities Framework.

Prior to 9/11, the DOD Intelligence Production Program (DODIPP) was the managing entity of analytic production components in the department. After 9/11, the establishment of DIAP dismantled the unpopular DODIPP in favor of a decentralized program that essentially allowed each member to perform the entire breadth of capabilities for its respective organizations, which in turn created enterprise-wide duplications and redundancies. DIAP shifted the focus from quantity of production to level of effort by measuring outcomes rather than counting products. In this case, "outcomes" refers to things that took place as a result of analytic effort, such as operations or special activities.

After DOD funding decreased in 2014 and 2015, DIAP was the only vehicle through which the enterprise could implement changes to defense intelligence processes adjusted to diminished resources. Today, DIAP manages risk mitigation and requirements prioritization. The new era of defense intelligence analysis demands collaboration among all analytic partners. Reduced funding countered by increasing requirements necessitates unified effort and much tighter integration among enterprise members. Primary responsibility resides where primary capability resides, and this critical synchronization of enterprise capabilities not only creates trust among members, but it also enables necessary transparency under the new paradigm of shared responsibility.

Director of National Intelligence James Clapper gives testimony before Senate Intelligence Hearing, January 30, 2012 (Kit Fox/Medill/Flickr)

Technology Solutions to Provide Transparency. DIA is investing in the transparency needed to maximize the efforts of every analyst with a suite of initiatives and tools. The Source is a consolidated production portal that will function as an aggregator of all finished defense intelligence, regardless of organization, on one site. It will improve and increase discoverability for customers, reduce the likelihood of duplicative production, and bolster the expectation that intelligence analysis relies on the existing body of knowledge. The next generation of The Source and the underlying technologies, such as Defense Intelligence Online, will add tools related to production management, tasking, and individual profiles.

One capability enables analysts and customers to see trending analytic subjects based on usage from across the enterprise. This capability makes use of an existing technology that tracks intelligence use and aims to correlate production and usage data for better security, business analytics, and customer service. In addition, production data are mined to provide a "Find the Expert" capability that ensures customers are able to contact an expert for follow-on questions or for future collaboration across the enterprise on any given topic searched. By investing in better tools to capture analytic levels of effort (business analytics), we enable

greater insight that allows every member of the defense intelligence all-source analytic community to understand where the enterprise must focus its efforts. Ensuring that these technologies and data schemas are common across the enterprise also ensures a transparent baseline of information to make more informed decisions.

Investing in Our People

Training and Career Management for Common Understanding. In the longer term, training and tradecraft that foster confidence and trust in products across the enterprise will need to be addressed. Currently, even if analysts find the right expertise or product, they must be confident that their own analytic rigor is mirrored in the products authored by outside organizations. Even with all of the tools and communication vehicles available to analysts, an uncoordinated product that is duplicative is easier than trying to leverage outside expertise for a collaborative, more holistic product.

To build the levels of professional trust and skills needed for this degree of sophisticated collaboration, DIA is making strategic investments in training, education, and professional development. We will establish and measure critical analytic skills for the Defense Intelligence Enterprise through the analyst professional certification program. The program will assess analyst knowledge and performance of critical skills and emphasize continuous analytic proficiency through lifelong learning. These shared skill standards will ensure analysts in the Defense Intelligence Enterprise are synchronized in their use of analytic tradecraft.

Improving and adhering to standards ensure that all-source defense intelligence analysts are equipped with the best tradecraft and skills to perform at peak levels. We have graduated two foundational Professional Analyst Career Education classes for new DIA analysts who received extensive formal training in their first 6 months. We also have developed a curriculum, which was rolled out in October 2014, geared for midlevel analysts and has graduated six classes. We are also refreshing our senior ranks with a 3-day executive version—the third class was just completed in September.

This robust training will give analysts the skills for foundational and advanced analytic tradecraft, and incorporate the latest intelligence and academic methods related to military capabilities, network analysis, sociocultural analysis, analytic design, and alternative futures. Most importantly, this professional development will ensure a superior level of tradecraft. Investing in common training standards will instill a culture of trust by creating analytic cohesion and transparency. This strategy is a cost-effective way for the greater Defense Intelligence Enterprise to minimize duplication and bolster existing networks to create analytic reserve strength. Moreover, DIA understands the need for hiring individuals with nontraditional skills who can operate in an environment where tools and methodologies must change as quickly as data evolve.

That said, the major challenge over the next decade is to develop intelligence officers who better understand the IC apparatus. Analysts must have a broader range of experiences outside traditional intelligence analysis, in both strategic and operational environments. We need analysts who understand nontraditional sources, work comfortably inside collection platforms, fully comprehend the strategic and operational needs of the broad set of defense customers, and can drive focused collection to address key intelligence gaps by using quantitative methodologies and innovative tools. In the fiscally austere future, actively managing intelligence officers will be critical to ensure a collaborative, trusting, and efficient enterprise.

Working with Our Partners

In an increasingly complex world with a wide range of collection targets, we must take advantage of not only our own intelligence assets but those of our foreign partners as well. DIA has always recognized the enormous value of coalition partners and the added value they bring to collection and analysis. Their collaborative participation has provided an important outside perspective that has informed our own in production of strategic defense intelligence in both joint and combined environments. We must understand the culture of our allies' intelligence services and that their intelligence collection employs different methods, under different assumptions, and with different analytical lenses. Understanding these differences up front facilitates seamless exchanges during times of crisis, when relationships are put to the test and are the most valuable.

The United States and its allies possess comparative advantages in different regional and functional areas. This potential allied strength should be leveraged through delineating analytic areas on which we can be interdependent. For example, one of our allies may have a comparative advantage in a part of the world where the United States is less engaged. By relying on that ally's expertise to cover that part of the "intelligence perimeter," we can realign our focus on problems where our strengths lie. Such mission-sharing is a smart investment for the enterprise and the broader Intelligence Community.

This interdependence requires a high level of trust and mutual commitment between the United States and its intelligence partners, as well as the acceptance of some risk in those areas and the loss of the expert knowledge that comes with the day-to-day focus on them. Yet in a time of fiscal austerity, deepening partnerships will expand our capacity to understand the operational environment in mission areas with limited focus. This is a fundamental reason that DIA established its Five Eyes Center, with Commonwealth allies working alongside U.S. analysts to develop more efficient and effective intelligence-sharing practices while breaking down cultural-sharing barriers.

Impediments to better integration with our allies are a combination of a traditional reluctance to share sensitive information and policy and information technology issues. These barriers must be overcome. With analytic modernization efforts based in technology improvements, information-sharing becomes

easier for even the most junior analyst. As that tagging of data is completed at the "atomic" level, making the information releasable without revealing sourcing becomes automatic. When analysts can see the shared knowledge, collaboration with allied partners becomes easier.

In the mid-term, DIA has placed resources and people to reexamine our security policies in light of the current information environment. When information is shared in near real time and highly dynamic situations render analysis perishable, we cannot afford a lengthy release process. We must put in place the proper authorities and develop agreements or understandings with allies to mitigate becoming mired in process. Over time, an ad hoc patchwork of agreements will do little to address the holistic concerns dealing with releasability. The IC challenge is to ensure the range of policy and authorities related to the complex question of releasability deals with the current operational environment and technology.

Our allies and partners have been an integral part of how we overcome the complex operating environment that requires both policy and technical solutions to optimize our collaboration. Synchronization of these efforts holds great promise for focusing and integrating the capabilities of DIA with those of our allies and partners.

The Future Look of Defense All-Source Analysis

The challenges that defense intelligence faces are complex and will require innovative solutions if we are to maintain a strategic advantage. Fortunately, more than a decade of integrated operations in the field has provided a blueprint. Joint operations have already proved that the hardest problems are solved not by a single intelligence discipline or single agency. Breakthroughs derive from technological advances that naturally enhance cross-intelligence discipline collaboration and elimination of organizational and cultural barriers. Yet the field is not the hallways of Washington, and the operational boundaries between brigades are not the interagency community. What worked in a forward area cannot always be generalized to another venue, and we do a disservice if we try to directly translate lessons that worked in an interagency task force in Afghanistan to a large and complex organization such as DIA without adapting such lessons to the scale of the organization and the unique processes inherent therein.

Afghan National Army soldiers wait for updates during runoff elections at Forward Operating Base Gamberi, Laghman Province, Afghanistan, June 14, 2014 (U.S. Army/Dixie Rae Liwanag)

The operational interaction with intelligence will look different in the future. Historically, operators have been given a lengthy analytic paper or a large intelligence annex describing enemy composition, disposition, and most likely courses of action. In the future, using analytic models of enemy doctrinal templates, the IC will create a dynamic environment that will enable the warfighter and policymaker to interact with enemy weapons systems, command and control apparatus, and doctrine in a more dynamic, iterative environment.

A current example of this modeling and simulation (M&S) technique has been developed at DIA's Missile and Space Intelligence Center (MSIC). MSIC analysts, in close cooperation with their National Air and Space Intelligence Center (NASIC), National Ground Intelligence Center (NGIC), and Office of Naval Intelligence/Farragut Technical Analysis Center (ONI/FTAC) counterparts, are providing combatant commands with projected threat capabilities to counter U.S. contingency operation plans. These threat performance assessments, requested specifically by the planning elements at the major commands, have led to significant modifications to existing contingency plans, including target allocations; munitions selection platform routing; weapons tactics; targeting rules of engagement; and intelligence, surveillance, and reconnaissance placement. These innovative techniques, refined through years of iterative process improvement, are now adopted for use in the U.S. research, development, and acquisition communities.

Building on these M&S-based analyses for the combatant commands, MSIC is leading development of the next generation of integrated analysis capability. The Integrated Threat Analysis and Simulation Environment (ITASE) provides DOD with a modeling and simulation capability to predict the holistic performance and effectiveness of foreign and U.S. weapons systems and plans. ITASE, which is jointly developed by DIA/MSIC and NASIC, NGIC, and ONI/FTAC, establishes a standard solution for integrated weapons system modeling, simulation, and analysis across

Japanese nationalist far-right group Ganbare Nippon stages Senkaku Islands protest, January 23, 2013 (Wikimedia Commons)

intelligence production centers. The environment brings together disparate weapons systems models from different IC organizations to evaluate complex scenarios, including examinations of antiaccess/area-denial and contested and degraded environments. This type of analysis is the future and is integral to how customers interact with the avalanche of intelligence data.

Leaders of large intelligence organizations must take what action they can to overcome obstacles that organizational history presents them. This future of a modernized analytic environment will succeed only when leaders foster the breakdown of single-source stovepipes, invest in the modernization of analysis, drive efficiencies across the enterprise, invest in people, and partner with our allies. The real art of such leadership is to identify the key elements that will change the organizational culture and to work to operationalize those elements.

Defense intelligence must become better organized, and the synchronization effort through the leadership of DIA can increase cooperation throughout the defense intelligence all-source analytic community, increasing the cogency of analytic effort and the effectiveness of collection. The challenges of big data that analysts face will be mitigated by how we develop our personnel and the tools and concepts we provide that optimize their abilities.

Ultimately, DIA must support the warfighter across the spectrum of military operations; that is the benchmark by which all of our actions must be measured. In the 21st century, warfighting effectiveness includes a great deal more than active combat; it includes the full range of military options open to our national leadership, from security force assistance to nuclear war. The Defense Intelligence Agency and the defense intelligence all-source analytic enterprise must position themselves for success now and in the future, creating a collaborative intelligence environment with allies, partners, and the Intelligence Community. **JFQ**

Notes

[1] General Keith Alexander, USA (Ret.), "Closing Remarks at Accumulo Summit, June 2014," June 12, 2014, available at <http://accumulosummit.com/archives/2014/program/talks/>.

[2] *The National Intelligence Strategy of the United States 2014* (Washington, DC: Office of the Director of National Intelligence, 2014).

[3] Rosemary Heiss, "GEOINT IT Changing to Better Support Analysts, Integrated Intelligence," *Pathfinder* 10, no. 1 (September–October 2012), 6–7, available at <www1.nga.mil/MediaRoom/Press%20Kit/Documents/Pathfinder%20Magazines/2012/2012_sept-oct.pdf>.

[4] Steve Lohr, "For Big-Data Scientists, 'Janitor Work' Is Key Hurdle to Insights," *New York Times*, August 17, 2014.

[5] Heiss.

[6] Chief Information Officer (CIO), Office of the Director of National Intelligence (ODNI), "Enterprise Audit," *DNI.gov*, available at <www.dni.gov/index.php/about/organization/chief-information-officer/enterprise-audit>.

[7] CIO, ODNI, "IdAM: Full Service Directory," *DNI.gov*, available at <www.dni.gov/index.php/about/organization/chief-information-officer/idam-full-service-directory>.

[8] CIO, ODNI, "REST Service Encoding Specifications for Security Markings," *DNI.gov*, available at <www.dni.gov/index.php/about/organization/chief-information-officer/rr-security-markings>.

[9] CIO, ODNI, "XML Data Encoding Specification for Need-To-Know Metadata," *DNI.gov*, available at <www.dni.gov/index.php/about/organization/chief-information-officer/need-to-know-metadata>; CIO, ODNI, "REST Service Encoding Specifications for Security Markings."

Army and Air National Guardsmen carefully exit helicopter pad during PATRIOT Exercise 2015 at Mile Bluff Medical Center in Mauston, Wisconsin, July 2015 (U.S. Air National Guard/Paul Mann)

Improving Joint Interagency Coordination

Changing Mindsets

By Alexander L. Carter

Joint interagency coordination is incredibly important but difficult work that is hampered by cultural differences among team members and an absence of clear and focused performance measures. Despite some rare successes in interagency work between the Department of Defense (DOD) and other partners in the past 20 years, successful interagency teamwork remains elusive across the combatant commands. This article examines the recent history of joint interagency coordination, discusses some of the key cultural and organizational impediments facing these teams, and introduces a set of performance measures for immediate use across these commands. These measures, if adopted by these teams, would positively impact performance and inform our senior civilian and military leadership on the nature of how we exercise national power to support our allies and defeat our enemies.

Major Alexander L. Carter, USAR, is a U.S. Army Civil Affairs Officer. He currently works in the Leader Development Division in the U.S. Army Human Resources Command at Fort Knox.

Why It Matters

Clearly, the world is getting more dangerous and unpredictable, and not just within the traditional paradigms of war and conflict. There have been global and regional conflicts involving the United

States, but there have also been natural and manmade disasters (hurricanes, earthquakes, tsunamis, oil spills, refugee crises, and so forth) around the world. And we have supported our allies and friends in their own humanitarian and disaster recovery efforts. At the discretion of the President and Congress, we have responded to many of these events by typically leveraging our military resources through any one of the unified combatant commands. Increasingly, these manmade and natural conflicts and disasters create a new and much more complicated set of challenges—that is, wicked problems—for our military planners. These problems require a different set of skills, ones that are increasingly being sourced outside of our military structure and institutions.

Wicked problems are almost impossible to solve. For example, there are multiple stakeholders whose interests are linked to the problem(s). Wicked problems are unique; they are not discrete. Typically, as the wicked problem gets analyzed, it morphs into a new or different set of problems.[1] In short, those holding opposing viewpoints would (and should) approach these problems from different biases, perspectives, and experiences in order to create a "shared understanding of the problem[s],"[2] especially when they cannot be "solved by traditional processes."[3] Thus, the U.S. military's opportunities to work more closely with its non-DOD (that is, interagency) partners have never been more relevant and timely. We cannot solve or attempt to solve these wicked problems without the expertise and skills of those drawn from all of our instruments of national power (diplomatic, information, military, and economic, or DIME),[4] including those from outside the government sector (contractors, academicians, not-for-profit agencies, corporations, and so forth). Joint interagency teams, therefore, should be increasingly viewed as attractive forums and vehicles to leverage our combined national power in support of U.S. interests, at home and abroad. So how has joint interagency work evolved and progressed (or not) over the years, and what lessons can help us make better use of these unique organizations?

Ups and Downs

In the last 25 years, the U.S. experience with joint interagency coordination has evolved, spurred by our military interventions in Panama (1989–1990), Somalia (1992–1994), and Haiti (1994–1995).[5] Reflecting on those interventions, President Bill Clinton issued Presidential Decision Directive 56, "Managing Complex Contingency Operations," in May 1997, which established standardized processes and structures relating to joint interagency coordination.[6] However, a report reviewing the directive criticized the joint interagency environment, citing a continuing lack of a "decisive authority and . . . the contrasting approaches and institutional cultures."[7] Later, with our involvement in the wars in Iraq and Afghanistan, President George W. Bush promulgated national-level guidance relating to joint interagency coordination on December 7, 2005: National Security Presidential Directive 44, "Management of Joint Interagency Efforts Concerning Reconstruction and Stability."[8] The directive expanded the need for joint interagency coordination across the "spectrum of conflict: complex contingencies, peacekeeping, failed and failing states, political transitions, and other military interventions."[9]

Another key publication that continued the evolution of joint interagency coordination was Joint Publication (JP) 3-08, *Interorganizational Coordination During Joint Operations*,[10] which established guidance within DOD on the structures and processes in place to support joint interagency coordination, including key U.S. Government agency responsibilities and lead designations for different types of military and nonmilitary interventions. JP 3-08 also formalized a joint interagency team structure that U.S. Central Command had created years earlier: the Joint Interagency Coordination Group. The goal of JP 3-08 was to:

provide sufficient detail to help Combatant Commanders, subordinate Joint Force Commands, their staffs, and joint interagency partners understand the Joint Interagency Coordinating Group (or equivalent organization) as a capability to enable the coordination of all instruments of national power with joint operations.[11]

It is during this period of recent history, and with the backdrop of these supporting directives and policies, that we can point to some rare but relevant success stories with joint interagency work, despite organizational and cultural obstacles. Two such examples are the Bosnian train and equip program and Joint Interagency Task Force–South.

Congress funded the Bosnian train and equip program following the Bosnian war and the 1995 signing of the Dayton Peace Accords.[12] The objective of the program was to provide the Bosnian Federation military force with training, weapons, and other types of equipment to build up their capability to defend themselves against the neighboring Serbian military. An interagency task force that drew its ranks initially from DOD, the Department of State, and the Central Intelligence Agency was created to oversee the program.

At the outset, the task force faced significant challenges. Initially, it had "no money, no equipment, and no training."[13] But during the first 2 years of operation, the task force was able to obtain adequate funding, secure and execute critical training contracts, obtain weapons (mostly donated from other countries), and overcome anti-U.S. sentiment against the program at home and abroad. Yet in writing about the task force, its former deputy Christopher Lamb asserts that its success was due to a combination of organizational, team, and individual variables. Ultimately, Dr. Lamb surmised, the train and equip program "rectified the military imbalance between Bosnian Serb and Federation forces, reassuring the Bosnians and sobering the Serbs,"[14] and it "facilitated the integrated approach the United States pursued in Bosnia, proving remarkably adept at implementing its controversial security assistance program."[15]

Another example of interagency success is Joint Interagency Task Force–South (JIATF-South), headquartered in Key West, Florida. Its mission is to conduct "interagency and international

detection and monitoring operations, and the interdiction of illicit trafficking and other narco-terrorist threats in support of national and partner nation security."[16] Since its latest formation in 2003, when it combined with another task force (JIATF-East), the team's composition has reflected a diverse body of team members including all branches of the U.S. military, U.S. Coast Guard, Drug Enforcement Administration, Federal Bureau of Investigation, National Security Agency, National Geospatial-Intelligence Agency, Central Intelligence Agency, and U.S. Customs and Border Protection. Additionally, JIATF-South has a plethora of international partners across the region. Over the past 10 years, JIATF-South's accomplishments have been impressive, with its successes allowing "JIATF-South to stand toe-to-toe with the drug traffickers . . . driving up their costs, cutting their profits, raising their risk of prosecution and incarceration, and forcing them to divert their trade to less costly destinations . . . accounting for roughly 50 percent of global cocaine interdiction."[17]

Despite these two examples of interagency successes, however, joint interagency coordination within the combatant commands continues to be difficult to achieve despite publications, speeches, briefs, endless memoranda, directives, and working groups. For example, two combatant commands were the subject of a 2010 review by the U.S. Government Accountability Office (GAO).[18] In its report, GAO cited that U.S. Africa Command (USAFRICOM) demonstrated some practices that "sustain collaboration, but areas for improvement remained"[19] in key staff work associated with linking geographic combatant command theater security cooperation plans to country and Embassy strategic plans. In addition, USAFRICOM staff had "limited knowledge about working with U.S. embassies and about cultural issues in Africa, which has resulted in some cultural missteps."[20]

U.S. Southern Command, on the other hand, was viewed as having "mature joint interagency processes and coordinating mechanisms,"[21] but GAO was still critical of the command's handling of its logistical support to the 2010 Haiti earthquake disaster relief effort and the command's underlying joint interagency planning and staffing processes.[22] The U.S. Agency for International Development expressed similar disappointment in its after-action review of that same relief effort, commenting that, in effect, the military commanders on the ground were not adequately educated on the humanitarian assistance/disaster relief operations.[23]

Specialists prepare to investigate mock chemical weapons inside training village of Sangari at Joint Readiness Training Center, Fort Polk, Louisiana (40th Public Affairs Directorate/William Gore)

Why do some interagency teams succeed while others struggle? In reviewing the examples of the Bosnian train and equip program and JIATF-South, Dr. Lamb writes that both interagency teams were successful because they exhibited 10 positive "determinants of effectiveness" within 3 broad performance areas: organizational (purpose, empowerment, and support), team (structure, decisionmaking, culture, and learning), and individual (composition, rewards, and leadership).[24] A successful team will generally have positive indicators within these areas. Similarly, in reviewing interagency teams or environments that were not successful, it can be argued there were negative indicators assessed within these same areas.

Culture Clash and Structure

Two indicators of interagency team success or failure that deserve additional enquiry relate to the team's culture and structure. Perhaps joint interagency coordination can be challenging because

the individuals and institutions they represent are so different in terms of the cultures and organizational structures. For example, in comparing military officers (DOD) with Foreign Service Officers from the Department of State, the contrasts in approach and style are significant. For example, whereas the DOD mission is to prepare for and fight war, the State mission is to conduct diplomacy. Unlike DOD, State does not see training as a major activity or as important for either units or individuals. DOD is uncomfortable with ambiguity, but State can deal with it. Doctrine is seen as critical to DOD but not to State. Where DOD is focused on discrete events and activities with plans, objectives, courses of action, and endstates, State is focused on ongoing processes without expectation of an endstate.[25] DOD views plans and planning as a core activity, yet State views a plan in general terms to achieve objectives but values flexibility and innovation.[26] Is it any wonder, then, that "most Foreign Service Officers spend the majority of their time engaging their host-nation equivalents, not directing actions along a line of subordinates?"[27]

If we are to become more effective with joint interagency coordination, DOD must understand and appreciate the value that joint interagency partners bring to the fight. Joint interagency coordination cannot "be described like the command and control relationships for a military operation. . . . [U.S. Government] agencies may have different organizational cultures and, in some cases, conflicting goals, policies, procedures, and decision-making techniques and processes."[28] Because of the cultural and ideological differences between DOD and non-DOD participants, the level of commitment exhibited by members of this joint interagency team may vary tremendously, which will prevent or impede the team's ability to become a "high performance group."[29]

Joint interagency teams can organize themselves in many ways to accomplish their mission. Too often, though, they face challenges in governance—how work gets done and by whom. One observer noted, "The principal problem of joint interagency decisionmaking is lack of decisive authority; there is no one in charge."[30] In reviewing the more scientific study of organizational psychology, an argument can be made that joint interagency teams fit the definition of "leaderless groups," which are those that "usually do not have a professional leader or facilitator who is responsible for the group and its functioning."[31] Instead, members assume the role of leader or facilitator. The purpose for which the group was created can become lost or blurred over time. Group members who assume the role of leader are likely to be untrained in group leadership and consequently may not understand group dynamics and how to manage group leadership tasks. These groups may run the risk of groupthink that produces a situation where disagreement and differences are not tolerated.[32] Some basic team tasks, such as enforcing ground rules and team norms, may not be accomplished. Finally, team meetings may lack structure, focus, or direction.[33]

Given these cultural and structural challenges, joint interagency teams may benefit from a common set of standards or measures to strive toward, linking them with common standards and norms. Joint interagency teams may benefit by using some methods to evaluate how effective they are within their respective combatant commands. The questions surrounding measurement of joint interagency teams, however, are initially daunting: How do you measure teamwork? How do you measure coordination? How do you quantify a group's success when most of its products and services (such as advice) are not quantifiable? Should we compare our joint interagency efforts to other similar organizations or functions in other combatant commands? Any measures adopted by the team must be clear, unambiguous, and unifying to the team.

Performance Measures

Group behavior and performance in a joint interagency group would be most effectively harnessed and channeled by focusing on agreed-upon performance measures. Introducing these critical few measures would help channel discussion, focus, and overall results. The framework developed by Lamb provides a good starting point to assess the environment within which any joint interagency operates.[34] But actionable measures within this framework are needed to tie individual, team, and organizational performance together. What measures are needed?

The military typically refers to measures of effectiveness (MOEs) and measures of performance (MOPs). *MOEs* are defined as criteria used to assess changes in system behavior, capability, or operational environment that are tied to measuring the attainment of an endstate, achievement of an objective, or creation of an effect. *MOPs* are defined as criteria used to assess friendly actions tied to measuring task accomplishment.[35] Taken together, these measures can inform and drive team performance if built and regularly reported on. According to JP 3-0, *Joint Operations*, "continuous assessment helps the Joint Force Command and joint force component commanders determine if the joint force is doing the right things (MOE) to achieve its objectives, not just doing things right (MOP)."[36] MOEs and MOPs add concrete, tangible indicators of whether a joint interagency team is operating effectively, but these measures should be grouped according to a general area of observation or performance.

Both are important types of measures for the purposes of driving joint interagency team behavior and performance. In the table, the first column includes the 10 Postulated Determinants of Effectiveness that serve as an overall performance framework through which to measure level of joint interagency success; the second column specifies the Supporting Measures. This column is a collection of example performance measures (a combination of MOEs and MOPs).

Building and Using Performance Measures

The work of joint interagency teams could and should be measured primarily in how they produce advice, conduct coordination, and, in some cases, lead the combined U.S. Government

Table. Postulated Determinants of Effectiveness and Supporting Measures

Purpose	Mission, goals, objectives, and measures regularly reviewed and adjusted by sponsoring agency or command leadership. Customer satisfaction surveys consistently score in "meets" or "exceeds" expectations in terms of interagency products, services, and support.
Empowerment	Team members are able to speak and make resource decisions on behalf of their home agency. One or more team members are deployed with joint task force or equivalent organization in support of a regional event requiring a U.S. whole-of-government response.
Support	A percentage of theater security cooperation activities and exercises is supported and resourced by non–U.S. Government partners annually. Development of Annex V and supporting theater campaign plans (TCPs) is led by a Senior Executive Service (SES) civilian from an interagency partner.
Structure	Leadership of team (facilitator) is rotated monthly on a random basis. X members of the joint interagency team are permanently staffed/embedded within the combatant command's current or future operations directorate (J33 or J35). Ratio of assigned versus authorized joint interagency billets is equal at each combatant command. Team member tours are at least 12 months and no more than 36 months in length.
Decisionmaking	A number of combatant command's TCPs are synchronized with country work plans annually. A percentage of TCPs is completed with joint interagency input annually.
Culture	A number of non-DOD personnel from joint interagency teams are formally trained on DOD combatant command planning processes. A percentage of joint interagency personnel who have received onsite Embassy briefs from country teams within the combatant command's area of operation is present. Location of team meetings is rotated monthly on a random basis. Cultural briefs/social events among DOD, State Department, and other interagency partners are held on a quarterly basis.
Learning	A number of intergovernmental/nongovernmental organizations (IGOs/NGOs) partner with combatant command and/or State Department participating in TCP reviews, discussions, and plan approvals. A percentage of joint interagency personnel who receive foreign language training (and tested) annually through combatant command or home agency are present. A number of joint interagency personnel (non-DOD) who have system access to a combatant command's Theater Security Cooperation Management System (or equivalent) are present. Team-sponsored symposiums on joint interagency work within the region occur. Team-authored articles on joint interagency work within the region are published.
Composition	Team members represent the full spectrum of support that can be provided through joint interagency coordination (governmental, IGO, NGO, nonprofit, business sector). Level of funding for mobilized Reservists who support joint interagency exercises (civilian expertise) is equal.
Rewards	Formal and informal training opportunities are offered to joint interagency team members based on informal group consensus-driven "Order of Merit List" based on individual contributions to supporting team products and services. Performance evaluations are completed by general officer/SES equivalents.
Leadership	A number of wicked problems are introduced, discussed, and solved annually relevant to the team's area of responsibility. Quarterly state of interagency work is briefed to senior leadership who provide support to the joint interagency team or command (DOD, State Department, other).

Source: Table based on Christopher J. Lamb with Sarah Arkin and Sally Scudder, *The Bosnian Train and Equip Program: A Lesson in Interagency Integration of Hard and Soft Power*, INSS Strategic Perspectives 15 (Washington, DC: NDU Press, March 2014), 57.

response to planned or unplanned events around the world in support of national interests and as directed by senior diplomatic or military leadership. But how does one truly measure teamwork? How can performance measures really gauge how well team members cooperate or how well they provide outstanding staff support to their command or joint activity? To answer this question, the team should understand the areas of performance that it can influence within its structure and mission by conducting a team assessment of where it stands and where it needs to go. This is done through three simple steps.

First, a team self-assessment must be conducted using the framework areas of performance, focusing on where the team rates generally positively or negatively for each of the 10 areas within the framework. For example, one team's members might review the framework and self-assess that while they generally are doing fine in the areas of composition, decisionmaking, and leadership, they believe that they could do better in culture, structure, and empowerment. This initial and subjective team assessment sets a baseline for where to improve team performance. This should be a subject of hearty discourse and heated debate—an agenda item that may be best planned as a singularly focused offsite retreat. Second, the team should identify a set of a few critical measures (5–7 MOPs or MOEs within the table) across organization, team, and individual areas. The team may choose the ones offered in the table or create others more appropriate,

Crew of Coast Guard Cutter *Stratton* stands by to offload 34 metric tons of cocaine in San Diego, California, August 2015 (U.S. Coast Guard/Patrick Kelley)

adhering to the principle of definition that each measure be specific, measurable, attainable, relevant, and timely.[37] Third, each measure must be selected with the endstate of improving joint interagency team results.

The team should then assign someone to be responsible for collecting the data and tracking and reporting the team's progress against each agreed MOP and MOE. That person is also responsible for helping to define where the team wants to go with that area of performance. As such, the measure will have some clear thresholds of what determines underperforming, performing, or overperforming. The point is that the team determines which measures are right for it and charts a path forward on how to achieve success in these measures.

Any joint interagency team members can take the measures they have adopted to help them channel their individual and collective energies toward more productive activity. Measures will give the team focus, direction, and added meaning as team members seek to support their command organization, whether it be a combatant command or some other joint activity. Individuals will benefit from being able to link their efforts and contributions to the team. They will be able to report back to their parent commands or agencies in a more factual and descriptive manner, informing their leadership in richer ways about how their agency is supporting this joint effort. But these measures will not only drive performance and results within each joint interagency team; this new model or framework with its supporting measures also has the opportunity to influence and inform the most senior levels of military leadership.

There are many forms of joint interagency team constructs within the U.S. Government. The more familiar ones may be found within unified combatant commands or even at Embassies, but there are others. Regardless of where they are and whom they support, these teams operate within an enterprise, driven by either senior military or civilian leadership. These teams may ultimately report to four-star generals, Federal agency administrators, governmental senior executives, or even specially appointed directors with quasi-governmental jurisdiction and powers. All of these leaders are charged with the responsibility to support their organizational or enterprise mission and track progress toward goals and objectives on a regular basis. The measures developed for joint interagency teams can be a critical component of a leader's evaluation of how joint interagency teams are supporting their "customers." One technique borrowed from the business sector that is worth a brief mention is the power of comparing similar activities (in this case, joint interagency coordination) across geographies (that is, U.S. Southern Command, U.S. European Command, U.S. Central Command) or even comparing similar functions (that

is, theater security cooperation activities). Why do this?

As senior leaders are facing increasingly complex problems within their areas of interest and operation and are being asked to do more with less through appropriated funding constraints, they also are having to question the efficiency and effectiveness of the programs and activities for which they are responsible. By comparing similar activities or functions using the same measures, leaders could be better informed about the resource and manpower decisions they make within these joint support activities.

Many leading businesses, whether in the manufacturing, service, or retail industries, for example, regularly score their performance using industry standard measures. Using this internal assessment, they can see how their company performance stacks up against other similar companies in the same industry. For example, a manufacturing company may have as one of its key measures or metrics a need to capture "purchase order cycle time." This would be a metric that would be regularly updated, reported on, and assessed relative to how other companies were performing in this same metric. Information on this measure would be collected from various sources on a regular basis. It is assumed that this metric is so universal that a comparison of company-level performance across the industry would be instructive because it would allow the company to see how it is doing relative to its peers—where it stands. This review offers the company an external, independent look at a part of its operations and usually motivates it to improve upon key aspects of its business. This process is called *benchmarking*, which can be defined as:

a standard of performance . . . benchmarking helps organizations [to] *identify standards of performance in other organizations and to import them successfully to their own. It allows them to discover where they stand in relation to others. By identifying, understanding, and comparing the best practices and processes of others with its own, an organization can target problem areas and develop solutions to achieve the best levels of government.*[38]

Soldier with 5th Battalion, 3rd Field Artillery Regiment, 17th Field Artillery Brigade, 7th Infantry Division readies firefighting gear at unit headquarters on Joint Base Lewis-McChord, Washington, August 2015 (28th Public Affairs Directorate/Patricia McMurphy)

Benchmarking is an example of a productivity solution (or management tool) in the business world that can be properly applied to the joint interagency environment. Another way to look at benchmarking (which should have increasing relevance to the government in light of continuing Federal budget challenges) is as "the routine comparison with similar organizations of administrative processes, practices, costs, and staffing, to uncover opportunities to improve services and/or lower costs."[39]

Critics of using self-defined measures to benchmark themselves against others might be afraid of what they may find. As Jeremy Hope and Steve Player write, "Benchmarking is the practice of being humble enough to admit that others are better at something than you are and

wise enough to learn how to match or even surpass them."[40] Proponents of this benchmarking practice, on the other hand, argue that "setting aspirational and directional goals can inspire and motivate teams. The process recognizes that everything is connected and achieving any one goal depends on making progress towards all others."[41]

The measures introduced above should be further discussed, defined, and operationalized within each combatant command. With adopted measures in place, joint interagency teams are better able to chart a course of improvement by understanding where they are (baseline) and where they need to go (endstate). But these measures by themselves are of limited value if they are not put in the broader context of how similar joint interagency activities are performing across the combatant commands, since each of these commands competes for funding and resources. For example, are there some measures that should be candidates for comparison across combatant commands, despite their differences in mission, climate, geography, the type of interagency supported historically provided, and so forth? How can we compare joint interagency activities across the DOD enterprise using metrics defined within our own combatant command?

Final Thoughts

The United States will continue to be called upon to support its allies and fight its enemies across a broad spectrum of conflict. Our measured response to each of these calls for help should not be confined to purely military or diplomatic lines. As we see more wicked problems taking the world stage, we must look to our joint interagency teams and the commands and agencies they represent to deliberate on and provide advice across the full range of our national instruments of power (DIME). But these teams will continue to be hamstrung by cultural clashes and structural challenges unless changes are put in place to properly structure and support these teams. By doing so, the teams could leverage the combined talents and resources from capabilities across government, the nonprofit sector, academia, and even the business sector.

These changes to our joint interagency teams would involve a mental shift in the way they (and others) evaluate their performance through meaningful performance measures. These measures must gauge not only whether we are doing things right, but also whether we are doing the right things. Through the adoption of a performance framework and supporting measures, teams can channel their energies, talents, and resources to support the leaders entrusted to represent national interests overseas. With measures in place and teams properly aligned, the Nation's leaders, civilian and military, can begin an informed dialogue about how to potentially assess and benchmark team performance that cuts across and transcends geographies, jurisdictions, and commands. **JFQ**

Notes

[1] Debra E. Hahn, "Predicting Program Success—Not Child's Play," *Defense AT&L* 43, no. 1 (January–February 2014), 46.

[2] Gabriel Marcella, *Affairs of the State: The Interagency and National Security* (Carlisle Barracks, PA: U.S. Army War College, 2009), 38.

[3] Christopher M. Schnaubelt, "Complex Operations and Interagency Operational Art," *PRISM* 1, no. 1 (December 2009), 47.

[4] Joint Publication (JP) 3-0, *Joint Operations* (Washington, DC: The Joint Staff, August 11, 2011), VII.

[5] Marcella, 29.

[6] Ibid.

[7] Ibid., 30.

[8] Ibid., 31.

[9] Ibid.

[10] JP 3-08, *Interorganizational Coordination During Joint Operations* (Washington, DC: The Joint Staff, March 17, 2006).

[11] Ibid., D-1.

[12] Christopher J. Lamb with Sarah Arkin and Sally Scudder, *The Bosnian Train and Equip Program: A Lesson in Interagency Integration of Hard and Soft Power*, INSS Strategic Perspectives 15 (Washington, DC: NDU Press, March 2014).

[13] Ibid., 24.

[14] Ibid., 56.

[15] Ibid., 118.

[16] See Joint Interagency Task Force–South Web site at <www.jiatfs.southcom.mil/index.aspx>.

[17] Evan Munsing and Christopher J. Lamb, *Joint Interagency Task Force–South: The Best Known, Least Understood Interagency Success*, INSS Strategic Perspectives 5 (Washington, DC: NDU Press, June 2011), 76.

[18] U.S. Government Accountability Office (GAO), *Interagency Collaboration Practices and Challenges at DOD's Southern and Africa Commands*, GAO-10-962T (Washington, DC: GAO, July 2010).

[19] Ibid., 2.

[20] Ibid.

[21] Ibid., 3.

[22] GAO, *U.S. Southern Command Demonstrates Interagency Collaboration, but Its Haiti Disaster Response Revealed Challenges Conducting a Large Military Operation*, GAO-10-801 (Washington, DC: GAO, July 2010), 1.

[23] Donald A. Ziolkowski, "Whole of Government Approaches: How Can We Capitalize on the Experience of Our Reserve Forces in Order to Ensure a Whole of Government Approach to Unfolding Crises? Can We Ensure We Replicate Inter-agency Processes During Large-scale Exercises?" unpublished paper, Joint Forces Staff College, April 2013.

[24] Lamb with Arkin and Scudder, 57.

[25] Schnaubelt.

[26] Ibid.

[27] Ibid., 43.

[28] *Commander's Handbook for the Joint Interagency Coordination Group* (Norfolk, VA: U.S. Joint Forces Command, March 1, 2007), II-2.

[29] David W. Johnson and Frank P. Johnson, *Joining Together: Group Theory and Group Skills*, 9th ed. (Boston: Pearson Education, Inc., 2006), 20.

[30] Marcella, 37.

[31] Nina Brown, *Facilitating Challenging Groups: Leaderless, Open, and Single Session Groups* (New York: Routledge, 2013), 5.

[32] Ibid., 3.

[33] Ibid., 88.

[34] Lamb with Arkin and Scudder, 57.

[35] JP 1-02, *Department of Defense Dictionary of Military and Associated Terms* (Washington, DC: The Joint Staff, November 8, 2010), 159.

[36] JP 3-0, II-10.

[37] George T. Doran, "There's a S.M.A.R.T. Way to Write Management's Goals and Objectives," *Management Review* 70, no. 1 (1981), 35–36.

[38] Jeremy Hope and Steve Player, *Beyond Performance Management: Why, When, and How to Use 40 Tools and Best Practices for Superior Business Performance* (Boston: Harvard Business Review Press, 2012), 87–88.

[39] Mark Howard and Bill Kilmartin, *Assessment of Benchmarking within Government Organizations* (New York: Accenture, 2006).

[40] Hope and Player, 94.

[41] Ibid., 33.

U.S. Army paratroopers assigned to 1st Battalion, 503rd Airborne Infantry Regiment, 173rd Airborne Brigade Combat Team prepare to jump while conducting airborne operations during exercise Allied Spirit II at U.S. Army's Joint Multinational Readiness Center in Hohenfels, Germany, August 13, 2015 (U.S. Army/Matthew Hulett)

Decentralized Stability Operations and Mission Command

By Jeffrey M. Shanahan

Since the term first appeared in U.S. Army Field Manual 100-5, *Operations*, published in 1982,[1] *mission command* has steadily risen to prominence as the Armed Forces' preferred command and control (C2) strategy.[2] In fact, "the decentralized execution of centralized, overarching plans"[3] permeates joint and individual Service publications across the spectrum of military missions, from amphibious warfare to stability operations.[4] Yet arguably mixed results and seemingly slow progress in applying the concept to the stability operations mission set in Iraq and Afghanistan over the last decade have called into question the efficacy of the approach and its suitability to Phase IV contexts. The increasingly strategic, political gravity of otherwise tactical decisions in such environments, it is argued, renders the risks associated with decentralized execution simply too high,[5] while the decidedly robust and capable nature of contemporary U.S. military communications networks leaves the approach ostensibly unnecessary. Furthermore, the complexity, turbulence, and dynamism inherent in postconflict environments make setting the clear, concise objectives and engendering the shared understanding so critical to successful mission command exceedingly difficult.[6]

Lieutenant Commander Jeffrey M. Shanahan, USN, is the Program Manager for the Air Training Program of the Chief of Naval Air and is on the Staff of the Chief of Naval Air Force Reserve.

Local police, government leaders, and villagers gather outside new Anaba District Center in Panjshir Province, Afghanistan, August 11, 2008, to view weapons turned in through Disbandment of Illegal Armed Groups program (DOD/Jillian Torango)

Paradoxically, many of these same characteristics necessitate the highly adaptable, flexible, and rapid decision and execution processes that mission command is uniquely suited to afford. Phase IV operations rarely provide clear distinctions among offensive, defensive, and stabilization efforts, demanding a C2 system capable of quickly transitioning from one mission set to the next, and often encompassing all three simultaneously.[7] Solutions must be tailored, often to individual communities or villages,[8] leaving a one-size-fits-all approach inefficient at best, and more often entirely ineffective. Adversary C2 networks, despite paling in technological sophistication compared to U.S. systems, are quick, elusive, and highly efficient, demanding that U.S. approaches afford superior speed and flexibility as minimum capabilities.[9] Finally, the significant increase in applicable stakeholders inherent in stability operations—coalition and interagency partners, nongovernmental organizations, and private volunteer organizations—render traditional military C2 structures ill suited to the more holistic, team-based solutions required.[10]

In an attempt to address these competing concerns, this article examines the effectiveness and suitability of mission command as it pertains to postconflict stability operations. This is accomplished through a brief analysis of two decentralized C2 approaches as well as a more detailed examination of three contemporary initiatives in Operation *Enduring Freedom* (OEF) and Operation *Iraqi Freedom* (OIF). In short, it is posited that acknowledged shortcomings in the success of stability operations in OEF/OIF are attributable not to underlying weaknesses in mission command as a theoretical construct, or to its lack of suitability to Phase IV operations, but to a failure to meet fully the prerequisites so critical to the concept's success. Ultimately, mission command remains an essential tool in overcoming the complex challenges inherent in Phase IV operations, and an essential tenet of U.S. military doctrine, one that should be further refined, developed, and studied as a means of ensuring future operational effectiveness.

Historical Context

The concept of distributive, decentralized leadership and mission execution in military operations is by no means new. Emerging in response to decisive defeats by Napoleon at Jena and Auerstädt in 1806, the concept is generally attributed to Field Marshal Helmuth von Moltke the Elder, Prussian and then German Chief of Staff from 1857 to 1888.[11] First termed *Auftragstaktik*, the theory hinges upon the dispersed decisionmaking, initiative, and creativity of subordinates, each guided by a superior commander's larger objectives,

constraints, and intent.[12] U.S. interest in mission command, despite the evidence of its dramatic potential displayed by German tactical ingenuity during World War II,[13] and the more obvious limitations of the U.S. penchant for centralized C2 processes in Vietnam,[14] did not begin in earnest until confronted by the numerical superiority of an impending Soviet Cold War threat.[15] Notwithstanding the relative diminishment of that threat in recent decades, the increasing complexity and dynamism of the modern battlespace and the world as a whole account for continued interest in mission command as a fundamental C2 concept among U.S. and several international forces.[16]

The strategy was most recently reemphasized as central to U.S. military operations and culture in particular by General Martin Dempsey in a white paper entitled *Mission Command*, published in April 2012. General Dempsey noted, "Our need to pursue, instill, and foster mission command is critical to our future success in defending the nation in an increasingly complex and uncertain operating environment."[17] As described by the general, mission command is characterized by three overarching attributes or enablers: understanding, intent, and trust.[18] These principles also generally complement those identified by researchers studying the Dutch military's mission command doctrine: autonomy of action, clarity of objectives, adequacy of means, and trust between commanders.[19] Taken in sum, such attributes reflect a continually evolving understanding of mission command as a guiding C2 strategy, yet also highlight the credible challenge in adequately quantifying what remains a fundamentally psychosocial leadership theory. Nonetheless, the widespread and lasting appeal of decentralized mission execution is abundantly clear.

Likewise, the prevalence of stability operations as a contemporary military mission set, and the concept's development as a refinement of the more generalized term *military operations other than war*,[20] is increasingly apparent. In fact, a 2004 Defense Science Board study found that, on average, the United States has conducted postconflict stability operations every 18 to 24 months since the end of the Cold War, with each operation lasting from 5 to 8 years.[21] Moreover, while stability operations in Afghanistan and Iraq have undoubtedly taken center stage among U.S. foreign military interests, Michael J. McNerney, former Director of International Policy and Capabilities in the Office of the Deputy Secretary of Defense for Stability Operations, notes that additional, concurrent Phase IV operations conducted in the Philippines, Yemen, Georgia, and the Horn of Africa are clear evidence of the firmly entrenched nature of stability operations as a 21st-century U.S. military mission set.[22]

U.S. military doctrine, however, has been slow to acknowledge this stark reality. Not until November 2005, with the issuance of Department of Defense Directive 3000.05, were stability operations established as "a core U.S. military mission" to be afforded "priority comparable to combat operations."[23] An accompanying U.S. Army field manual dedicated to the subject was not released until October 2008,[24] and a joint publication of the same name did not appear until September 2011.[25] Even more recently, then–Secretary of Defense Chuck Hagel suggested in 2014 that fiscal year 2015 defense budget proposals would limit the U.S. military's ability to conduct future stability operations on the magnitude of those seen in OIF/OEF,[26] perhaps reigniting the debate concerning Phase IV operations as a core U.S. military competency. The strategic implications of this discourse are ultimately well outside the scope of this article, but both the enduring nature of stability operations as an inevitable consequence of armed conflict, and the prevalence of such operations in the post–Cold War environment, are impossible to ignore.

Two Decentralized C2 Antecedents

While the U.S. military's doctrinal commitment to mission command and the prevalence of Phase IV operations as a contemporary military mission are readily evident, less so is the relationship between the two, and more specifically, the potential and suitability of decentralized C2 constructs in meeting the daunting challenges presented by stability operations. Prior to assessing mission command's validity in modern postconflict contexts, however, it is prudent to consider its historical antecedents. While some form of Phase IV operation has accompanied virtually every sustained U.S. combat effort, the two in which C2 decentralization efforts bear closest resemblance to OEF/OIF stability operations, and the two therefore most suited to comparison, are those conducted during the Philippine-American and Vietnam wars.

At the conclusion of formal hostilities in the Philippines in 1902, U.S. efforts to stabilize the country and its population were largely based upon the decentralized, tactical unit execution of larger strategic and operational intent. Employing more than 500 small garrisons throughout the islands,[27] the United States succeeded in neutralizing the remaining insurrection and stabilizing the Filipino population within 1 year of conflict termination,[28] an accomplishment made all the more remarkable by a decade of similar struggle in OEF/OIF. According to historian John Morgan Gates, ultimate success in stability operations in the Philippines was attributable to both the broad distribution of American units as well as to the wide variety of techniques and tactics employed by localized subordinate commanders.[29] In fact, the writer purports that much of the credit for any transfer of American ideals or conventions to the subsequent colonial government was a result not of a grand operational initiative, but rather the relationships between individual soldiers and the Filipino population.[30]

While the positive impact of decentralization in stability operations during the Philippine-American War is strikingly obvious, its effectiveness during Phase IV of the Vietnam War is less palpable, largely overshadowed by more conventional approaches that met with eventual failure.[31] While admittedly slow in reaching its ultimate form, the U.S. Civil Operations and

Revolutionary Development Support (CORDS) program, organized around small civil-military provincial teams positioned throughout all 250 districts in South Vietnam,[32] is heralded as a definitive bright spot in an otherwise dark U.S. experience.[33] In fact, it has been suggested that a more comprehensive commitment to the program as a priority in Vietnam may have ensured U.S. victory in the conflict.[34] Regardless, the notable success of the CORDS program is attributable in large part to its decentralization. Characterized by significant levels of local adaptation, senior CORDS leadership "specified only the chain of command, certain functional sections, and a presence at the district level, but left subordinates free to adjust the organization to the circumstances."[35] Such an approach, based in the empowerment of subordinate commanders to act within a broad set of operational guidelines, to determine *how* to accomplish the *what* and *why* specified by superior commanders, lies at the heart of mission command. While certainly not without its limitations, the historical precedent for the effectiveness of the concept in Phase IV operations is undeniable.

Contemporary Conflicts

History will also judge the lasting effectiveness of decentralized C2 strategies in contemporary conflicts, and yet a more detailed analysis of U.S. efforts to exercise mission command in OEF/OIF is warranted as a means of assessing the concept's continued applicability to Phase IV operations. Three such efforts are examined in this pursuit: the Commander's Emergency Response Program (CERP), the Provincial Reconstruction Team (PRT) construct, and the Village Stability Operations (VSO) program. Arguably, the more mixed success in the majority of these initiatives relative to their historical antecedents renders them invaluable in assessing the assertion that U.S. struggles with stability operations in OEF/OIF are due more to larger failures to set the aforementioned conditions for mission command than to any weakness in the strategy itself.

Commander's Emergency Response Program. CERP, first initiated in Iraq and later in Afghanistan, was designed to provide tactical commanders direct access to discretionary endowments in support of postconflict reconstruction and development efforts.[36] First funded by recovered Ba'athist Party cash stockpiles discovered in Baghdad during the 2003 invasion, the program sought a more flexible, adaptive, and timely solution to the challenges of Phase IV operations at the local level.[37] Stated simply, the idea was to allow "soldiers who are patrolling the streets, and have a ground-level view of people's needs, to make a quick impact without having to go through the bureaucratic details that government contracts usually require."[38] These impacts, though decided on and executed by subordinate leaders, were to be governed by larger objectives, constraints, and reporting mechanisms set by joint task force and geographic combatant commanders.[39] Recognition of the program's initial success led to the appropriation of U.S. funds in continued support of the initiative in Iraq, and later accounted for its adoption in Afghanistan.[40] Remarkably, CERP grew to encompass more than 10 percent of Afghanistan's gross domestic product by 2010,[41] and inspired the development of a commander's handbook titled *Money as a Weapons System*, published in April 2009.[42]

Despite its popular success, however, CERP has been the subject of much criticism. *Washington Post* columnist Ariana Eunjung Cha highlights concerns that the program provided *too* much autonomy to local commanders, who possessed little to no detailed knowledge regarding contracting or development operations, and that a relative lack of supervision generated a system susceptible to corruption.[43] *Foreign Policy* columnists Andrew Wilder and Stuart Gordon similarly cite a lack of contextual and cultural understanding on the part of U.S. military commanders concerning the fundamental "zero-sum nature of Afghan society and politics," with aid projects often "creating perceived winners and losers" and subsequently producing a decidedly *de*-stabilizing effect.[44] And, in an *Interagency Journal* article, Timothy D. Gatlin suggests that CERP, like many military initiatives, is ultimately susceptible to a larger military culture in which short-term, largely quantitative measures of performance are prized over longer term, more qualitative measures of effectiveness. As a result, CERP initiatives, Gatlin argues, often failed to consider larger sustainability issues,[45] and the subordinate commanders responsible for them often lacked adequate forces to ensure consistent supervision and security of reconstruction efforts.[46]

Taken together, these criticisms highlight the credible limitations of decentralized C2 strategies in postconflict stability operations. However, suggesting that these shortcomings invalidate the concept of mission command in such contexts altogether ignores the significant successes enjoyed by the program. In merely 1 year in Iraq, for example, CERP-funded initiatives resulted in 999 water and sewage repair projects; 1,758 road, bridge, and similar infrastructure reconstruction ventures; 188 humanitarian relief distribution efforts; 742 projects aimed at facilitating local government standup; the refurbishment of over 400 schools; and the repatriation of countless Iraqis displaced by the conflict.[47] More importantly, evidence suggests that such largely quantitative measures, at least in part, were successful in achieving the desired qualitative effect. "When well spent," notes Mark S. Martins, CERP "funding convinced Iraqis of coalition commitment to their well being, increased the flow of intelligence to U.S. forces, and improved security through economic conditions."[48]

A closer examination of the criticisms also highlights ambiguous and often competing operational objectives. While perhaps not consciously stated or intended by superior commanders, an amalgamation of security, stability, economic development, and humanitarian assistance goals, each a distinct mission in its own right, undermined the clarity of intent so crucial to effective mission command.[49] The improperly prioritized reward systems further exacerbated this phenomenon, as subordinate

Soldiers rehearse night-raid training mission as part of Steadfast Javelin II, a NATO exercise focused on increasing interoperability and synchronizing complex operations between allied air and ground forces through airborne and air assault missions (USEUCOM/143rd Expeditionary Sustainment C)

commanders were frequently forced to choose between the needs of the local community and the favor of higher headquarters.[50] Finally, the lack of adequate force strength with which to supervise and provide security for CERP initiatives reflects a failure to ensure that appropriate means to accomplish the mission were afforded to subordinate commanders, another key prerequisite of mission command.

Provincial Reconstruction Teams. Much like CERP, the PRT concept, first introduced by U.S. forces in the capital of Afghanistan's Paktia Province, Gardez, in December 2002,[51] was designed to confront the diversity inherent in the country's distinctly provincial and tribal culture.[52] Comprised of relatively small and highly autonomous civil-military teams, the overarching objectives of the PRT system were the extension of the Afghan government at the provincial level, security of ongoing interagency and nongovernmental organization operations, intelligence and information-gathering and dissemination, and the facilitation of minor reconstruction and development efforts.[53] Individual teams were ultimately responsible to regional area coordinators, an executive steering committee, and the International Security Assistance Force headquarters,

Students of Sar Asyab Girls High School in Kabul sing national anthem of Afghanistan at ribbon-cutting ceremony commemorating completion of new school funded by U.S. Forces–Afghanistan Commander's Emergency Response Program (U.S. Air Force/Jordan Jones)

which set broad operational objectives and constraints.[54]

C2 strategies were characteristically loose, seen as consultative rather than directive, exhibiting a definitive preference for decentralization.[55] Like CERP, the PRT program has been lauded for "great success in building support for the U.S.-led coalition and respect for the Afghan government. . . . [It has] played important roles in everything from election support to school-building to disarmament to mediating factional conflicts."[56]

In recognition of these successes, in November 2005 the model was also adopted in Phase IV operations in Iraq.[57] While divergent in structure and organization from its OEF counterpart (OIF PRTs were civilian led, not military-led OEF teams), the overall objectives of the program in Iraq remained relatively constant[58] and clearly demonstrated the U.S. belief in, and commitment to, the decentralized execution of stability operations.

In spite of these notable accomplishments, McNerney notes that "PRTs always have been a bit of a muddle," plagued by "inconsistent mission statements, unclear roles and responsibilities, ad hoc preparation, and most important, limited resources [that] have confused local partners and prevented PRTs from having a greater effect."[59] These sentiments are echoed by Mark Sedra, who adds that the strict and frequent turnover of PRT personnel rendered achieving unity of effort difficult,[60] and by Touko Piiparinen, the lead political advisor to PRT Meymaneh in 2006, who notes that a complete lack of standardization in PRT structure often set the conditions for constant change within the PRT decisionmaking process.[61] Former Foreign Service Officer Mark Dorman, in reference to OIF PRTs in particular, notes that teams were consistently established without regard for whether the province in question had truly shifted from conflict to stability,[62] without clear objectives or authority,[63] and with wholly inadequate logistical support, often lacking basic office supplies in what came to be commonly, albeit tragically, referred to as the "pencil problem."[64]

Such criticisms are undoubtedly alarming and well justified, yet again signal a failure *not* in the decentralization of C2 in stability contexts, or in the adoption of mission command itself, but rather an unequivocal failure to recognize, appreciate, and cultivate the conditions for its success. A failure to establish commander's intent prohibited a unified and cohesive response to stabilization, characterized by "the impression that the PRTs were to be observing and facilitating everything—being all things to all people—but not actually

accomplishing anything vital to the political or military mission."[65] The competing priorities of civilian and military leadership, and the same ambiguous assessment mechanisms that troubled CERP initiatives, further limited clarity of intent and prevented a common understanding among PRT leaders and their operational commanders.[66] For example, performance measurements with regard to the Disbandment of Illegal Armed Groups, a common PRT mission, oscillated between the qualitative sociopolitical signals valued by civilian leadership and the quantity of weapons collected prioritized by military superiors.[67] Finally, inadequate human and material means with which to accomplish the assigned mission both limited the program's potential success and undermined the mutual trust so central to mission command.

In sum, each of these shortcomings inhibited the overall effectiveness of decentralized C2, not because it was unsuited to Phase IV operations but because it was never given a chance to work. In fact, it may be argued that in the absence of the aforementioned conditions, mission command was not, in fact, being exercised at all; rather, some amorphous or mutated form of C2 falling well outside the doctrinal spectrum was being employed. The resulting effect, as expressed from the perspective of Foreign Service Officers, was often that of being let go or abandoned, a mere "pin on a map" seen as politically favorable but lacking the true mission focus or commitment of senior leadership.[68] Further evidence of these conclusions is provided by the fact that PRT performance was assessed to have improved significantly as the program's objectives became clearer and focused; as sufficient personnel, equipment, and financial support were provided; and as tour lengths of PRT personnel were extended (allowing more time to build common understanding and trust).[69] As a more specific example, James A. Russell argues that the issuance of Integrated Civil Military Campaign Plans by General Stanley McChrystal and Ambassador Karl Eikenberry in the summer of 2009, and by General David Petraeus and Ambassador Eikenberry in early 2011, were instrumental in clarifying objectives and priorities within the stabilization and reconstruction effort, "nest[ing] tactical operations by military units and supporting activities by civilian agencies with the operational and strategic levels of the war."[70]

Village Stability Operations. While the effectiveness of CERP and the PRT program was undoubtedly mixed, a third U.S. attempt at mission command, the VSO program, has met with decidedly more consistent success. Started in the fall of 2009, the program is led predominantly by U.S. special operations forces (SOF) in conjunction with limited civil affairs and military information support operations personnel. The overall goals were to facilitate organic village-level security capability through the development of Afghan Local Police (ALP) and, much like the PRT program, connect local community leaders to larger district and provincial governments.[71] Exhibiting the essence of mission command, former VSO participant and SOF operator Rory Hanlin describes the program as "characterized by managing and completing a vast array of seemingly unrelated tasks that interact in complex unimaginable ways, all in a system of decentralized execution."[72] That such efforts have achieved notable progress in many areas of Afghanistan is well documented in terms of notable reductions in coalition and civilian casualties, security incidents, and enemy-initiated attacks, as well as a November 2011 national intelligence estimate that cited VSO as markedly more successful than other coalition initiatives.[73] The 2012 and 2013 iterations of the Department of Defense *Report on Progress Toward Security and Stability in Afghanistan* similarly highlight the VSO and ALP programs as making considerable advancements in the stability of rural Afghanistan and its population.[74]

While admittedly of limited duration relative to CERP and the PRT program, the fact that VSO have thus far enjoyed more consistent success in the application of decentralized C2 strategies to Phase IV operations is quite clear. In fact, the seemingly stark contrast in results between the CERP/PRT and VSO initiatives begs the question: what made the ultimate difference? In large part, the disparity seems attributable to VSO's more comprehensive satisfaction of the conditions and prerequisites for effective mission command.

While still significantly ambiguous, the relatively more narrow objectives set for VSO by senior operational leaders, namely the development of ALP forces and connection of community leaders to the larger district and provincial government, resulted in greater clarity and understanding of commander's intent by subordinate units. Likewise, the highly specialized cultural and linguistic training of SOF relative to more conventional forces undoubtedly facilitated the deeper contextual understanding so critical to effective mission command—and so critically lacking within CERP.[75] Such factors are also likely to have positively influenced the trust that operational leaders were willing to place in VSO unit commanders compared to their less specialized PRT counterparts, fulfilling another key condition for decentralized C2. The significantly more limited scope of VSO compared with CERP and PRT efforts, as well as the more reliable funding and personnel support provided to SOF, ensured means were adequate to conduct the mission assigned. Finally, the adoption of more reasonable and accurate assessment mechanisms for the VSO program, considered fluid and constantly evolving in response to local conditions, limited the disunity of effort that seemed to plague the CERP and PRT models,[76] reinforcing shared understanding of *what* was to be accomplished and *why*, but leaving the *how* in the hands of subordinate commanders.

The limited critiques that have been offered regarding VSO rightly center upon the program's long-term sustainability. Developing ALP in sufficient numbers to ensure Afghanistan's continued stability is likely to stretch U.S. SOF capability to the limit, and continued reliance upon U.S. funding for the project is a credible challenge.[77] Furthermore, while the specialized cultural and linguistic training possessed by SOF is undoubtedly a mission command multiplier, it is

impractical and far from financially feasible to expect the same level of training to be afforded on any large scale, though some would argue that U.S. ranks are "flush with highly-trained, highly-intelligent, and highly-capable Soldiers [who] would serve as ideal supplements to the VSO mission."[78] Likewise, it is increasingly politically difficult for the United States to limit the scope of its stability operations to those areas that force capability will allow—though lessons learned from operational art would suggest that limiting the scope would be a prudent course of action.

Conclusion and Recommendations

Ultimately, the challenges mentioned herein, while irrefutably significant, do little to dismiss the fact that mission command is both the best and arguably the only command and control construct capable of maximizing the success of postconflict stability operations in a global environment increasingly characterized by complexity and disorder. Furthermore, it is apparent that in the absence of the concept's prerequisites—intent, understanding, trust, and means—success in Phase IV operations will continue to prove elusive and inconsistent. How, then, might operational commanders best create, develop, and sustain an environment conducive to the decentralized execution so critical to effective stability operations? While by no means all encompassing, several lessons may be deduced.

The first is that the intricacy and dynamism inherent in contemporary postconflict contexts are unlikely to diminish, and may in fact continue to increase in future conflicts.[79] This reality will also undoubtedly increase the already substantial difficulty faced by senior leaders in clearly and concisely articulating operational objectives and a larger commander's intent. Thus, senior leaders must grow comfortable in embracing several concurrent lines of effort, often with seemingly wide divergence along the stability operations spectrum, and in prioritizing them as clearly as possible for subordinate units. Security, counterinsurgency, humanitarian assistance, development, and other stability goals must be made as distinct as possible, and coupled with a clearly delineated precedence that allows subordinate commanders to quickly shift and adapt their missions as conditions change. Likewise, assessment mechanisms must be flexible and robust enough to assess largely qualitative effects, placing no undue pressure on subordinate commanders to adopt a strategy unsuited to the contextual nuances of the unique and perhaps completely opposite situation they might face compared with units only yards or miles away.

These are difficult challenges, and while certainly worthy of an operational commander's best effort, the pursuit of the remaining preconditions for mission command (understanding, trust, and means) may prove more fruitful. In fact, research suggests that increasing capability in these areas may offset the deficiency in clarity of objectives associated with the ambiguity often inherent in Phase IV contexts.[80] Increased levels of understanding or trust between superior and subordinate commanders, for example, may facilitate effective mission command even in the absence of clear intent.

As evidenced by the success of the VSO program, increases in linguistic or cultural training have the potential to improve stability operations outcomes, and these should continue to be a focus for both special operations and conventional forces to the maximum extent feasible. With respect to the challenges to any large-scale cultural awareness program, however, McNerney's suggestions concerning the integration of conventional forces into VSO units, and vice versa, are worthy of further development. Ensuring training and exercises integrate and encourage collaboration of capabilities is also essential moving forward, and will undoubtedly enhance the common understanding so central to trust and effective mission command.

Finally, operational commanders must continue to ensure that adequate means are provided to subordinate commanders for the objectives assigned, or reduce the scope of those objectives accordingly. While seemingly obvious, and a basic principle of effective operational design, shortcomings in this area in OIF/OEF suggest that it is a lesson worth reemphasizing. The reality is that significantly more personnel and material resources are often required to execute stability operations than more traditional or visible Phase III operations;[81] a failure to recognize this reality undermines not only the effectiveness of mission command strategies, but also more broadly the U.S. stability mission as a whole.

The success of decentralized command and control in postconflict stability operations is largely dependent upon the extent to which the preconditions for mission command are set and maintained by operational leaders, and not by any deficiency in its suitability to such contexts. In fact, contemporary Phase IV environments are simply too complex, too dynamic, and too localized to adopt any command and control strategy *other than* mission command. While an undoubtedly daunting challenge, the U.S. military's doctrinal commitment to the construct is well founded, and every effort should be made to ensure its adoption, refinement, and perfection by forces engaged in current and future stability operations. Enduring success depends upon it. **JFQ**

Notes

[1] Eitan Shamir, "The Long and Winding Road: The U.S. Army Managerial Approach to Command and the Adoption of Mission Command (Auftragstaktik)," *Journal of Strategic Studies* 33, no. 5 (2010), 653.

[2] Joint Publication (JP) 1, *Doctrine for the Armed Forces of the United States* (Washington, DC: The Joint Staff, 2013).

[3] Ibid., V-14.

[4] Marine Corps Doctrinal Publication 1-0, *Marine Corps Operations* (Washington, DC: Headquarters U.S. Marine Corps, 2011); and JP 3-07, *Stability Operations* (Washington, DC: The Joint Staff, 2011).

[5] Milan N. Vego, *Joint Operational Warfare: Theory and Practice,* 2nd ed. (Newport, RI: U.S. Naval War College, 2009), X-22.

[6] A.L.W. Vogelaar and E.H. Kramer, "Mission Command in Ambiguous Situations," in *The Human in Command: Exploring the Modern Military Experience*, ed. Carol McCann and Ross Pigeau (New York: Kluwer Academic/Plenum Publishers, 2000), 230.

[7] Jeffrey Buchman, Maxie Y. Davis, and Lee T. Wright, "Death of the Combatant Command? Toward a Joint Interagency Approach," *Joint Force Quarterly* 52 (1st Quarter 2009), 94; and JP 3-07, viii.

[8] James A. Russell, "Into the Great Wadi: The United States and the War in Afghanistan," in *Military Adaptation in Afghanistan*, ed. Theo Farrell, Frans Osinga, and James A. Russell (Stanford: Stanford University Press, 2013), 54.

[9] Charles G. Sutten, Jr., "Command and Control at the Operational Level," in *The Challenge of Military Leadership*, ed. Lloyd J. Matthews and Dale E. Brown (Washington, DC: Pergamon-Brassey's International Defense Publishers, Inc., 1989), 75.

[10] David S. Alberts and Richard E. Hayes, *Command Arrangements for Peace Operations* (Washington, DC: NDU Press, 1995), 14; JP 3-07, xi.

[11] Shamir, 647.

[12] Ibid.

[13] Ibid., 650.

[14] Ibid., 652.

[15] Ibid., 653.

[16] Decentralized execution guided by commander's intent is central to the military doctrine of, among others, Australia, Canada, Israel, the Netherlands, and the United Kingdom.

[17] Martin E. Dempsey, *Mission Command White Paper* (Washington, DC: The Joint Staff, April 3, 2012), 3, available at <www.dtic.mil/doctrine/concepts/white_papers/cjcs_wp_missioncommand.pdf>.

[18] Ibid., 5–6.

[19] Vogelaar and Kramer, 412.

[20] JP 3-07, *Joint Doctrine for Military Operations Other Than War* (Washington, DC: Chairman of the Joint Chiefs of Staff, 1995), available at <http://ids.nic.in/Jt%20Doctrine/Joint%20Pub%203-0MOOTW.pdf>.

[21] Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, *Transition to and from Hostilities*, Defense Science Board 2004 Summer Study (Washington, DC: Department of Defense, 2004), iv, available at <www.acq.osd.mil/dsb/reports/ADA430116.pdf>.

[22] Michael J. McNerney, "Stabilization and Reconstruction in Afghanistan: Are PRTs a Model or a Muddle?" *Parameters* (Winter 2005–2006), 34.

[23] Department of Defense (DOD) Directive 3000.05, "Military Support for Stability, Security, Transition, and Reconstruction (SSTR) Operations," DOD, November 28, 2005, available at <https://www.fas.org/irp/doddir/dod/d3000_05.pdf>.

[24] Field Manual 3-07, *Stability Operations* (Washington, DC: Headquarters Department of the Army, 2008), available at <www.fas.org/irp/doddir/army/fm3-07.pdf>.

[25] JP 3-07.

[26] Nick Simeone, "Hagel Outlines Budget Reducing Troop Strength, Force Structure," *Defense.gov*, February 24, 2014, available at <www.defense.gov/news/newsarticle.aspx?id=121703>.

[27] McNerney, 43.

[28] John Morgan Gates, *Schoolbooks and Krags: The United States Army in the Philippines, 1898–1902* (Westport, CT: Greenwood Press, Inc., 1973), 270.

[29] Ibid., 270–271.

[30] Ibid., 288–289.

[31] McNerney, 44.

[32] Henry Nuzum, *Shades of CORDS in the Kush: The False Hope of "Unity of Effort" in American Counterinsurgency* (Carlisle, PA: U.S. Army War College, 2007), 53, available at <www.dtic.mil/dtic/tr/fulltext/u2/a518709.pdf>.

[33] McNerney, 44.

[34] Jacob Kipp et al., "The Human Terrain System: A CORDS for the 21st Century," *Military Review* (September–October 2006), 10, available at <www.dtic.mil/dtic/tr/fulltext/u2/a457490.pdf>.

[35] Nuzum, 56.

[36] Mark S. Martins, "No Small Change of Soldiering: The Commander's Emergency Response Program (CERP) in Iraq and Afghanistan," *The Army Lawyer* (February 2004), 2, available at <www.jagcnet.army.mil/DOCLIBS/ARMYLAWYER.NSF/0/722f6e45b32037d885256e5b0054c6f1/$FILE/Article%201.pdf>.

[37] Ibid.

[38] Ariana Eunjung Cha, "Military Uses [Saddam] Hoard for Swift Aid; Red Tape Cut, Cash Flows to Iraqi Contracts," *Washington Post*, October 30, 2003, 1.

[39] Martins, "No Small Change," 3.

[40] Ibid., 11.

[41] Gregory Johnson, Vijaya Ramachandran, and Julie Walz, "The Commander's Emergency Response Program in Afghanistan and Refining U.S. Military Capabilities in Stability and In-Conflict Development," paper prepared for Senior Conference at the U.S. Military Academy, West Point, NY, 2011, 6.

[42] *Commander's Guide to Money as a Weapons System*, Handbook No. 09-27 (Fort Leavenworth, KS: U.S. Army Combined Arms Center, 2009).

[43] Eunjung Cha, 1.

[44] Andrew Wilder and Stuart Gordon, "Money Can't Buy America Love," *Foreign Policy* (December 1, 2009), 2, available at <www.foreignpolicy.com/articles/2009/12/01/money_cant_buy_america_love>.

[45] Timothy D. Gatlin, "An Institutional Analysis of the Commander's Emergency Response Program," *InterAgency Journal* 5, no. 1 (Winter 2014), 44, available at <http://thesimonscenter.org/iaj-5-1-winter-2014/>.

[46] Ibid., 45.

[47] Martins, "No Small Change," 8.

[48] Mark S. Martins, "The Commander's Emergency Response Program," *Joint Force Quarterly* 37 (2nd Quarter 2005), 49.

[49] Johnson, Ramachandran, and Walz, 11.

[50] Gatlin, 45.

[51] Touku Piiparinen, "A Clash of Mindsets? An Insider's Account of Provincial Reconstruction Teams," *International Peacekeeping* 14, no. 1 (2007), 143.

[52] Mark Sedra, *Civil-Military Relations in Afghanistan: The Provincial Reconstruction Team Debate*, Canadian Institute of Strategic Studies (CISS) Strategic Datalink #126 (Toronto: CISS, March 2005), 2, available at <www.opencanada.org/ wp-content/uploads/2011/05/SD-126-Sedra.pdf>.

[53] Ibid.

[54] Piiparinen, 149.

[55] Ibid.

[56] McNerney, 33.

[57] Shawn Dorman, "Iraq PRTs: Pins on a Map," *Foreign Service Journal* 24 (March 2007), 21, available at <www.tamlyn-serpa.com/images/ Iraq_PRTs_1.pdf>.

[58] Ibid., 22.

[59] McNerney, 33.

[60] Sedra, 2.

[61] Piiparinen, 149.

[62] Dorman, 31–32.

[63] Ibid., 23.

[64] Ibid., 32.

[65] McNerney, 36.

[66] Ibid.; Piiparinen, 147.

[67] Piiparinen, 147.

[68] Dorman, 23.

[69] McNerney, 38.

[70] Russell, 71.

[71] Seth A. Shreckengast, "The Only Game in Town: Assessing the Effectiveness of Village Stability Operations and the Afghan Local Police," *Small Wars Journal*, March 27, 2012, 2, available at <http://smallwarsjournal.com/jrnl/art/the-only-game-in-town-assessing-the-effectiveness-of-village-stability-operations-and-the-a>.

[72] Rory Hanlin, "One Team's Approach to Village Stability Operations," *Small Wars Journal*, September 4, 2011, 9, available at <http://smallwarsjournal.com/print-pdf/11412>.

[73] Shreckengast, 5.

[74] *Report on Progress Toward Security and Stability in Afghanistan: Report to Congress* (Washington, DC: DOD, December 2012), 77, available at <www.defense.gov/pubs/pdfs/1230_Report_final.pdf>; *Report on Progress Toward Security and Stability in Afghanistan: Report to Congress* (Washington, DC: DOD, July 2013), 97–98, available at <www.defense.gov/pubs/Section_1230_Report_July_2013.pdf>.

[75] Shreckengast, 8.

[76] Hanlin, 9.

[77] *Report on Progress*, 2013, 99.

[78] Shreckengast, 8.

[79] Dempsey, 3.

[80] Vogelaar and Kramer, 422.

[81] McNerney, 34.

The NDU Foundation Congratulates the Winners of the 2015 Writing Competitions

The NDU Foundation is proud to support the annual Secretary of Defense, Chairman of the Joint Chiefs of Staff, and *Joint Force Quarterly* essay competitions. NDU Press hosted the final round of judging on May 15–16, 2015, during which 24 faculty judges from 15 participating professional military education institutions selected the best entries in each category. The First Place winners in each of the three categories are published in the following pages.

Secretary of Defense National Security Essay Competition

In 2015, the 9th annual competition was intended to stimulate new approaches to coordinated civilian and military action from a broad spectrum of civilian and military students. Essays were to address U.S. Government structure, policies, capabilities, resources, and/or practices and to provide creative, feasible ideas on how best to orchestrate the core competencies of our national security institution. The NDU Foundation awarded the first place winner a generous gift certificate from Amazon.com.

First Place
Lieutenant Colonel Wallace R. Turnbull III, USAF
Air War College
"Time to Come in from the Cold (War): Nuclear Force Structure for an Uncertain World"

Second Place
Colonel Patrick J. Dolan, USAF
Air War College
"It Is Time for an International Convention to Ban Permanent Human Enhancements for Warfighting Purposes"

Third Place
Commander William G. Dwyer, USCG
U.S. Army War College
"Interesting Times: China's Strategic Interests in the Arctic"

Chairman of the Joint Chiefs of Staff Strategic Essay Competition

This annual competition, in its 34th year in 2015, challenges students at the Nation's joint professional military education institutions to write research papers or articles about significant aspects of national security strategy to stimulate strategic thinking, promote well-written research, and contribute to a broader security debate among professionals. The first place winners in each category received a generous Amazon.com gift courtesy of the NDU Foundation.

Strategic Research Paper

Lieutenant Colonel (P) Patrick Michael Duggan, USA
U.S. Army War College
"Strategic Development of Special Warfare in Cyberspace"

Second Place
Lieutenant Colonel Michael S. Miller, USAF
Air War College
"Hybrid Warfare: Preparing for Future Conflict"

Third Place
Major Jesse W.J. Hamel, USAF
Air Command and Staff College
"Adaptive Airpower: Arming America for the Future Through 4D Printing"

Strategy Article

First Place
Lieutenant Colonel Robert William Schultz, USA
U.S. Army War College
"Countering Extremist Groups in Cyberspace"

Second Place
Lieutenant Commander Graham C. Winegeart, USN
Naval War College (Junior)
"The Strategic Significance of China's Recent Focus on the Rule of Law"

Third Place
Colonel Samuel L. Calkins, USA
National War College
"Recommendations on Reforming Strategy Development and Implementation"

Joint Force Quarterly Kiley Awards

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

Best Forum Article
Brett T. Williams, "The Joint Force Commander's Guide to Cyberspace Operations," *JFQ* 73

Best Features Article
Joris D. Kila and Christopher V. Herndon, "Military Involvement in Cultural Property Protection: An Overview," *JFQ* 74

Best Recall Article (tie)
Bert Frandsen, "Learning and Adapting: Billy Mitchell in World War I," *JFQ* 72
and
J. Darren Duke, Rex L. Phillips, and Christopher J. Conover, "Challenges in Coalition Unconventional Warfare: The Allied Campaign in Yugoslavia, 1941–1945," *JFQ* 75

Distinguished Judges

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

Front row, left to right: Dr. Larry D. Miller, U.S. Army War College; Ms. Erin L. Sindle, NDU Press; Colonel Tricia York, USAFR, Joint Forces Staff College; Lt Col Michelle Ewy, USAF, Air Command and Staff College; Dr. Donna Connolly, Naval War College; Dr. Richard DiNardo, Marine Corps Staff College; Dr. Benjamin (Frank) Cooling, Eisenhower School. Back row, left to right: Colonel Stephen J. Mariano, USA, National War College; Ms. Joanna E. Seich, NDU Press; Captain Bill Marlowe, USN (Ret.), Joint Forces Staff College; Dr. Jim Chen, Information Resources Management College; Dr. William T. Eliason, Editor in Chief, *Joint Force Quarterly*; Mr. John L. O'Brien, Information Resources Management College; Dr. Stephen Burgess, Air War College; Dr. Larry Garber, Eisenhower School; Dr. James Kiras, School of Advanced Air and Space Studies; Dr. Lindsay P. Cohn, Naval War College; Dr. Ryan Wadle, Air Command and Staff College; Dr. David A. Anderson, Command and General Staff College; Dr. Jan S. Breemer, Naval War College; Dr. James A. Mowbray, Air War College; Dr. Anand Toprani, Naval War College

Not shown: Dr. Antulia (Tony) Echevarria, U.S. Army War College; Dr. Geoffrey Gresh, College of International Security Affairs; Dr. James Lacey, Marine Corps War College; Dr. Andrew Novo, College of International Security Affairs; Ambassador Paul Wohlers, National War College

Photo by Katie Lewis, NDU

Participants in Iran nuclear negotiations in Vienna on day deal was signed (Flickr/Dragan Tatic)

Time to Come in from the Cold (War)

Nuclear Force Structure for an Uncertain World

By Wallace R. Turnbull III

The U.S. nuclear deterrent is at a turning point. Seven decades have passed since a nuclear weapon was used, and many noted leaders have called for the abolition of nuclear weapons altogether—a "Global Zero."[1] At the same time, the legs of the U.S. nuclear deterrent triad are overdue for modernization at a projected cost of $1 trillion over the next 30 years.[2] This modernized triad—consisting of a new long-range bomber and cruise missile, a replacement intercontinental ballistic missile, and a new ballistic missile submarine, as well as refurbished nuclear warheads—will be fielded in the 2030s and, based on historical recapitalization rates, will operate well into the 2060s.

This article considers the strategic environment of 2040 and beyond to assess whether the planned nuclear force structure is sufficient to provide deterrence in the uncertain world of the future. Keir Lieber and Daryl Press observed that the only way to do this "is to work through the grim logic of deterrence: to consider what actions will need to be deterred, what threats will need to be issued, and what capabilities will be needed to back up those threats."[3] This article assesses the U.S. nuclear deterrent using the framework recommended by Lieber and Press to show that the nuclear capabilities provided by the current and planned force are insufficient to provide credible deterrence in the 21st century. It argues for the addition of low-yield, high-accuracy nuclear weapons and electromagnetic pulse weapons to the air leg of the triad to bolster deterrence against limited nuclear war.

The reality that nuclear weapons did not disappear with the end of the Cold War has been acknowledged by a number of scholars, including Keith Payne, Paul Bracken, and Thérèse Delpech, as the so-called second nuclear age.[4] Defined by Bracken as "the spread of the bomb for reasons that have nothing to do with the Cold War," this second nuclear age is characterized by a multipolar world that contains a variety of nuclear actors who wield a range of nuclear weapons and whose interests have nothing to do with U.S.-Soviet dynamics.[5] New nuclear actors such as Pakistan, India, North Korea, and Iran have all decided that these weapons are useful, and established nuclear powers such as Russia have rediscovered the value of such weapons. Russian President Vladimir Putin declared, for example, that "only nuclear weapons allowed Russia to maintain its independence in the troubled 1990s" and that "developing and deploying an entirely new generation of nuclear weapons and delivery systems" will be a main point of Russia's defense modernization activities.[6] This should not be surprising because, as Bracken notes, the United States once "found the bomb a most useful weapon."[7] The stark reality of the second nuclear age is that many actors find nuclear weapons useful and are pursuing their development and acquisition. Some may even use them.

Lieutenant Colonel Wallace R. Turnbull III, USAF, wrote this essay while a student at the Air War College. It won the 2015 Secretary of Defense National Security Essay Competition.

Emerging Strategic Environment

To understand which actions will need to be deterred by U.S. nuclear forces, we must first consider the strategic environment in which deterrence is expected to function. Former Secretary of Defense Robert Gates observed that divining the strategic environment of the future is fraught with uncertainty: "When it comes to predicting the nature and location of our next military engagements, since Vietnam . . . we have never once gotten it right."[8] Rather than making firm predictions, we can only form some broad characterizations that appear likely given the current strategic environment.

According to Bracken, the most significant feature of the second nuclear age is that it is a multiplayer game.[9] Unlike the bipolar Cold War world, the emerging strategic environment is characterized by the existence of many independent nuclear actors. Today, there are many states with nuclear weapons, and the tumultuous history of proliferation suggests this number may grow in the future.[10] A consequence of the multiplayer game is that most nuclear actors now face security threats from more than one nuclear-armed opponent. India, for example, is concerned about deterring both China and Pakistan. This security trilemma, as it has been called by Linton Brooks and Mira Rapp-Hooper, means "actions taken by one state to defend against another state have the effect of making a third state feel insecure."[11] Overlapping security trilemmas suggest crisis stability dynamics are geometrically more complicated in the second nuclear age. Thérèse Delpech noted that one has only to look at the last three centuries of multipolar European history to conclude that the strategic environment of the future is "just as likely to be one of confrontation as of stability" and may indeed be less stable than the bipolar Cold War world.[12]

In the Nuclear Futures Project, Duncan Brown and Thomas Mahnken observed that another feature of the second nuclear age is the "imbalance in political stakes between the United States and potential adversaries."[13] Unlike the Cold War, where the Soviet Union represented an existential threat to U.S. security, the Nation today "has limited stakes in many potential conflicts," while many potential adversaries are likely to view conflict with the United States as an existential threat.[14] This imbalance poses the danger that adversaries may be motivated not only to pursue nuclear weapons but also to use those weapons to avoid defeat by superior conventional power.[15] The key lesson for adversaries in the second nuclear age, as demonstrated by the swift defeat of the regimes of Muammar Qadhafi and Saddam Hussein, is that in a conventional fight with the United States, America's enemies may be "fighting for their lives."[16] Deterring escalation during a conventional conflict when the adversary believes the regime, and even its existence, is at stake may make Cold War deterrence look relatively easy by comparison.[17]

A third feature of the emerging strategic environment is the potential for catalytic instability and escalation from terrorism or a nuclear accident. Terrorism, according to Bracken, provides a catalyst that "was not present in the first nuclear age."[18] For example, a terrorist attack could greatly increase the risk of nuclear escalation if it occurred in the midst of an ongoing Indian-Pakistani crisis. Likewise, catalytic escalation could be caused by terrorists who managed to acquire nuclear material in the form of fuel or radioactive waste from a nuclear powerplant and built a radiological dirty bomb.[19] In addition to terrorism, a nuclear accident would be a powerful catalyst. Though fortunately none resulted in a nuclear explosion, there were at least 32 documented accidents involving U.S. nuclear weapons between 1950 and 1980.[20] The U.S. nuclear stockpile is, on average, more than 20 years old, and many weapons lack modern safety features.[21] The same concerns likely apply to Russia's arsenal. More alarming, however, are newer members of the nuclear club such as Pakistan, which lacks decades of experiential nuclear learning and whose stockpiles of nuclear weapons lack sophisticated safety features.[22] A nuclear accident in this environment is not unthinkable.

Limited Nuclear War in the Second Nuclear Age

Due to the potent combination of multiplayer dynamics with overlapping security trilemmas, imbalanced political interests, and an increasing risk of catalytic escalation, the second nuclear age is likely to be a dangerous one. Jeffrey Larsen argues that these factors and others result in an increasing risk of *limited nuclear war*, defined as "a conflict in which nuclear weapons are used in small numbers and in a constrained manner in pursuit of limited objectives . . . or in the face of conventional defeat."[23] During the Cold War, Herman Kahn suggested that there were "very large and very clear 'firebreaks' between nuclear and conventional war."[24] In Kahn's firebreak model, there were strong incentives for the United States and Soviet Union to maintain the firebreak and avoid nuclear war. Barry Watts, however, observed that the strategic environment suggests the nuclear-conventional firebreak is shrinking and that "the taboo against nuclear use is being threatened" by the prospect of limited nuclear war.[25] The current U.S. nuclear force was built to deter the Soviet Union from waging total nuclear war against the United States. In the uncertain world of the second nuclear age, the United States must also be prepared to deter a wide range of nuclear opponents across a variety of circumstances.

Thomas Mahnken evaluated a number of plausible limited nuclear conflict scenarios such as demonstration attacks or nuclear use to prevent conventional defeat.[26] These scenarios are useful for considering what actions the United States might need to deter in the future. Mahnken's key insight is that in each scenario, an adversary uses a relatively small amount of nuclear force in a limited manner to accomplish limited objectives. The plausibility of these scenarios lies in the perception of the adversary, who believes nuclear weapons are useful and that the United States lacks a credible deterrent against limited use due to the structure of the current arsenal, which emphasizes high-yield weapons delivered via ballistic

President Ford and Soviet General Secretary Leonid Brezhnev sign Joint Communiqué following talks on limitation of strategic offensive arms in Vladivostok, November 24, 1974 (Gerald R. Ford Library/David Hume Kennerly)

missiles. Bruce Bennett, analyzing possible U.S. nuclear responses to limited-use scenarios, observed that the United States would seek to minimize civilian casualties and thus use only a few weapons, noting that the current nuclear force does not provide the limited options a U.S. President might want and "thereby may be inadequate to deter adversary nuclear weapon threats."[27]

In recent years, numerous studies and reports have examined the optimal shape of the nuclear triad.[28] By and large, these have focused on the structure of the triad—the specific mix of bomber aircraft, submarine-launched ballistic missiles (SLBMs), and land-based intercontinental ballistic missiles (ICBMs)—or on the quantity of weapons required for deterrence. The contribution of a triad of delivery systems to strategic stability is not being disputed.[29] However, perhaps more important to deterrence in the second nuclear age than the means used to deliver a nuclear weapon is the type of weapon being delivered and the effects that weapon will produce.

The United States maintains nuclear weapons "to create the conditions in which they are never used."[30] To create such conditions, the United States must be able to brandish a credible threat such that an adversary concludes the cost of limited nuclear use outweighs any possible benefit. The prospect of limited nuclear war highlights the need to be able to threaten a flexible, limited counterforce nuclear response that minimizes civilian casualties and avoids third-party escalation, such as overflying Russia on the way to a target.[31] This is not a new revelation. The 2009 Congressional Commission on the Strategic Posture of the United States, for example, emphasized the need for a spectrum of flexible force employment options, as did the 2011 Nuclear Futures Project, which concluded that the United States needed the ability to rapidly deliver nuclear weapons with a range of yield options to "achieve military effects and political objectives without causing extensive collateral damage."[32] Likewise, Lieber and Press concluded in 2009 that the United States needed high-accuracy, low-yield nuclear weapons to give "leaders options they can stomach employing in these high-risk crises."[33]

Required Capabilities

In view of the types of limited nuclear scenarios that seem likely in the second nuclear age, the most significant gap in the current U.S. nuclear force structure is a lack of nuclear capabilities useful for controlling escalation while minimizing collateral damage. A number of authors have concluded that low-yield nuclear weapons and electromagnetic pulse (EMP) weapons are particularly useful in many potential limited nuclear scenarios.[34] It is worth noting that

these capabilities have, in the past, been included in the U.S. nuclear force.

In his 1957 work on limited nuclear war, Robert Osgood argued that deterrence credibility "requires that the means of deterrence be proportional to the objectives at stake."[35] Unfortunately, the bulk of the currently deployed U.S. nuclear deterrent consists of ballistic-missile weapons with yields in the hundreds of kilotons.[36] In a limited nuclear war, these weapons lack proportionality and thus are not useful in most scenarios, calling into question U.S. deterrence credibility. In a limited nuclear war, the lack of U.S. means proportional to the limited objectives at stake means the President will be faced with only two options, both unacceptable: either acquiesce or escalate to general nuclear war, in effect committing mass murder by inducing significant collateral damage. The lack of credible escalatory options short of general nuclear war means nuclear opponents may calculate that the United States is unlikely to respond, thus increasing the adversary's perceived value of nuclear escalation. In addition to continuing to modernize the existing triad of delivery systems, the United States must preserve credibility for the second nuclear age by investing in new low-yield and EMP nuclear capabilities and the means to accurately deliver these capabilities.

Conventional Weapons as Substitute?

Those in favor of eliminating the U.S. nuclear deterrent often argue that its conventional weapons are able to provide a sufficient deterrent against nuclear attack on the United States. The Global Zero Nuclear Policy Commission report, for example, stated that "strong conventional forces and missile defenses may offer a far superior option for deterring and defeating a regional aggressor" and "precision-guided conventional munitions hold at risk nearly the entire spectrum of potential targets, and they are useable."[37] When evaluated against the stark realities of the strategic environment, however, these arguments do not stand up. As illustrated earlier, a number of nuclear powers see utility in acquiring nuclear weapons precisely to counter the conventional superiority of countries such as the United States. In a limited regional nuclear scenario, it might be possible for a U.S. President to absorb a limited nuclear strike against the United States and respond only with conventional force. It is prudent to ask, though, what the impact of such a move on existing deterrence regimes would be.

The first effect of a U.S. failure to retaliate in kind would be for all other nuclear parties to question the long-term credibility of U.S. nuclear deterrence. Any nation, particularly a nuclear-armed one, seeking to attack the United States might entertain a theory of victory in which the United States did not respond. Such thinking could lead to crisis instability and risk further escalation. Thomas Schelling asserted that a country's reputation for action, which he called "face," "is one of the few things worth fighting over" because it "preserve[s] one's commitments to action in other parts of the world and at later times" and hence maintains credibility.[38]

A second grave effect of failing to retaliate in kind to a nuclear attack would be a serious erosion of the concept of extended deterrence and, with it, the nonproliferation regime. Not only would future adversaries view U.S. deterrence as not credible, but so too might our allies, who rely upon the extended deterrence provided by the U.S. nuclear umbrella.[39] After a 2013 North Korean nuclear test, polls showed 66 percent of the South Korean public favored developing a domestic nuclear weapons program.[40] That number would likely be much higher if, as Schelling warned, the United States lost face in a limited nuclear scenario by not living up to its reputation for action.

While it remains desirable to eliminate U.S. dependence on nuclear weapons, the realities of the second nuclear age and the emerging strategic environment suggest this is not likely to happen soon. The knowledge to develop nuclear weapons cannot be unlearned. As Thomas Reed and Danny Stillman have observed, the proverbial train has left the station, and the "Nuclear Express now hurtles into a new century with a boxcar of nuclear technology."[41] Looking ahead to 2040, the United States can expect to still be competing in a multiplayer nuclear game in which there are more nuclear actors, possibly including both state and nonstate actors, and characterized by imbalanced political stakes and subject to the influence of dangerous catalytic escalations. It is prudent to invest now in the capabilities that may contribute to deterrence in the uncertain world ahead so that the United States is ready when the Nuclear Express once again pulls into the station.

Recommendations

High-Accuracy, Low-Yield Weapons. A number of limited nuclear use scenarios illustrate the utility of low-yield weapons to control escalation while limiting collateral damage.[42] Nuclear opponents, for example, may use low-yield weapons in demonstration attacks or selective nuclear attacks or to prevent a conventional defeat, believing the use of relatively small weapons may avoid further escalation due to a perceived lack of credible U.S. response options. Other nations, most notably Russia, find low-yield weapons attractive and are pursuing the design of sub-kiloton-class warheads for battlefield use.[43] To fill the low-yield credibility gap, the United States should pursue a two-pronged approach. First, the United States should evaluate options for leveraging existing stockpile weapons designs to field low-yield capabilities in the near term, and second, the United States should develop a new low-yield weapon coupled with a high-accuracy delivery mechanism suitable for minimizing collateral damage.

The B61-12 nuclear bomb, now under development, offers one near-term opportunity to field the recommended capability. The B61-12 program encompasses both a life-extension program to replace aging components and extend the life of the B61 bomb family, as well as a guided tail kit assembly to significantly improve the accuracy of the weapon.[44] By improving accuracy with a guided tail kit, a first for a nuclear weapon, the B61-12

General Dempsey testifies on Iran nuclear deal before Senate Armed Services Committee, July 29, 2015 (DOD/Glenn Fawcett)

is able to hold at risk the same targets as a much larger weapon.[45] The United States does not publicly disclose nuclear weapons yields. It is therefore not possible to know if the B61-12 will provide the required low-yield capability, though the technology developed for it significantly reduces the risk of fielding the needed capability. Paul Robinson, a former director of Sandia National Laboratories, has suggested using dummy secondary stages in existing weapons such as the B61 to produce yields in the low-kiloton range. By replacing the secondary stage with an inert dummy, the only yield produced would be from the fission-only primary stage.[46] The United States should continue the B61-12 program, but should consider technical options to field an accurate variant with very low yield.

The next opportunity to field a low-yield weapon in the mid-term is to design such a feature into the warhead for the long-range standoff weapon (LRSO), which is a cruise missile being designed to replace the circa 1980s air-launched cruise missile (ALCM) and is scheduled for fielding in 2027.[47] The U.S. Nuclear Weapons Council recently selected the W80-1 warhead, currently deployed on the ALCM, as the warhead for the LRSO.[48] Due to its age, the W80-1 warhead will need a life-extension program, designated W80-4, before it can be placed in service on the LRSO.[49] This life-extension program, just now entering the design phase, provides an opportunity to modify the W80-4 design to include a low-yield variant for use on the LRSO missile.

The recommendation to field low-yield variants of existing weapons could be coupled with declaratory policy stating that the United States would employ low-yield weapons only in limited-use scenarios, providing a stepping-stone to credible nuclear deterrence for the second nuclear age. These actions are not, however, by themselves sufficient. As described earlier, developments in the second nuclear age show a worrying trend toward the fielding of "highly usable" nuclear weapons that may significantly alter the firebreak between conventional and nuclear weapons. To avoid a situation where adversary decision calculus favors the early use of such weapons, the United States should pursue the design of new very-low-yield weapons coupled to highly accurate delivery systems. Similar weapons once existed in the U.S. arsenal, and, given sufficient political will, there are no technical challenges preventing their re-introduction.

EMP Weapons. In addition to low-yield nuclear weapons, a number of limited-use scenarios show weapons designed to produce electromagnetic pulse effects may be useful. An EMP is an extremely energetic radio wave that can be generated naturally by the interaction of a powerful solar flare with the Earth's geomagnetic field or artificially through nuclear or nonnuclear means.[50] The energy from an EMP interacts with electronic equipment, causing a range of effects from temporary upset to permanent damage, but causing no biological harm to humans or other organisms.[51]

Nearly all nuclear explosions produce an EMP, the characteristics of which vary according to the altitude of the explosion (also known as the height of burst).[52] A high-altitude EMP occurs when a nuclear weapon is detonated at an altitude of 30 kilometers or more, and in such a burst the EMP will affect a large area.[53] It is estimated that a multi-megaton nuclear EMP weapon detonated over the center of North America would cause severe disruption and damage from coast to coast and, according to Dr. Peter Pry, could possibly "blackout the national electric grid for months or years and collapse all the other critical infrastructures."[54]

Conducting a catastrophic EMP attack, such as the one just described, against the United States would require significant capability—the attacker would need a multi-megaton weapon and space launch capability to deliver the weapon over the United States at high altitude.[55] There is some evidence North Korea may have conducted a practice test of such a capability in April 2013 when North Korea's KSM-3 satellite passed over the eastern seaboard of the United States at the optimal altitude for an EMP attack on the East Coast electrical grid.[56]

In many scenarios, an EMP attack, having the potential to be as catastrophic as a large-scale nuclear strike, will likely be subject to the nuclear-conventional firebreak—an adversary might be reluctant to cross the firebreak and escalate to nuclear war. However, for an adversary with limited nuclear capability, an EMP attack may be seen as a way to maximize the military utility of a small arsenal. Such an adversary may be more motivated to conduct an EMP attack, which might result in no direct casualties, if it believed the United States would not respond with a

nuclear attack that could potentially kill thousands or even millions of people.[57]

It is also possible to create a smaller EMP by adjusting the detonation altitude and yield of the weapon.[58] Such a weapon capable of generating effects over a few hundred square kilometers would have much more military utility in a limited-use scenario and, like low-yield nuclear weapons, would likely shrink the firebreak between conventional and nuclear use. There is evidence that China, for example, already views EMP weapons as a means to achieve information dominance in a regional "high-tech local war." In their book *The Science of Military Strategy*, Chinese generals Peng Guangqian and Yao Youzhi write that "nuclear energy . . . will be employed to seek information dominance. For instance, the electromagnetic pulse weapon still in laboratory stage is a kind of nuclear weapon. It is possible for nuclear weapons to move from deterrence into warfighting."[59]

In a nuclear escalation scenario, the United States might also consider the use of a limited EMP weapon as a sort of nuclear halfway house to control escalation by signaling resolve and demonstrating use of a nuclear weapon without direct loss of life. Another scenario in which an EMP capability might be useful is to control escalation horizontally in a scenario in which an adversary seeks to attack U.S. space capabilities.[60] For example, if an adversary who was much less reliant on space than the United States threatened U.S. space systems, horizontal escalation by EMP attack might be more effective than a response-in-kind against the adversary's space systems.

In the heavily interconnected digital world of the 21st century, nuclear EMP weapons have the potential to create catastrophic effects both on the battlefield and against civilian infrastructure. Furthermore, these weapons are not difficult to produce for a state possessing both nuclear weapons and ballistic missile or space launch capability and, in a crisis, may be destabilizing as a limited nuclear power seeks to maximize utility of its arsenal. Conversely, EMP weapons with regional effects might also be useful to restore deterrence and control escalation if they were used to answer a limited nuclear strike or the use of an EMP weapon. The United States should field a regional nuclear EMP capability to bolster its deterrent credibility in scenarios in which adversaries may consider an EMP or limited nuclear attack.

The United States can likely develop an EMP weapon by modifying an existing warhead, and it may even be able to use a current ballistic missile warhead, launched on an SLBM or ICBM, set to detonate at the correct altitude. Utilizing ICBMs to deliver an EMP weapon is problematic, though, as the missile would in almost all target scenarios overfly Russia, and in many cases China, posing a serious escalation risk as those nations might think they are under attack.[61] SLBMs launched from ballistic missile submarines (SSBNs) are also problematic, though less so, because of overflight concerns as the SSBN patrol areas are optimized for attacks against Russia and China.[62] One possible solution is to mate an existing warhead to a new delivery system that avoids overflight concerns. An air-launched missile, for example, would allow an EMP weapon to be forward deployed and launched toward the target while avoiding most overflight issues. The U.S. Air Force developed and tested an antisatellite missile, the ASM-135, in the 1980s that was capable of reaching the required altitude for EMP generation when launched from an F-15 aircraft.[63] Another option is to modify a commercial space launch system such as Orbital's Pegasus air-launched rocket.[64] Given the political will to field an EMP weapon, there appear to be feasible technical delivery options.

Long-Range Penetrating Bomber. The triad of nuclear delivery methods—bomber aircraft, land-based ICBMs, and sea-based SLBMs—is likely to be useful to deterrence in the second nuclear age.[65] The weapons capabilities recommended in this article can likely be adapted to be delivered via any leg of the nuclear triad, though this may not be desirable. As described, ICBMs and SLBMs are problematic for a number of limited nuclear scenarios. Employing the recommended nuclear capabilities on bomber aircraft, however, eliminates most of the concerns with ICBMs and SLBMs, as bombers can avoid most overflight issues.

Bomber aircraft possess a number of other useful attributes for limited nuclear war. A 2013 RAND study examined contributions of the triad legs to crisis stability by evaluating 48 crises, concluding that long-range penetrating bombers were key contributors to crisis stability.[66] Bomber aircraft also offer flexibility; they can be recalled as well as retargeted in-flight and are also useful for signaling resolve to the adversary. For example, in response to North Korean provocations, the United States sent B-2 bombers to overfly South Korea in March 2013 in a demonstration of capability and resolve.[67] Low-yield nuclear weapons are well suited for delivery by bombers, as weapons with similar capabilities, such as the B61 bomb, already exist. To employ an EMP weapon on bomber aircraft requires development of a new air-launched missile to reach the requisite detonation altitude, although the technology to build such a missile already exists.[68]

Bomber aircraft are likely to be particularly useful in the limited nuclear wars of the future, and the Air Force should continue developing a nuclear-capable penetrating bomber. The Air Force's next-generation bomber program should be fully funded and remain a top priority.[69] The Service should also begin studying solutions for an aircraft-delivered EMP weapon compatible with the new bomber and should seek to accelerate development of the LRSO cruise missile while ensuring it is compatible with future low-yield nuclear weapons. Critics will argue that the combination of a long-range bomber and a capable, accurate nuclear cruise missile coupled with a low-yield warhead is dangerous because it offers a nuclear capability that is actually usable in a nuclear conflict. It is precisely because such weapons are usable that they offer a potent deterrent to nuclear actors who might consider limited nuclear war.

Other Considerations. In addition to pursuing highly accurate nuclear weapons with low-yield and EMP effects and a new bomber and cruise missile to employ

these effects, there are a number of other considerations important to maintaining a credible nuclear deterrent in the second nuclear age. First and foremost is a reinvigoration of strategic thought about nuclear weapons; there has been a dearth of thinking in the United States about how to actually use nuclear weapons should deterrence fail. The world is entering an age where the unthinkable may actually happen. U.S. policymakers and military leaders need to consider how to employ nuclear weapons to control escalation and restore deterrence in limited nuclear war. A reinvigoration of strategic thought about nuclear weapons must also be coupled with a robust nuclear exercise regime so these thoughts can be tested and practiced.[70] Second, the United States will need to improve intelligence gathering on adversary nuclear programs as well as improve the ability to attribute a nuclear attack.[71] In the intertwined security trilemmas of the second nuclear age, it may not be immediately obvious who initiated a limited nuclear strike, and thus attribution becomes more important than it was during the Cold War. Third, the United States should eliminate the dichotomy in the U.S. nuclear lexicon between *strategic* and *tactical* nuclear weapons. This distinction will not make sense in the uncertain world of the future where some actors may wield a range of nuclear capabilities for both tactical and strategic effect.

The grim logic of deterrence did not disappear with the end of the Cold War. Colin Gray observed in 1979 that "one of the essential tasks of the American defense community is to help ensure that in moments of acute crisis the Soviet general staff cannot brief the Politburo with a plausible theory of military victory."[72] Though the adversary may be different, this task will be no less essential in the uncertain world of 2040, where there will still be many nuclear-armed actors, perhaps more than there are today, some of whom may desire to inflict harm upon the United States. To ensure no potential adversary ever contemplates a theory of victory for limited nuclear war, the United States must maintain an effective deterrent by investing in flexible nuclear capabilities such as low-yield and EMP weapons and a long-range penetrating bomber and cruise missile to accurately deliver these weapons. Choices made today will impact the nuclear force for decades to come. By making the choice to invest in the nuclear capabilities most useful for deterring limited nuclear war, the United States can improve the odds that another 70 years pass without a nuclear weapon being detonated in anger. **JFQ**

Notes

[1] George P. Shultz et al., "A World Free of Nuclear Weapons," *Wall Street Journal*, January 4, 2007; James E. Cartwright, chair, *Modernizing U.S. Nuclear Strategy, Force Structure, and Posture*, Global Zero U.S. Nuclear Policy Commission Report (Washington, DC: Global Zero, May 2012).

[2] Jon B. Wolfsthal, Jeffrey Lewis, and Marc Quint, *The Trillion Dollar Nuclear Triad* (Monterey, CA: James Martin Center for Nonproliferation Studies, January 2014), 4.

[3] Keir A. Lieber and Daryl G. Press, "The Nukes We Need," *Foreign Affairs* 88, no. 6. (November–December 2009), 40.

[4] Thérèse Delpech, *Nuclear Deterrence in the 21st Century: Lessons from the Cold War for a New Era of Strategic Piracy* (Santa Monica, CA: RAND, 2012), 5.

[5] Paul J. Bracken, *The Second Nuclear Age: Strategy, Danger, and the New Power Politics* (New York: Henry Holt and Co., 2012), 96.

[6] Pavel Felgenhauer, "Putin Declares His Defense Agenda for the Next Decade," *Eurasia Daily Monitor* 9, no. 38 (February 2012).

[7] Bracken, 33.

[8] Robert M. Gates, address at the United States Military Academy, West Point, NY, February 25, 2011.

[9] Bracken, 106.

[10] Stephen M. Younger, *The Bomb: A New History* (New York: Ecco Press, 2009), 69–97.

[11] Gregory D. Koblentz, *Strategic Stability in the Second Nuclear Age*, Council Special Report No. 71 (New York: Council on Foreign Relations, 2014), 20.

[12] Delpech, 6.

[13] Duncan Brown and Thomas G. Mahnken, *Nuclear Futures Project* (Laurel, MD: The Johns Hopkins University Applied Physics Laborator, February 2011), 8.

[14] Ibid.

[15] Ibid.

[16] Lieber and Press, 40.

[17] Ibid.

[18] Bracken, 118.

[19] Worldwide, there are 435 nuclear reactors in operation, with another 72 under construction. Nuclear Energy Institute, "World Statistics," available at <www.nei.org/KnowledgeCenter/Nuclear-Statistics/World-Statistics>.

[20] Emma Lacey-Bordeaux, "Declassified Report: Two Nuclear Bombs Nearly Detonated in North Carolina," *CNN.com*, June 12, 2014, available at <www.cnn.com/2014/06/12/us/north-carolina-nuclear-bomb-drop/index.html>.

[21] Nuclear Watch New Mexico, "Oldest U.S. Nuclear Weapons in Planned Stockpile Are Seven Decades Younger than Expected Lifetime," *NukeWatch.org*, available at <www.nukewatch.org/facts/nwd/WeaponsAge.pdf>.

[22] David Albright, "Securing Pakistan's Nuclear Weapons Complex," paper presented at 42nd Strategy for Peace Conference, Warrenton, VA, October 25–27, 2001, available at <www.isis-online.org/publications/terrorism/stanleypaper.html>.

[23] Jeffrey A. Larsen, "Limited War and the Advent of Nuclear Weapons," in *On Limited Nuclear War in the 21st Century*, ed. Jeffrey A. Larsen and Kerry M. Kartchner (Stanford: Stanford University Press, 2014), 6.

[24] Herman Kahn, *Thinking About the Unthinkable in the 1980s* (New York: Simon and Schuster, 1984), 29.

[25] Barry D. Watts, *Nuclear-Conventional Firebreaks and the Nuclear Taboo* (Washington, DC: Center for Strategic and Budgetary Assessments, 2013), 72.

[26] Thomas G. Mahnken, "Future Scenarios of Nuclear Conflict," in *On Limited Nuclear War in the 21st Century*, 129–143.

[27] Bruce W. Bennett, "On U.S. Preparedness for Limited Nuclear War," in *On Limited Nuclear War in the 21st Century*, 211–212.

[28] For example, see Dana J. Johnson, Christopher J. Bowie, and Robert P. Haffa, *Triad, Dyad, Monad*, Mitchell Paper 5 (Washington, DC: Mitchell Institute for Airpower Studies, 2009); Evan B. Montgomery, *The Future of America's Strategic Deterrent* (Washington, DC: Center for Strategic and Budgetary Assessments, 2013); Marc A. Peterson, "The New Triad," Research Report (Maxwell AFB, AL: Air War College, 2011); Michael A. Samuel II, "Rebalancing the Nuclear Weapons Triad," Research Report (Maxwell AFB, AL: Air War College, 2011); Michèle A. Flournoy and Clark A. Murdock, *Revitalizing the U.S. Nuclear Deterrent* (Washington, DC: Center for Strategic and International Studies, 2002).

[29] For a thorough analysis of the current triad's suitability to deter in Mahnken's possible future scenarios, see Bennett, 211–243.

[30] William J. Perry and James R. Schlesinger, *America's Strategic Posture: The Final Report of the Congressional Commission on the Strategic Posture of the United States* (Washington, DC: United States Institute of Peace Press, 2009), 20.

[31] Bennett, 229–230.

[32] Perry and Schlesinger, 23; Brown and Mahnken, 17.

[33] Lieber and Press, 51.

[34] Bennett, 211–241; Brown and Mahnken, 17–24; Lieber and Press, 39–51. *Yield* refers to the energy released during a nuclear explosion. It is generally measured in tons, kilotons, or megatons of TNT (trinitrotoluene) equivalent. Younger, 73–74.

[35] Quoted in Larsen, "Limited War and the Advent of Nuclear Weapons," 12.

[36] See table 1 in Hans M. Kristensen and Robert S. Norris, "U.S. Nuclear Forces, 2014," *Bulletin of the Atomic Scientists* 70, no. 1 (January 6, 2014), 86.

[37] Cartwright, 2.

[38] Thomas C. Schelling, *Arms and Influence: With a New Preface and Afterword* (New Haven: Yale University Press, 2008), 124.

[39] George W. Quester, "The End of the Nuclear Taboo," in *On Limited Nuclear War in the 21st Century*, 183; Robert Windrem, "Japan has Nuclear 'Bomb in the Basement,' and China Isn't Happy," NBC News, March 11, 2014, available at <www.nbcnews.com/storyline/fukushima-anniversary/japan-has-nuclear-bomb-basement-china-isnt-happy-n48976>.

[40] Kim Jiyoon and Karl Friedhoff, *The Fallout: South Korean Public Opinion Following North Korea's Third Nuclear Test*, Issue Brief No. 46 (Seoul: The Asan Institute for Policy Studies, February 24, 2013), available at <en.asaninst.org/contents/issue-brief-no-46-the-fallout-south-korean-public-opinion-following-north-koreas-third-nuclear-test/>.

[41] Thomas C. Reed and Danny B. Stillman, *The Nuclear Express: A Political History of the Bomb and Its Proliferation* (Minneapolis: Zenith Press, 2009), 319.

[42] Bennett, 211–241.

[43] James L. Denton, "The Third Nuclear Age: How I Learned to Start Worrying About the Clean Bomb," Research Report (Maxwell AFB, AL: Air War College, 2013), 7; Central Intelligence Agency, *Intelligence Memorandum: Evidence of Russian Development of new Sub-Kiloton Warheads* (Washington, DC: Central Intelligence Agency, August 30, 2000), 3. Document is now declassified.

[44] Hans M. Kristensen, *Non-Strategic Nuclear Weapons*, Special Report No. 3 (Washington, DC: Federation of American Scientists, May 2012), 23–24.

[45] Hans M. Kristensen and Robert S. Norris, "The B61 Family of Nuclear Bombs," *Bulletin of the Atomic Scientists* 70, no. 3 (April 22, 2014), 83.

[46] C. Paul Robinson, "A White Paper: Pursuing a New Nuclear Weapons Policy for the 21st Century," Sandia National Laboratories, March 22, 2001, available at <www.sandia.gov/media/whitepaper/2001-04-Robinson.htm>. Most modern nuclear weapons are based on a two-stage design. The first stage—also called the primary—uses high explosives to implode a plutonium "pit" to produce a fission reaction. The resultant energy implodes the second stage—or secondary—that actually produces most of the weapon's yield. See also Younger, 23–24, 69–74.

[47] Hans M. Kristensen, "W80-1 Warhead Selected for New Nuclear Cruise Missile," Federation of American Scientists, October 10, 2014, available at <http://fas.org/blogs/security/2014/10/w80-1_lrso/>; Gabe Starosta, "Long-Range Standoff Missile Development Pushed Back by Three Years," *InsideDefense.com*, March 5, 2014, available at <http://insidedefense.com/201403052463350/Inside-Defense-General/Public-Articles/long-range-standoff-missile-development-pushed-back-by-three-years/menu-id-926.html>.

[48] Kristensen, "W80-1 Warhead."

[49] Ibid.

[50] Peter V. Pry, "Electromagnetic Pulse: Threat to Critical Infrastructure," Testimony before the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies, House Committee on Homeland Security, 113th Congress, May 8, 2014, 2–6. See also Clay Wilson, *High Altitude Electromagnetic Pulse (HEMP) and High Power Microwave (HPM) Devices: Threat Assessment*, RL32544 (Washington, DC: Congressional Research Service, July 21, 2008), 9; Guoqi Ni, Benqing Gao, and Junwei Lu, "Research on High Power Microwave Weapons," paper presented at Asia-Pacific Microwave Conference, Suzhou, China, December 4–7, 2005.

[51] John P. Geis, *Directed Energy Weapons on the Battlefield: A New Vision for 2025*, Occasional Paper No. 32 (Maxwell AFB, AL: Air University Center for Strategy and Technology, 2003), 9–10; Pry, "Electromagnetic Pulse," 3–6.

[52] Samuel Glasstone and Philip J. Dolan, eds., *The Effects of Nuclear Weapons*, 3rd ed. (Washington, DC: Department of Defense and Energy Research and Development Administration, 1977), 514, 534.

[53] Pry, "Electromagnetic Pulse," 3; Glasstone and Dolan, 537.

[54] Geis, 9; Pry, "Electromagnetic Pulse," 1.

[55] Glasstone and Dolan, 536–537.

[56] Peter V. Pry, "EMP Threat from North Korea, 2013," Family Security Matters, April 27, 2014, available at <www.familysecuritymatters.org/publications/detail/emp-threat-from-north-korea-2013>.

[57] Wilson, 20.

[58] Glasstone and Dolan, 537–538.

[59] Peng Guangqian and Yao Youzhi, ed., *The Science of Military Strategy* (Beijing: Military Science Publishing House, 2005), 404.

[60] For a discussion of horizontal and vertical escalation, see Kerry M. Kartchner and Michael S. Gerson, "Escalation to Limited Nuclear War in the 21st Century," in *On Limited Nuclear War in the 21st Century*, 152.

[61] Bennett, 235.

[62] Ibid., 229–230.

[63] Peter Grier, "The Flying Tomato," *Air Force Magazine*, February 2009, 66.

[64] Orbital ATK, "Pegasus Fact Sheet," available at <http://cms.orbitalatk.com/SiteCollectionDocuments/Orbital%20Data%20Sheets/2B2_Pegasus.pdf>.

[65] For a more complete assessment of the triad's contribution to limited nuclear war, see Bennett, 211–241.

[66] Forrest E. Morgan, *Crisis Stability and Long Range Strike: A Comparative Analysis of Fighters, Bombers, and Missiles* (Santa Monica, CA: RAND, 2013), xx.

[67] Jethro Mullen, "U.S. says it sent B-2 stealth bombers over South Korea," *CNN.com*, March 28, 2013, available at <www.cnn.com/2013/03/28/world/asia/korea-us-b2-flights/index.html>.

[68] An aircraft employing an EMP missile would likely be exposed to the resultant electromagnetic pulse. Electromagnetic hardening therefore should be a design consideration and would likely drive additional requirements for the hardening of the aircraft systems.

[69] Brian Everstine, "USAF Sends Next-Gen Bomber Requirements to Industry, Few Details Made Public," Defense News, July 10, 2014, available at <www.defensenews.com/article/20140710/DEFREG02/140710001/USAF-Sends-Next-Gen-Bomber-Requirements-Industry-Few-Details-Made-Public>.

[70] James Blackwell, "Deterrence at the Operational Level of War," *Strategic Studies Quarterly* 5, no. 2 (Summer 2011), 49.

[71] Bennett, 228–229.

[72] Colin S. Gray, "Nuclear Strategy: The Case for a Theory of Victory," *International Security* 4, no. 1 (Summer 1979), 56.

Philippine special operations forces soldier fast ropes out of SH-60 Sea Hawk during training with U.S. and Australian SOF soldiers at Fort Magsaysay, Philippines, May 2014 (U.S. Marine Corps/Pete Thibodeau)

Strategic Development of Special Warfare in Cyberspace

By Patrick Michael Duggan

Today, small teams of special operators armed with asymmetric cyber-tools, irregular warfare tactics, and mass disinformation can have truly strategic effects.

—General Joseph L. Votel, USA[1]

Why are regional powers such as Iran and Russia better prepared for cyber-enabled special warfare operations than the United States? How do Iran and Russia empower their tactical operators, while the United States masses its cyber-authorities and cyber-capabilities at the strategic level? Why are U.S. policies, authorities, and doctrine for cyber-enabled special operations so immature despite their first announcement over 20 years ago?[2] Although these are serious questions, what is even graver for the Nation is addressing the root question: How does the United

Lieutenant Colonel (P) Patrick Michael Duggan, USA, wrote this essay while attending the U.S. Army War College. It won the Strategic Research Paper category of the 2015 Chairman of the Joint Chiefs of Staff Strategic Essay Competition.

States develop a strategic cyber-enabled special warfare capability?

As far back as 1993, cyber-thinkers John Arquilla and David Ronfeldt in their seminal study *Cyberwar Is Coming!* foreshadowed recent cyber–special operations forces (SOF) actions by Iran and Russia. The prescient notion that "numerous dispersed small groups using the latest communications technologies could act conjointly"[3] to master networks and achieve a decisive advantage over their adversaries has been played out repeatedly. As predicted by Arquilla and Ronfeldt, "We're no longer just hurling mass and energy at our opponents in warfare; now we're using information, and the more you have, the less of the older kind of weapons you need."[4] As senior leaders have recently recognized, groups of special operators armed with asymmetric cyber tools, irregular warfare tactics, and mass disinformation can have strategic effects.[5]

This article argues that Iran and Russia have already successfully employed cyber-enabled special warfare as a strategic tool to accomplish their national objectives. Both countries have integrated cyber-SOF that clearly demonstrate they understand how to leverage this tool's potential within the asymmetric nature of conflict. The countries' asymmetric innovations serve as powerful examples of an irregular pathway for aspiring regional powers to circumvent U.S. military dominance and secure their strategic interests.[6] The diffusion of inexpensive yet sophisticated technology makes it easier for potential adversaries to develop significant capabilities every year. Thus, the time has come for the United States to make a strategic choice to develop cyber-enabled special warfare as an instrument to protect and project its own national interests.

Russia

In February 2013, Russian Chief of the General Staff Valery Gerasimov published an article titled "The Value of Science in Prediction" in the obscure military journal *Military-Industrial Courier*. In the article, General Gerasimov heralded a game-changing new generation of warfare whose strategic value would exceed the "power of force of weapons in their effectiveness."[7] He called for widespread asymmetric actions to nullify enemy advantages through "special-operations forces and internal opposition to create a permanently operating front through the entire territory of the enemy state, as well as informational actions, devices, and means that are constantly being perfected."[8]

In spring 2014, Russia successfully demonstrated its new understanding of how to integrate asymmetric technology into unconventional warfare (UW) operations by supporting paramilitary separatists in eastern Ukraine.[9] Russia dispatched small teams of unmarked *Spetsnaz*, or special forces, across the Ukrainian border to seize government buildings and weapons armories, and then turn them over to pro-Russian separatist militias.[10] Concurrently, Russia disconnected, jammed, and attacked digital, telephone, and cyber communications throughout Ukraine. Russia enlisted virtual "privateers" and bounty hunters to conduct cyber attacks against Ukrainian government information and logistic infrastructure, from Internet servers to railway control systems.[11] Russia bankrolled a "troll army" to wage *deza*, a Russian hacktivist term for disinformation, paying millions for each troll to post 50 pro-Russian comments a day on social media, blogs, and news sites that were critical of Russia's actions.[12] Russia surged epic streams of disinformation, both inside and outside Ukraine, not only to obscure its cyber-enabled UW campaign, but also to create complete political illusions: "Russia doesn't deal in petty disinformation, forgeries, lies, leaks, and cyber-sabotage usually associated with informational warfare. . . . It reinvents reality, creating mass hallucinations that translate into political action."[13]

In response, during a North Atlantic Treaty Organization (NATO) security summit in September 2014, the Supreme Allied Commander Europe, General Phillip Breedlove, USAF, proclaimed that Russia's "hybridized" UW in eastern Ukraine represented "the most amazing information warfare blitzkrieg we have ever seen in the history of information warfare."[14] General Breedlove urged the Alliance to develop new capabilities to counter Russia's mastery of UW, propaganda campaigns, and cyber assaults immediately.[15] NATO and the West were caught off guard by Russia's ability to advance its political objectives using nontraditional means in a manner once "not even considered warfare by the West."[16]

Russia did not use Spetsnaz, information operations (IO), or cyber capabilities in a piecemeal manner to accomplish its objectives. Instead, as General Gerasimov described, "Wars are no longer declared"; they simply happen when SOF armed with advanced technology and mass information create the conditions for conventional forces to achieve strategic objectives "under the guise of peacekeeping and crisis."[17] In other words, choreographed cyber disinformation and cyber attack bought time and space for laptop-carrying Spetsnaz to conduct unconventional warfare "between the states of war and peace."[18] Russia's cyber-enabled UW was a brilliant success, not simply for its cyber-SOF hybridization, but also for successfully invading a signature partner nation of the European Union without sparking any meaningful Western military response.

Iran

In summer 2009, the Iranian regime strangled the Green Movement with the very tools that were supposed to liberate it: information and communication technologies (ICTs). The regime exploited "emancipating" ICTs to target activists, induce fear, and expand military and paramilitary suppression of cyberspace.[19] Shortly after the Green Movement began, the government dispatched its Islamic Revolutionary Guard Corps (IRGC) to break the "counter-revolutionaries." Charged with fighting domestic and foreign threats to the regime, the IRGC mobilized its subordinate Basij cyber units and its notorious clandestine paramilitary wing, the IRGC–Quds Force (IRGC-QF). The IRGC commander, Major General Mohammad Ali Jafari, quickly restruc-

tured and integrated Iran's cyber, paramilitary, and clandestine capabilities into a brutal national tool to terrorize Green Movement dissidents into "inaction and passivity."[20]

The Basij used various devious cyber-intimidation methods against activists, such as sending threatening emails and Internet messages, publishing activists' photos and offering rewards for their capture on government Web sites, infiltrating social media networks, seeding disinformation, sowing leader mistrust, and staging false events to arrest people who showed up.[21] The Basij also institutionalized cyber skills on "blogging, social networking sites, psychological operations, online spying . . . mobile phones and their capabilities, and computer games with the aim of targeted entry in the virtual world."[22] In concert with Basij cyber-targeting activities, the IRGC-QF tracked, imprisoned, tortured, or assassinated regime threats.[23] Iran had set in motion a new symbiotic cycle of misattributable/nonattributable cyber-targeting activities married to old-fashioned brute force. Iran would subsequently strengthen its marriage of counterinsurgency (COIN) and cyber activities in Syria.

Syria

In 2012, Iran dispatched IRGC-QF operators and ICT experts, who had mastered their craft in breaking the Green Movement, to Syria to advise pro–Bashar al-Asad forces.[24] Iran sent "several hundred members of the Revolutionary Guards al Quds force" to Syria armed with domestic COIN expertise, money, arms, and advanced equipment "designed to disrupt communications, the Internet, email, and cell phone communications."[25] Operations in Syria fell under the command of Major General Qasem Soleimani, an infamous figure described by General David Petraeus as "truly evil" and characterized by a senior Central Intelligence Agency officer as the "single most powerful operative in the Middle East."[26]

Under Soleimani's authority, Quds Force operators trained proxy Hizballah and Syrian elements in Iranian camps such as Amir Al-Momenin and integrated themselves into key command and control centers across Syria.[27] According to Dexter Filkins, "To save Assad, Soleimani called on every asset he had built since taking over the Quds Force: Hezbollah fighters, Shiite militiamen from around the Arab world and all the money and materiél he could squeeze out of . . . Assad's own besieged government."[28] Inside Syrian operation centers, Quds Force operators initially provided advice on techniques for suppressing social media and deterring civil disobedience, but soon escalated "with all kinds of kinetic options" to crush the rebellion, just like they had done at home.[29] The Quds Force showed a ruthless understanding of cyber-enabled COIN using "their intelligence networks to train the Syrian army how to fight people without killing; how to use force to cause injury, without being accused of a massacre . . . teaching them how to control Web sites and social media and how to jam television channels."[30]

As with the 2009 attacks on the Green Movement, the Quds Force backed up its cyber-targeting activities with brute force. By this time, however, operatives had learned to distance themselves from the Iranian-trained Syrian, Iraqi, and Hizballah proxies doing the dirty work. As a RAND paper pointed out, "Iran has skillfully employed its own special warfare capabilities as part of a long-term regional strategy, using state and nonstate proxies to advance its regional interests."[31] At the same time, the Syrian Electronic Army (SEA) benefited from Iranian expertise, money, and technology to attack anti-Assad social media and Web sites.[32] The SEA "aggressively engaged in a wide range of online activities to punish perceived opponents and to force the online narrative in favor of the Assad regime."[33] The SEA used distributed denial-of-service attacks, jammed online portals, overloaded networks, and used malware to thwart opponents' messages and actions.[34] Supporting the efforts from Iran, the Basij actively disseminated propaganda, developed increasingly advanced cyberspace capabilities, and professionalized offensive paramilitary hacker field training.[35] It seems that the Basij inundated the Internet with disinformation to obscure Iran's true complicity in Syria and redirect any blame as a Western conspiracy to overthrow Assad.

Iran succeeded against the Green Movement and anti-Assad forces by interweaving ICT efforts to identify key human and information networks with brute force. Beginning with Jafari's reorganization of the IRGC, Iran's cyber-enabled COIN was later perfected with Soleimani's operations in Syria. Throughout both campaigns, the Basij cyber force was a "core state instrument of suppression," honing its techniques to provide cover for Iran's ruthless actions.[36] Iran's cyber-enabled COIN is a stunning success, not only for its cyber-SOF hybridization but also for crushing two separate rebellions and never triggering any meaningful Western military response.

Lessons Learned

There are four primary lessons learned from the actions of Iran and Russia that inform a conceptual framework for aligning cyber capabilities to U.S. special warfare operations.

1. There is a distinction between the offensive cyber tools the IRGC-QF and Spetsnaz employed at the tactical level and those that exist at the strategic level. Iranian and Russian operators targeted tactical-level "circumscribed or closed networks,"[37] such as local communications, social media, and regional Internet and logistic infrastructure, while seemingly keeping their more sophisticated open network tools in reserve.

2. Cyber-enabled special warfare is primarily a proxy-executed endeavor that values minimal source attribution. As described by General Gerasimov, "Long-distance, contactless actions against the enemy are becoming the main means of achieving combat and operational goals."[38] Cyber-enabled SOF generally avoid direct force-on-force engagement and strive to operate in the gray areas between peace and war. As observed in Ukraine and Syria, cyber-enabled violence seeks to retain a modicum of deniability, letting proxies execute the dirty guerrilla tactics of assassination, sabotage, and

Insurgents in Donetsk, Ukraine, May 9, 2014 (Wikipedia/Andrew Butko)

ambush. Russia and Iran retained the strategic flexibility to cut and run should things go awry.

3. ICT exploitation, cyber attack, and IO play significant roles in cyber-enabled irregular campaigns. Properly conducted, traditional special warfare campaigns extend to far more than SOF; "they involve the comprehensive orchestration of broader capabilities to advance policy objectives."[39] Likewise, for these campaigns to work, expertise from other arenas must be integrated and synchronized.

4. Cyber-enabled special warfare could both deter conflict and be applied throughout the spectrum of conflict because it "is well suited to all phases of operation, from shaping the environment through intense warfare through reconstruction."[40] Even though Iran and Russia have operated at the malicious end of the spectrum, cyber-enabled special warfare has a constructive side, too. The proliferation of low-cost information and communication technologies benefits partner nations in the building of security, thereby helping to keep conflicts from breaking out.

Cloud-Powered Foreign Internal Defense

Cloud-powered foreign internal defense (FID) is both a technical computing concept and a metaphor for building partner capacity and trust through virtual means. Although not yet fully defined, FID clouds link cross-disciplined communities together to better understand human, geographic, and virtual arenas, and then act conjointly on targeted overlaps. Technically speaking, FID clouds strengthen partner relationships through federated architectures that share data in real time, enhance automation, and diffuse analytic processes. Clouds have adjustable configurations that can take the shape of private, public, community, and hybrid models, each characterized by different software, platform, and infrastructure architectures.[41] FID clouds power encrypted mobile applications, analytic tools, and pooled data through smart technology in the hands of those involved with building security. Although data are virtually tethered to a cloud, the real value lies in enabling the diffusion of timely information to elements at the tactical level. FID clouds are also a metaphor for persistent and vibrant partnerships because, like the technology, the data never rest and the networks do not go idle. This technology is simply a vehicle to empower a deeper, broader, and more contextual community of understanding for the sociocultural, political, and historical factors that all too frequently fuel strife. Instead of reactive relationships characterized by intermittent FID deployments, which achieve a spotty understanding, FID clouds are metaphors for building a more persistent form of capability, capacity, and trust between partnered nations.

Senior Airman from 21st Special Tactics Squadron conducts air traffic control operations on edge of Geronimo Landing Zone at Fort Polk, Louisiana, during Joint Readiness Training Center rotation 13-09, August 2013 (U.S. Air Force/Parker Gyokeres)

FID clouds lay a virtual foundation for future growth of diverse institutions, centers, and laboratories that can help close the seams between U.S. interagency community interests in a country. From a strategic U.S. Government perspective, FID clouds are a pragmatic "partner-centric approach to design campaigns around a partner's core interests, rather than hoping to transform them in ways that have frequently proved to be ephemeral."[42] FID clouds also provide strategic discretion "when a public relationship of a U.S. partner state is problematic because of the partner state's domestic politics."[43]

FID clouds provide other opportunities as well. The technology and relationships that they foster across communities can be quickly scaled up to respond to sudden emergencies such as humanitarian assistance/disaster relief operations, counter-genocide, or noncombatant evacuation missions. They can save money, time, and manpower by feeding information to decisionmakers when time is of the essence. For partner-building efforts, FID clouds can store information hosted by indigenous non-U.S. social media platforms, enriching social network analysis, sociographic mapping, and behavior and sentiment trend analysis. Most importantly, FID clouds spread trust in a creative and super-empowered way that helps to establish long-lasting influence with allies, coalitions, and other partners.

Counternetwork COIN

Counternetwork COIN (CNCOIN) is a simple concept aimed at leveraging, harnessing, and exploiting social media networks.[44] Designed to break an adversary's asymmetric information advantage, CNCOIN employs nontechnical attacks against people to manipulate their perceptions, behaviors, and actions. It puts a military twist on many of the ill-defined yet ubiquitous anti–social networking tactics practiced across cyberspace. Although these tactics are not clearly defined, this article characterizes them as actions that obscure a perpetrator's true identity while he manipulates social media for reasons other than what is stated. Although social media pose a wide array of opportunities for any anti–social network, ranging from criminally exploitative to benignly misrepresentative, from a military perspective, social media present a rich array of information on ways to influence psychological vulnerabilities and an ideal attack platform from which to do it.

There are three broad functional categories for classifying CNCOIN: operations, intelligence, and IO. There are also several techniques within each functional category that help highlight

its practice rather than define it outright. These techniques are by no means all encompassing or without overlap.

The first CNCOIN category is operations. It includes but is not limited to cyber-pseudo and cyber-herding operations. A *cyber-pseudo operation* is a classic COIN strategy "in which government forces and guerrilla defectors portray themselves as insurgent units" to infiltrate enemy networks and apply advanced tradecraft inside the network to destroy it.[45] A *cyber-herding operation*, on the other hand, "is the action by which an individual, group, or organization drives individuals, groups, or organizations to a desired location within the electronic realm."[46] The beauty of both techniques is that they drive invisible wedges between insurgents and their command and control by exploiting the inherent weaknesses of communication and communication platforms within every network. Cyber-pseudo and cyber-herding operations prey on an enemy network's natural need to maintain a low signature to survive. Both techniques target intermittent and decentralized insurgent leader communications, manipulating or replacing them, which synergistically leads to growing opportunities for the cyber counterinsurgent.[47] The virtual world simply amplifies the environmental factors because personalities are harder to authenticate as real or fictitious.[48] The lack of command and control authentication, communication frequency, and platform availability are key cyber-pseudo and cyber-herding pressure points to manipulate, misinform, or drive targets toward desired outcomes.

The second CNCOIN category is intelligence, which includes but is not limited to crowdsourcing and social networking analysis (SNA) exploitation techniques. *Crowdsourcing* is a practice that taps into large pools of diverse knowledge willingly provided by participants to solve problems with new ideas, services, or observations and quickly broaden the organizer's perspective.[49] *SNA* visually depicts and measures relationships, their density, and the centrality of social links in order to illuminate social network structures.[50] The social network visualizations, or sociograms, provide a unique window to assess, map, and even predict the intensity of relationship events over temporal, geospatial, and relational horizons.[51]

During the September 2013 Zamboanga City crisis in the Philippines, rogue Moro National Liberation Front (MNLF) forces, dissatisfied with the state of national reconciliation, mobilized a force that seized over 200 civilian hostages, raided businesses, and burned buildings throughout the city.[52] During the crisis, both crowdsourcing and SNA exploitation were successful techniques. Although inadvertently at first, Philippine security forces (PSF) used crowdsourcing techniques to encourage Zamboanga residents to spot and report information on rogue MNLF locations throughout the city. The PSF fused crowdsourced information with intelligence analysis, informing both security and humanitarian operations. The PSF used SNA exploitation to assess populace support for rogue MNLF, as well as to counter and discredit rogue MNLF statements on social media by taking down propaganda Web sites that violated social media user agreements. The PSF also used crowdsourced information to cordon pockets of rogue MNLF forces and raid ad hoc command posts. Although less sophisticated than Iran's cyber-enabled COIN, the PSF thwarted rogue MNLF asymmetric advantage by using social media to target key information and leadership nodes, following up with physical force to defeat them.

The third CNCOIN category is IO and includes but is not limited to cyber aggression, sock-puppeting, and astro-turfing techniques. All three techniques exploit social media anonymously to misrepresent, misinform, and manipulate behavior, sentiment, and actions. Advanced by Diane Felmlee, *cyber aggression* "refers to electronic or online behavior intended to harm another person psychologically or damage his or her reputation" by using "email, instant messaging, cell phones, digital messages, chat rooms, as well as social media, video, and gaming Web sites" and is wider in scope than common cyber bullying.[53] Its anonymous application could cause substantial psychological harm and negative consequences as messages are repeatedly viewed by the target or forwarded across social media sites.[54] Its value to CNCOIN is in exploiting sensitive digital information that could shame, demoralize, or traumatize targets into taking psychologically impaired actions. These deliberate cyber aggression operations could undermine the target's credibility, influence, and power to the point of triggering the target to neutralize himself or other insurgents.

The other techniques, *sock-puppeting* and *astro-turfing*, are defined as fictitious online propaganda tools that disseminate contrived views to fabricate a broader illusion of support or nonsupport.[55] Astro-turfing is the same concept as sock-puppeting, but it is more sophisticated and organized and is undertaken on a larger scale than sock-puppeting.[56] Both astro-turfing and sock-puppeting use virtual personas and "bots" to pump false information across cyberspace to incite reaction or mobilize mass action. As witnessed with Russia's army of trolls, botnets, and hired hackers in Ukraine, astro-turfing networks are awash with an arsenal of propaganda, pictures, and videos stoking conflict and obscuring actions on the ground. Counternetwork IO becomes even more effective when combined with deliberate and misleading cyber-targeting activities, such as IRGC activities during the 2009 Green Movement.

Cyber UW Pilot Teams

The third way to advance U.S. cyber-enabled special warfare is the Cyber UW Pilot Team, a capability meant to harness social media networks to shape a physical environment, establish regional mechanisms, and stitch together area complexes prior to executing UW operations. Cyber UW Pilot Teams are purpose-built around the nucleus of a Special Forces Operational Detachment Alpha, augmented with interagency and technical support, whose mission is to digitally prepare an area for UW operations.[57] The teams undertake the same traditional pilot team tasks that previously

were accomplished upon infiltration in the physical domain, but do it through virtual means before they ever put boots on the ground in sensitive, hostile, or denied areas.[58] By operating virtually, Cyber UW Pilot Teams could decrease the time, risk, exposure, and attribution to the U.S. and partnered resistance forces because most of their activities would have been digitally accomplished prior to physical infiltration.[59]

Conceptually, Cyber UW Pilot Teams build human, physical, intelligence, and information infrastructures on social media platforms with cyber tools and advanced techniques. The teams could sharpen their localized language and cultural skills while deepening their understanding of the local human terrain. They could also identify resistance leaders, assess motivations, evaluate resistance capabilities, and assess overall support for U.S. Government objectives while simultaneously evaluating informal hierarchies, psychology, and behavior. In addition, the teams could blend into the white noise of the Internet by tapping into social media networks to "improve U.S. contextual understanding of potential partners and the situation on the ground before the United States commits to a course of action."[60]

Every Cyber UW Pilot Team would have tailored execution authorities and acceptable levels of UW infrastructure development. Once those levels are reached and authorities given, the same team that established the infrastructure virtually would ideally execute its own plan on the ground with the area complex and resistance forces they nurtured online. Cloaked in dual-purpose technology, indigenous equipment, and mobilized networks, these teams would digitally initiate and then physically execute their assigned UW operations from beginning to end.

While there has long been recognition of the strategic role of cyber operations in U.S. national security, this awareness has not fully translated into the development of clear strategic-level thinking and operational capacity. For example, the *Department of Defense Strategy for Operating in Cyberspace* offers few solutions or specifics, but rather reiterates earlier cyber themes in a five-point outline.[61] The lack of well-defined ideas creates a vacuum in cyber strategy that puts the United States in danger of ceding its superior cyber-technological advantage to potential adversaries.[62] In contrast, the asymmetric innovations demonstrated by Iran and Russia present a template for other aspiring regional and global powers to imitate as an irregular pathway to circumventing U.S. military dominance and securing their strategic interests.[63] Moreover, the diffusion of inexpensive yet sophisticated technology increases this potential every year. Iran and Russia have made the American lack of specificity in strategic-level cyberspace documents irrelevant, as the country does not need simply to write about strategy, but must now catch up.

Cyber-enabled special warfare is a strategic-level offensive capability gap that must be filled. Clearly, the United States must aggressively pursue a form of special warfare that integrates cyber operations into tactical-level irregular operations. A recent RAND report on special warfare concluded that "the United States needs to employ a more sophisticated form of *special warfare* to secure its interests . . . and given recent trends in security threats to the United States and its interests, special warfare may often be the most appropriate way of doing so."[64] Cyber-enabled special warfare is the answer in an increasingly interconnected global environment in which physical infrastructure is rapidly being assigned Internet Protocol addresses for assimilation into an "Internet of things." By the year 2020, over 50 billion machine-to-machine devices (compared to 13 billion today) will connect to cyberspace through "the embedding of computers, sensors, and Internet capabilities."[65] Cyber-enabled special warfare bridges the gap between the virtual and the physical by harnessing modern-day information networks and melding them with old-fashioned, face-to-face SOF partner engagement.

Today's global environment impels the United States to adopt cyber-enabled special warfare as a strategic tool of national military strategy. The devastating examples of integrating offensive cyber capabilities into irregular tactics as demonstrated by Iran and Russia pave the way for other U.S. adversaries to soon follow. This article offers the Nation three new options for aligning emerging technology to special warfare missions: cloud-powered FID, counternetwork COIN, and Cyber UW Pilot Team operations. Developing these three concepts to their fullest transcends simply maintaining a U.S. cyber-technology edge; their development projects revolutionary influence across the globe to build critical partnerships and shape issues across the spectrum of conflict. If successfully developed, cyber-enabled special warfare will become a powerful new strategic option for the Nation. **JFQ**

Notes

[1] General Joseph L. Votel, USA, commander of U.S. Special Operations Command, email correspondence with author, December 18, 2014.

[2] Maren Leed, *Offensive Cyber Capabilities at the Operational Level: The Way Ahead* (Washington, DC: Center for Strategic and International Studies and Georgia Tech Research Institute, 2013), 12, available at <http://csis.org/files/publication/130916_Leed_OffensiveCyberCapabilities_Web.pdf>.

[3] John Arquilla and David Ronfeldt, eds., *Networks and Netwars: The Future of Terror, Crime, and Militancy* (Santa Monica, CA: RAND, 2001), 2, available at <www.prgs.edu/content/dam/rand/pubs/monograph_reports/MR1382/MR1382.ch1.pdf>.

[4] Tom Gjelten, "First Strike: U.S. Cyber Warriors Seize the Offensive," *World Affairs* (January–February 2013), 1–2, available at <www.worldaffairsjournal.org/article/first-strike-us-cyber-warriors-seize-offensive>.

[5] Votel.

[6] Dan Madden et al., *Special Warfare: The Missing Middle in U.S. Coercive Options* (Santa Monica, CA: RAND, 2014), 1–4.

[7] Valery Gerasimov, "The Value of Science in Prediction," *Military-Industrial Courier*, February 27–March 5, 2013.

[8] *Towards the Next Defense and Security Review: Part Two—NATO*, HC 358 (London: House of Commons Defense Committee, August 5, 2014), 13.

[9] U.S. Army doctrine defines *unconventional warfare* as "activities conducted to enable a resistance movement or insurgency to coerce, disrupt, or overthrow a government or occupying power by operating through or with

an underground, auxiliary, and guerrilla force in a denied area." See Army Doctrine Reference Publication 3-05, *Special Operations* (Washington, DC: Headquarters Department of the Army, August 31, 2012), 1-5.

[10] Michael Gordon, "Russia Displays a New Military Prowess in Ukraine's East," *New York Times*, April 24, 2014, 2.

[11] Tom Fox-Brewster, "Russian Malware Used by 'Privateer' Hackers Against Ukrainian Government," *The Guardian* (London), September 25, 2014, 1–2.

[12] Misha Japaridze, "Inside Russia's Disinformation Campaign," *DefenseOne.com*, August 12, 2014, available at <www.defenseone.com/technology/2014/08/inside-russias-disinformation-campaign/91286/>.

[13] Peter Pomerantsev, "How Russia Is Revolutionizing Information Warfare," *DefenseOne.com*, September 9, 2014, available at <www.defenseone.com/threats/2014/09/how-russia-revolutionizing-information-warfare/93635/>.

[14] John Vandiver, "SACEUR: Allies Must Prepare for Russia 'Hybrid War,'" *Stars and Stripes*, September 6, 2014, available at <www.stripes.com/news/saceur-allies-must-prepare-for-russia-hybrid-war-1.301464>.

[15] Ibid.

[16] "Cyber Security Pro: Finland Under Hybrid Warfare Attack," *Yle.fi*, September 13, 2014, available at <http://yle.fi/uutiset/cyber_security_pro_finland_under_hybrid_warfare_attack/7470050>.

[17] Robert Coalson, "Top Russian General Lays Bare Putin's Plan for Ukraine," *World Post*, September 2, 2014, available at <www.huffingtonpost.com/robert-coalson/valery-gerasimov-putin-ukraine_b_5748480.html>.

[18] Ibid.

[19] Saeid Golkar, "Liberation or Suppression Technologies? The Internet, the Green Movement and the Regime in Iran," *International Journal of Emerging Technologies and Society* 9, no. 1 (May 2011), 50.

[20] Mark Dubowitz and Matthew Levitt, *Subcommittee on International Human Rights of the Standing Committee on Foreign Affairs and International Development*, Statements, House of Commons Chambre Des Communes Canada, 41st Parliament, 1st sess., May 30, 2013, available at <www.parl.gc.ca/HousePublications/Publication.aspx?Mode=1&DocId=6191680&Language=E>.

[21] Golkar, 62.

[22] Ibid., 63.

[23] Dubowitz and Levitt, 2.

[24] Farnaz Fassihi, Jay Solomon, and Sam Dagher, "Iranians Dial Up Presence in Syria," *Wall Street Journal*, September 16, 2013.

[25] Ephraim Kam, "The Axis of Evil in Action: Iranian Support for Syria," Institute for National Security Studies Insight No. 372 (October 10, 2012), 3, available at <www.inss.org.il/index.aspx?id=4538&articleid=5207>.

[26] Dexter Filkins, "The Shadow Commander," *The New Yorker*, September, 20, 2013, 3.

[27] Fassihi, Solomon, and Dagher.

[28] Filkins, 30.

[29] Dubowitz and Levitt, 6.

[30] "Iran Confirms Sending Troops to Syria, Says Bloodshed Otherwise Would Be Worse," *Al Arabiya*, May 28, 2012.

[31] Madden et al., 2.

[32] Gabi Siboni and Sami Kronenfeld, "Developments in Iranian Cyber Warfare, 2013–2014," Institute for National Security Studies Insight No. 536 (April 3, 2014), 1, available at <www.inss.org.il/index.aspx?id=4538&articleid=6809>.

[33] Max Fisher and Jared Keller, "Syria Digital Counter-Revolutionaries," *The Atlantic*, August 31, 2011, available at <www.theatlantic.com/international/archive/2011/08/syrias-digital-counter-revolutionaries/244382/>.

[34] Ibid.

[35] Gabi Siboni and Sami Kronenfeld, "Iran's Cyber Warfare," Institute for National Security Studies Insight No. 375 (October 15, 2012), 3, available at <www.inss.org.il/index.aspx?id=4538&articleid=5203>.

[36] Dubowitz and Levitt, 6.

[37] Leed, 12.

[38] Coalson, 3.

[39] Madden et al., 1–4.

[40] Ibid., 9.

[41] Department of Defense (DOD) Chief Information Officer, *Cloud Computing Strategy* (Washington, DC: DOD, July 2012), 41, available at <www.defense.gov/news/dodcloud-computingstrategy.pdf>.

[42] Ibid., 3.

[43] Ibid., 4.

[44] Joint Publication 3-24, *Counterinsurgency* (Washington, DC: The Joint Staff, November 22, 2013), I-2, defines *counterinsurgency* as "comprehensive civilian and military efforts taken to defeat an insurgency and to address any core grievances."

[45] Lawrence E. Cline, *Pseudo Operations and Counterinsurgency Lessons from Other Countries* (Carlisle, PA: U.S. Army War College, June 2005), 5, available at <www.strategicstudiesinstitute.army.mil/pdffiles/pub607.pdf>.

[46] David B. Moon, "Cyber-Herding: Exploiting Islamic Extremists," in *2007 JSOU and NDIA SO/LIC Division Essays*, Joint Special Operations University Report 007-5 (Hurlburt Field, FL: JSOU, April 2007), 4, available at <www.dtic.mil/get-tr-doc/pdf?AD=ADA495377>.

[47] Cline, 5.

[48] Moon, 15.

[49] Dragos Negoitescu and Mark Blaydes, "Crowdsourcing: Is NATO Ready?" *Three Swords Magazine*, no. 26 (2014), 2, available at <www.jwc.nato.int/images/stories/threeswords/crowdsourcing.pdf>.

[50] Seth Lucente and Greg Wilson, "Red Line: Social Media and Social Network Analysis for Unconventional Campaign Planning," *Special Warfare* 26, no. 3 (July–September 2013), 21–23, available at <www.dvidshub.net/publication/issues/12346>.

[51] Ibid.

[52] Al Jacinto, "Zambo Propaganda, Drama Plays On," *The Manila Times*, September 28, 2013, available at <www.manilatimes.net/zambo-propaganda-drama-plays-on/40435/>.

[53] Diane Felmlee and Robert Faris, "Toxic Ties: Networks of Friendship, Dating and Cyber Victimization," paper presented at the American Sociological Association Annual Meeting, Hilton, NY, August 9, 2013.

[54] Ibid.

[55] Alex Comninos, "Twitter Revolutions and Cyber Crackdowns: User-Generated Content and Social Networking in the Arab Spring and Beyond," *Academia.edu*, June 2011, 4, available at <http://academia.edu/633706/Twitter_revolutions_and_cyber_crackdowns_User-generated_content_and_socialnetworking_in_the_Arab_spring_and_beyond>.

[56] Ibid., 14.

[57] Patrick Duggan, "UW in Cyberspace: The Cyber UW Pilot Team Concept," *Special Warfare* 27, no. 1 (January–March 2014), 69, available at <http://static.dvidshub.net/media/pubs/pdf_14790.pdf>.

[58] Ibid.

[59] Ibid.

[60] Madden et al., 1–4.

[61] Thomas M. Chen, *An Assessment of the Department of Defense Strategy for Operating in Cyberspace* (Carlisle, PA: U.S. Army War College, 2013), 30.

[62] Ibid., 36–37.

[63] Madden et al., 1–4.

[64] Ibid., 4.

[65] Patrick Tucker, "The CIA Fears the Internet of Things," *DefenseOne.com*, July 24, 2014, available at <www.defenseone.com/technology/2014/07/cia-fears-internet-things/89660/>.

General Dempsey joins Secretary Carter for testimony before U.S. Senate Committee on Armed Services hearing discussing Counter-ISIL strategy, July 2015 (U.S. Army/Sean K. Harp)

Countering Extremist Groups in Cyberspace

By Robert William Schultz

How can the United States develop effective strategic options to counter extremist groups operating in cyberspace? For groups that promote hatred and violence, cyberspace provides a virtual safe haven from which to operate, using Web sites to promote their causes, raise funds, communicate, and grow. The ability to remain elusive has made these groups the true beneficiaries of cyberspace. Using social media outlets, these groups have a global reach for organizing, planning, and conducting operations. They instill loyalty among their followers through near-constant, clear communication. Cyberspace has also enabled extremist groups to adopt decentralized organizational structures with indiscernible command hierarchies, making them difficult to identify and target using conventional military power.[1]

Countering these adversaries poses a significant challenge. With an ever-increasing number of extremist Web sites, U.S. efforts to degrade these online operations have been inadequate, pointing to the need for innovative strategic solutions to counter these threats.[2] However, the same protection cyberspace offers them also makes these extremists susceptible to deception. This article argues that false-flag operations could provide the strategic means to mask a deception that could degrade the bonds of trust among extremists operating in cyberspace and their loyal supporters by undermining the legitimacy of their governing ideology.

Deception Works

Deception is often employed strategically to manipulate an adversary's perceptions to gain a competitive advantage while disguising the basic objectives, intentions, strategies, and capabilities of the deceiver.[3] In cyberspace,

Lieutenant Colonel Robert William Schultz, USA, wrote this essay while a student at the U.S. Army War College. It won the Strategy Article category of the 2015 Chairman of the Joint Chiefs of Staff Strategic Essay Competition.

suitable deception targets could include an organization's ideological infrastructure, legitimacy, and bonds of trust that connect the group with its followers. By targeting these three facets, a deception strategy could directly challenge an extremist group's online existence.

During the 20th century, deception was an essential element of significant military operations. Between 1914 and 1968, over 90 percent of the deceptions conducted in support of military operations were successful.[4] Based on the technology available at the time, these deceptions were executed in the physical domain where actions and messages had to be seen or heard by their intended audience for the deception to achieve its effect. In the virtual reality of cyberspace, however, anyone has the ability to post a message or influence perceptions. In loosely associated groups that are built on rigid ideology, there is space to sow the seeds of dissent by making members look as if they are not conforming to the agreed-upon ideology. Of note, "it is much easier to lead a deception target astray by reinforcing their existing beliefs, thus causing the target to ignore the contrary evidence of one's true intent, than it is to persuade a target to change his or her mind."[5] For this reason, the decision to employ deception must be based on the ability to deceive adversaries into believing something they want to believe as opposed to embracing an entirely new idea.[6] In light of this, the United States should acknowledge that rapidly improving information technologies enhance the ability to initiate unobserved operations and create believable deceptions in cyberspace over a protracted period of time.[7] With these favorable conditions, a means of employing deception could be realized through the use of an age-old operational concept called false-flag operations (FFO).

False-Flag Operations

The term *false flag* originated in naval warfare and describes a ship's attempt to deceive an enemy maritime vessel by hiding or replacing its flag to maneuver closely enough to destroy or capture the enemy's vessel. Though FFOs faded away in the mid-1800s because many states believed they were being carried out without proper oversight or governmental control, FFOs today are more than just a maritime deception tactic. They are holistically defined as secret or disguised operations intended to deceive an adversary into believing that groups or states other than those who planned and implemented the operations are responsible.[8] When employed in cyberspace, FFOs could disguise deceptions in a similar manner. Additionally, where traditional FFOs used a disguise to approach the enemy, in cyberspace the interaction between the deceiver and the deceived is reversed. The deception target must choose to visit the FFO's Web site in the first place for the deception to work.

Furthermore, this concept has long been legally acceptable under the Law of Armed Conflict, which permits the use of disguises prior to engaging in combat, and is also legitimized under Articles 37–39 of the Geneva Conventions: "Ruses of war are not prohibited. Such ruses are acts which are intended to mislead an adversary or to induce him to act recklessly."[9] Since posting Web-based content is far from engaging in combat, the need to eventually reveal attribution of the sponsor remains a question for legal study. Thus, without actual combat, the Web-based FFO concept is more akin to black or covert deceptions in which the sponsor's attribution remains hidden.[10]

How This Would Work

This concept of FFOs in cyberspace is designed around creatively developing Web sites, blogs, and chat rooms that mirror a targeted extremist group's ideology. First, cyber-deceivers would develop FFO Web-based content consistent with the targeted group's narrative in order to attract and co-opt potential extremist followers as readership and membership grew, the content on FFO sites would gradually change. Over time, the narratives would shift subtly to influence the target audience into believing the target group's ideology is either corrupt or so devious that the target audience would see the bond of trust had been broken, thus compelling supporters to terminate association with the extremist group in cyberspace.[11]

As an example, the recent trend of using online radicalization to fill the ranks of the Islamic State of Iraq and the Levant (ISIL) could be countered through the use of FFOs that undermine the bond of trust between ISIL and potential recruits by using false-flag Web sites to highlight the atrocities of the group's ongoing operations, thus delegitimizing the movement. Alienating extremist groups such as ISIL from the international Islamic community through FFOs would not only degrade such organizations in the short term, but could also potentially discredit its online activities over longer periods.

Implications

There are three effects we could expect to see if FFOs were successful in undermining the bonds of trust between targeted online extremist groups and would-be supporters. First, because cyberspace FFOs would target the legitimacy of extremist groups, we would see measurable changes in online activity, including decreases in membership, fundraising, blogs, and chats, and increases in offensive messages posted on FFO Web sites. Second, we would see targeted extremist groups policing or even attacking other like-minded Web sites because they are questioning the veracity of ideology on sites they do not directly manage. Finally, we would expect to see an overall change in the use of cyberspace, as targeted extremist groups and their supporters—even if they detect the FFO—would no longer feel secure operating in the virtual realm.

Mitigating Risk

FFOs normally have a limited shelf life, as targets will eventually become attuned to the presence of active deception.[12] However, in cyberspace, time is on the deceiver's side. Though cyber-based deceptions may take longer to be effective, the vastness and anonymity of cyberspace allow the deceiver to continually adjust messages and techniques with new strings of code. In terms of

Secretary Kerry and U.S. Ambassador to Jordan Alice Wells meet with King Abdullah II of Jordan, Crown Prince Hussein bin Abdullah, and other top advisors in Washington, DC, February 2015 (Department of State)

targeting ideology, cyber-based FFOs seek to achieve an aggregated effect over a series of unceasing efforts. Just as everyday Internet users have grown aware of the variety of hacking tactics, so will extremist groups grow to distrust their own Web sites as their ideological messages appear to deviate from approved narratives. Therefore, FFO compromises should be expected and welcomed in cyberspace; it would be just as advantageous to the deceiver if targeted groups discovered FFO sites and began to doubt their own information assurance measures.[13] Furthermore, cyberspace's ever-growing domain provides the deceiver with an increased area of operation. If compromised, it is a matter of taking the FFO offline, adjusting content, and then placing it elsewhere in the cyber realm. Regardless, common sense dictates that the United States should not ignore a low-cost and relatively safe tool to help achieve its goals.

Extremist groups such as ISIL are making highly effective use of the rapidly emerging cyber technologies that connect the world. Concepts such as false-flag operations could be instrumental in developing solutions to achieve the desired strategic effect of countering these groups in cyberspace. While some defensive cybersecurity tools are effective, more offensive capabilities are needed to counter emerging threats in the 21st century. Cyber-based deceptions such as FFOs offer a cost-effective complement to traditional military force in the fight against extremist groups. When it comes to undermining and marginalizing the legitimacy of a governing ideology in cyberspace, deception through the use of false-flag operations could provide a variety of strategic options from which to choose. In the end, targeted extremist groups would be hard-pressed to determine which of their own Web sites to trust. **JFQ**

Notes

[1] John Arquilla and David Ronfeldt, *Networks and Netwars: The Future of Terror, Crime, and Militancy* (Santa Monica, CA: RAND, 2001), 241.

[2] Gabriel Weimann, *Terror on the Internet: The New Arena, the New Challenges* (Dulles, VA: Potomac Books, 2006), 15.

[3] Richards J. Heuer, Jr., "Strategic Deception and Counterdeception: A Cognitive Process Approach," *International Studies Quarterly* 25, no. 2 (June 1981), 294.

[4] Barton Whaley, *Stratagem: Deception and Surprise in War* (Norwood, MA: Artech House Press, 2007), 82–118.

[5] Richards J. Heuer, Jr., "Cognitive Factors in Deception and Counterdeception," in *Multidisciplinary Perspectives in Military Deception*, ed. Donald C. Daniel et al. (Monterey, CA: Naval Postgraduate School, 1980), 60.

[6] Carolyn Pumphrey and Antulio Echevarria II, eds., *Strategic Deception in Modern Democracies: Ethical, Legal, and Policy Challenges* (Carlisle Barracks, PA: U.S. Army War College, November 2003), 4.

[7] Charles A. Fowler and Robert F. Nesbit, "Tactical Deception in Air-Land Warfare," *Journal of Electronic Defense* (June 1, 1995), available at <www.highbeam.com/doc/1G1-17620824.html>.

[8] Geraint Hughes, *The Military's Role in Counterterrorism: Examples and Implications for Liberal Democracies*, Letort Paper (Carlisle Barracks, PA: U.S. Army War College, May 2011), 105. Mid–19th century states feared pirates were primarily conducting false-flag operations (FFOs), and as a result the practice was discontinued. However, during both world wars, the German navy continued to conduct FFOs globally.

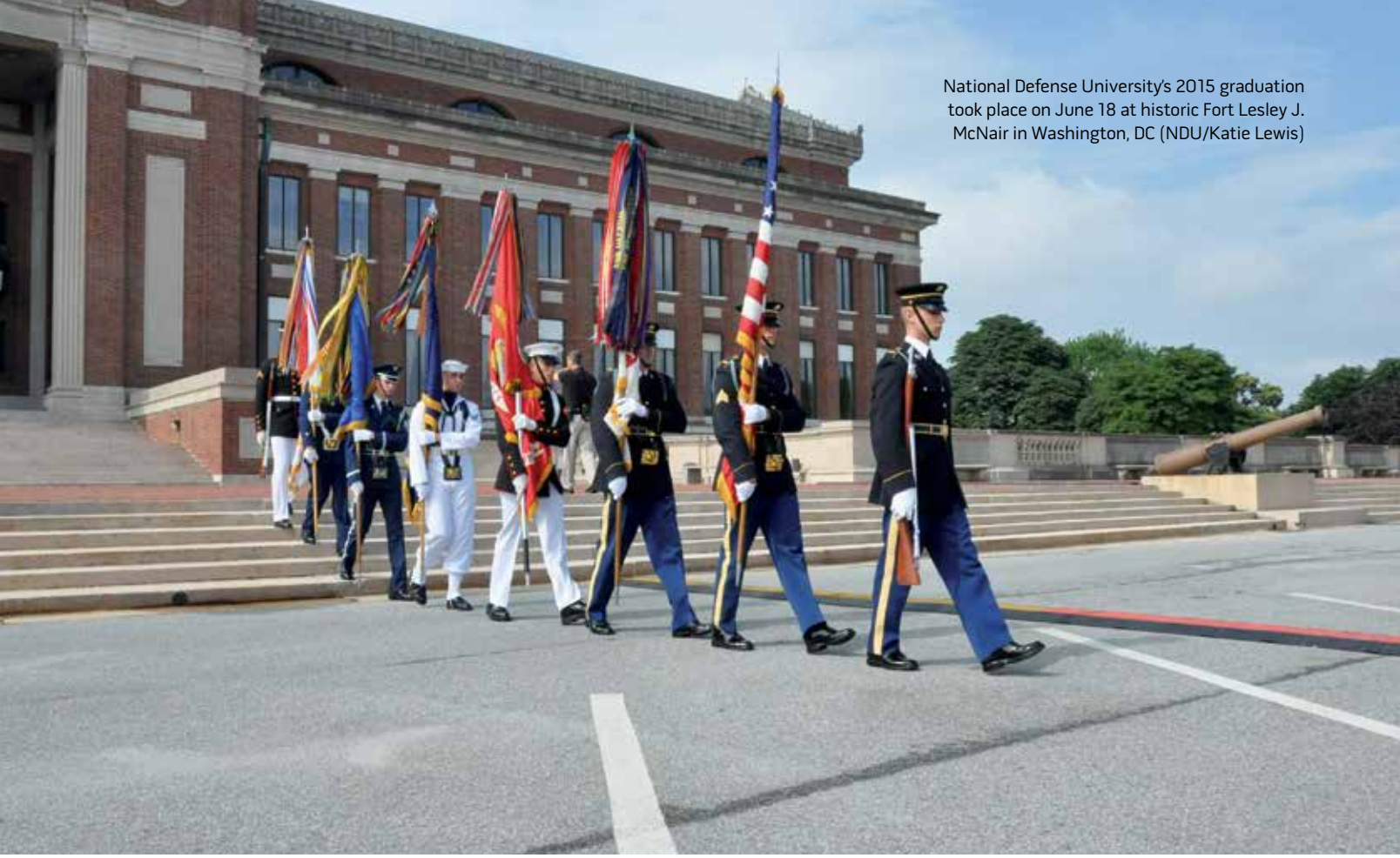
[9] Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977, Art. 37. See also Field Manual 27-10, *Law of Land Warfare* (Washington, DC: Headquarters Department of the Army, July 18, 1956), 23.

[10] Thomas W. Smith, Jr., *Encyclopedia of the Central Intelligence Agency* (New York: Facts on File, 2003), 31.

[11] Mark E. Stout, John R. Schindler, and Jessica M. Huckabey, *The Terrorist Perspectives Project: Strategic and Operational Views of Al Qaida and Associated Movements* (Annapolis, MD: Naval Institute Press, 2008), 122.

[12] James Adams, *The Next World War: Computers Are the Weapons and the Frontline Is Everywhere* (New York: Simon and Schuster, 2001), 286.

[13] Heuer, "Strategic Deception and Counterdeception," 294.



National Defense University's 2015 graduation took place on June 18 at historic Fort Lesley J. McNair in Washington, DC (NDU/Katie Lewis)

Writing, Integrity, and National Security

By Larry D. Miller and Laura A. Wackwitz

Advanced professional military education (PME) affords senior officers the opportunity to acquire solid intellectual footing and enter the strategic dialogue following over 20 years of progressively more responsible leadership. With that opportunity, however, comes a responsibility new to many career officers: engaging in ethical professional scholarship. The zenith of PME is transitional. Selected senior military officers are invited, indeed encouraged, to become "warrior-scholars"—individuals who recognize and understand strategic issues, have the intellectual skills to chart a path forward, and have mastered the professional competencies to make it happen.[1]

The mission is both educational and knowledge generative. Effective execution requires development of critical thinking and writing skills well beyond the norm in military culture. Throughout the military, "officers headed for high rank need to be challenged intellectually and to sharpen their skills in critical, precise, rigorous, and imaginative thinking and writing."[2] At the highest levels, the tasks shift from artfully executing campaigns and missions crafted by others to identifying strategic challenges, rendering assessments, and advocating well-reasoned options to the most senior military and civilian leadership. No longer is the requirement simply to understand what is being done, why, and how to do it; the new goal is to merge professional experience, critical thinking competencies, and acute insights to identify what could or should be done while advancing thoughtful analyses and perceptive recommendations supported by reason and evidence. Most officers arrive at senior Service colleges (SSCs) with considerable experience writing memoranda, operation orders, policy letters, point papers, and the like, but their written documents have been little more than tools for getting the job done effectively and efficiently.[3] Customarily, Army documents

Dr. Larry D. Miller is Professor and Director of Communicative Arts in the Strategic Studies Institute at the U.S. Army War College. Dr. Laura A. Wackwitz is Director of the Institute for Military Writing.

are written at a reading level halfway between that appropriate for a 12th-grade reader and a college graduate.[4] A well-honed mentality and skill set primed almost exclusively for efficient and cooperative execution provide little room and minimal appeal for the time-consuming, heavy intellectual lifting normally associated with knowledge generation.

The transition from writing as a routine day-to-day management tool to writing as the primary vehicle through which to demonstrate subject matter mastery, advance fresh insights,[5] and make reasoned strategic-level arguments is a challenge, to say the least. Though only a few of the best students are able to *fully* rise to the occasion, most learn to reason well and embrace writing as a tool for achieving strategic-level objectives. Some, however, fail to grasp the importance of the mission and fulfill it. The most unfortunate of these turn to plagiarism as a means of satisfying institutional requirements, demonstrating competence with the written word, and completing the degree program. Such is the nature of a normal distribution—some perform exceedingly well, most are successful, and a few fail miserably. But at an SSC, even the plagiarists are accomplished, well-seasoned military professionals, many of whom have held command over thousands, rendered decisions impacting human life, assumed responsibility for multimillion-dollar equipment, and generally devoted their careers to the service of the Nation. What accounts for plagiarism among a select population of respected warriors-scholars? Do writing integrity and personal/professional integrity equate? Yes and no.

As in every profession, a minority of would-be strategic leaders has risen through the ranks through a lifetime of ethically suspect and deceptive behaviors. But what of the otherwise honorable senior officers who resort to plagiarism? In a military milieu, the expectation for original thought, while essential, is counterintuitive for many and difficult for most. Challenging authority, dissecting policy, unraveling doctrine, and critically engaging the ideas and campaigns of world-class strategic thinkers are simply not the sort of activities that most senior officers customarily embrace and readily welcome. Writing integrity, like the ability to write itself, is an acquired skill, not an inborn trait. Thus, PME institutions and others charged with developing senior leaders must revision writing integrity as a competency to be taught, rather than a preloaded, well-embedded, and thoroughly integral component of a leader's character.

Deception in the House

Plagiarism is the antithesis of writing integrity and can carry heavy consequences. Generally recognized as a form of intellectual and academic misconduct, plagiarism entails "the appropriation of another person's ideas, processes, results or words without giving appropriate credit."[6] To plagiarize is to misrepresent—as one's own—the words and ideas of another. International and cultural sensitivity regarding what constitutes plagiarism and how seriously it should be viewed varies a great deal. In Colombia, for example, an author's "moral rights" to his/her intellectual work command legal standing. In one controversial case, the Colombian Supreme Court sentenced Professor Luz Mary Giraldo, an established literary critic, to a 2-year prison term for plagiarizing portions of her student's thesis in a brief article published in a Mexican literary journal.[7] In Germany, Karl-Theodor zu Guttenberg, a popular, promising, and highly effective member of Angela Merkel's cabinet, was pressured to resign as defense minister in 2011 after it became known that he had plagiarized portions of his 2007 doctoral dissertation.[8] More recently, German Education Minister Annette Schavan resigned from Merkel's cabinet following the revelations that her 1980 doctoral dissertation (titled somewhat ironically *Character and Conscience*) was revoked for "systematic and premediated" plagiarism.[9]

In the United States, plagiarism is deemed "a moral and ethical offense" rather than a legal one.[10] Historians and best-selling biographers Doris Kerns Goodwin and the late Stephen Ambrose, while publically embarrassed and apologetic, continue to be held in high esteem despite well-documented evidence of plagiarism in their professional writings.[11] The expectations and consequences are much higher, however, for those charged with protecting the public trust, advancing U.S. interests, and providing for national security. After revelations that U.S. Senator John Walsh secured his U.S. Army War College degree on the merits of a heavily plagiarized document, his degree was rescinded and he was forced to abandon his re-election bid amid widespread controversy.[12]

Cheating, plagiarism, and other forms of academic malfeasance are well documented, widely decried, and increasingly rampant across virtually every intellectual landscape and professional activity. PME institutions are not immune. Instances of plagiarism surface even among the most elite cadres of impressively accomplished military professionals preparing to assume the highest levels of national leadership. Because integrity is fundamental to a professional military ethic, plagiarism within SSCs is especially difficult to reconcile. Senior officers and their civilian counterparts are mature, experienced, well educated, hardworking, and by most counts amply compensated. At the Army War College, for example, all 308 members of the U.S. resident class of 2014 held baccalaureate degrees, and 73 percent had previously earned one or more advanced degrees from accredited graduate schools.[13] Their average age was 45 with 21 years of service. Ninety percent held the rank of lieutenant colonel, colonel, or equivalent, and 28 senior civilians represented a half-dozen Federal agencies. These are not youthful undergraduates who presumably plagiarize due to ignorance, confusion, academic deficiencies, laziness, or pressure to secure a degree to become gainfully employed or attend graduate school. These are seasoned members of the profession of arms who are considered above reproach.

Forms of Plagiarism at the SSCs

Plagiarism among senior leaders is unique in impact, striking at the very heart of democracy. Its form, however,

Historian and author Doris Kearns Goodwin speaks at a conference in Seattle, Washington, October 2006 (Quinn Dombrowski/Flickr)

is unexceptional. Three of the most common varieties of recurrent plagiaristic malfeasance are the weave and duck, heavy import, and patchwriting.

The *weave and duck* involves copying, typically word for word, portions of another's work, usually one or more complete lines of text, and then weaving it as artfully as possible into a larger document. Sometimes a few words are deleted, changed, or repositioned. An endnote frequently accompanies the text though no quotation marks identify the words as belonging to the original author. The plagiarist intends that the reader will presume the author has paraphrased what is actually directly lifted verbiage. If this scheme is noted and brought to the author's attention by higher authority, the typical response is to "duck," to sidestep the observation by acknowledging that the material "was supposed to be in quotes" while offering assurance that the error is but an honest mistake that will be rectified before becoming final. The practice of weaving another's words into a text without proper quotation, however, is seldom rare or happenstance. Should the advisor broach the issue of integrity, the student quickly takes offense, maintains that the advisor has compromised the bond of trust, and expeditiously seeks another mentor.

The *heavy importer* seeks to co-opt acceptably competent work lodged at the periphery of some topically relevant strategic concern. In a heavy import scenario, the plagiarist locates one or more existing documents consistent with a topic and writing task, but usually a little beyond the subject matter expertise/interest of the faculty mentor. The heavy importer then copies not only occasional sentences, but also entire pages and even whole sections. Transitions are offered as needed, and a fresh reference or two may be added in the interest of currency. Manuscripts drawn from library databases or sanctioned depositories such as the Defense Technical Information Center are generally considered "reliable sources of information" for plagiarizing.[14] Another less common practice for heavy importers with multiple language capability is to locate a document published in a language other than English and lift substantial portions, translate it into English, and present the ideas as original with or without mention of the original source.

Patchwriting is a far more frequent practice than is generally recognized at SSCs and in digital cultures across the globe.[15] *Patchwriting* entails "copying from a source text and then deleting some words, altering grammatical structures, or plugging in one-for-one synonym-substitutes."[16] A patchwritten document constitutes a more thoroughly integrated and complex mosaic than the

weave and duck, often involving integration of material from three or more sources. Quotation marks are often interspersed, along with paraphrasing, word changes, and light structural altering of the original—frequently accompanied by a source citation. What is blatantly missing, however, is original thought or substantive development beyond the mere recasting of the ideas and words of others. Somewhat paradoxically, the most facile of patchwriters display sufficient language facility to suggest that the writer could advance something original and worthwhile if he or she so desired. Moreover, in some circles patchwriting is considered a genuine, albeit preliminary, effort by a novice to affiliate with a discourse community, making identification of authorial intent[17] particularly troublesome.[18]

Plagiarism Mitigation at the SSCs

Characteristically a solitary initiative that surfaces somewhat unpredictably and arises where least expected, plagiarism is an accelerating societal and worldwide trend. Extensive debate rages over best practices for its mitigation and whether mitigation is necessary or even possible in a digital world. The challenge within the senior Service colleges is presumably modest, but of unknown magnitude. In educational milieus populated by mature, highly respectable, impressively accomplished, and academically credentialed senior leaders, comprehensive tracking of plagiarism is both inappropriate and difficult.

Although many institutions of higher education have adopted a "gotcha" mentality[19] toward plagiarism tracking, that approach is antithetical to the goals of professional military education and a potential threat to national security. The practice requires students to routinely submit documents to for-profit software companies such as Turnitin. Once submitted, documents are both compared to other documents in the archive and added to the database for future comparisons. The method may seem innocent enough on the surface but is, in fact, far more insidious than first glance suggests. Routinely performing—or asking students to perform—document checks fosters a culture of suspicion antithetical to American values, places senior officers in the role of presumed plagiarist rather than emerging strategic intellectual, and undermines confidence in both the self and the written word.[20] Educational institutions are encouraged to subscribe carte blanche to the services of these companies that neither provide compensation for data collection nor undergo external (for example, PME) review of their practices. The process is a self-reinforcing means of accumulating vast amounts of data without which the software would be useless. Software can only detect plagiarism if the plagiarized artifact is in fact already present in the dataset to which a paper is compared. Moreover, course papers and larger documents submitted become part of a potentially accessible database prior to institutional review. Presumably, classified research would never be submitted. Many unclassified SSC student documents, however, are not appropriate for unlimited distribution: some use restricted materials (for example, for-official-use-only documents, nonattribution speeches), some advance sensitive arguments (wargame scenarios, intervention strategies), and some start as Distribution A documents (approved for unlimited release) but migrate to Distribution B (authorized for approved government institutions) after higher review. Once submitted, however, papers cannot be recalled. The potential risk to national security and U.S. Government interests must outweigh the desire to opt for a quick fix to what is but a symptom of a larger problem: students poorly equipped for the strategic-level thinking and writing expected and required of senior leaders. PME institutions, as both benefactors and protectors of the public trust, must resist following suit. This is a rabbit hole we should avoid.

Even if aided by online detection software, unearthing plagiarized manuscripts is time intensive, burdensome, and unpleasant. Database comparisons are only as good as the database itself, so failing to identify many a plagiarized paper and incorrectly identifying some legitimate papers as plagiarized are possible scenarios. Accurate investigation requires extensive review well beyond the standard comparison report. A "clean" report, for example, provides no indication or assurance of writing integrity; it simply indicates that the proffered paper did not significantly overlap other papers in the database.

Because plagiarism frequently surfaces as a murky phenomenon open to multiple interpretations from diverse perspectives, adjudication is likewise difficult. Textual transgressions are documentable, but matters of authorial intent are characteristically far less transparent. At the Army War College, for example, most students who transgress offer apologies and admit carelessness when confronted with evidence of plagiarism in their submitted work. Transgressors tend to claim that they failed to grasp the seriousness of the offense, misunderstood faculty expectations, or unintentionally violated institutional standards. Explanations have included statements such as:

- "While I included no quotation marks, I intended to."
- "I sent the wrong version of my paper with the references inadvertently deleted."
- "My apologies, the quotation marks were left out due to an administrative oversight."
- "Quotation marks constitute busyness, which results in a cluttered writing style."

Most responses are softly apologetic acknowledgments moving as graciously as possible in the direction of plausible deniability.[21] Depending upon the magnitude of the offense, institutional response may include working closely with the student to address and correct the problem, allowing the student to voluntarily withdraw from the degree program, or empaneling an Academic Review Board (ARB) to conduct a formal plagiarism inquiry.[22] Review may be conducted at any point following discovery of a problematic document, regardless of when the transgression occurred. Some former students have been surprised to find their work questioned years after they have

U.S. Army War College graduating class of 2015 represented 387 men and women of the joint force, drawing from all branches of military, Federal agencies, and multinational environments (U.S. Army War College)

graduated and moved on. Some others never make it to graduation. Once convened, an ARB typically addresses two questions: Does the proffered document demonstrate clear evidence that work by another has been appropriated without proper credit or acknowledgment, and if so, is there evidence or reason to believe that the transgression reflects an intentional effort to deceive on the part of the person responsible? The matter of intent is frequently elusive, especially when the plagiarizer is nascent, that is, someone who is comparatively new at writing strategic analyses, which includes most students attending a senior Service college.[23]

A more sound approach, consistent with long-term national security interests, would be to treat plagiarism identified prior to graduation as an issue of professional competence. This postural and attitudinal shift would encourage more effective institutional intervention as a means of redirecting student efforts toward achieving true facility with the written word en route to assuming greater leadership responsibilities. Should the student continue to plagiarize as a means to satisfy written requirements, that student would eventually fail to meet standards. Students who fail to meet standards do not graduate. Writing without integrity is a failure to meet standards. Significantly, lack of writing integrity is also a viable predictor of failures yet to come should the student advance to ever-greater responsibility at the strategic level. Academic misconduct remains an issue, of course, but need not be the sole reason for denying degree status in an institution devoted to preparing warrior-scholars for service to the Nation. Plagiarism identified postgraduation should continue to be addressed as an issue of academic misconduct. At that point, lack of writing integrity reflects lack of personal/professional integrity as well; former students profited from their plagiarism by accepting degrees they know were fraudulent and not earned. Public trust is violated, judgment tarnished, and security placed at risk.

If PME institutions are to meet 21st-century challenges head on, they must embrace a cultural shift regarding the development of warrior-scholars. Future strategic leaders must be able to speak—and write—truth to power. They must be adept at advancing creative, original, and well-grounded ideas in support of national security, worldwide stability, and human welfare. They must learn to embrace the value of both knowing and sharing how ideas have been developed. And they must do so not as a means of protecting themselves, but as a means of protecting the Nation through the free intellectual exchange of ideas that are honest and original. Should students and faculty alike become convinced that original thinking and useful scholarship

are essential to national security and related endeavors, plagiarism—for all but the most ethically vacuous—will drop away quickly. Actively pursuing an "intellectual renaissance"[24] will bring forth a rededicated intellectual era in which empowered senior leaders aggressively pursue original thought as the only viable and enduring foundation for national security. Embedding writing integrity within these larger goals is a necessary first step toward mission success. JFQ

Notes

[1] See Anthony Cucolo and Lance Betros, "Strengthening PME at the Senior Level," *Joint Force Quarterly* 74 (3rd Quarter 2014), for a comprehensive examination of professional military education strengthening initiatives at the U.S. Army War College.

[2] Richard H. Kohn, "Beyond Sequester," *Joint Force Quarterly* 70 (3rd Quarter 2013).

[3] Chris M. Anson, "Fraudulent Practices: Academic Misrepresentations of Plagiarism in the Name of Good Pedagogy," *Composition Studies* 39, no. 2 (2011), 37.

[4] Chris M. Anson and Shawn Neely, "The Army and the Academy as Textual Communities: Exploring Mismatches in the Concept of Attribution, Appropriation, and Shared Goals," *Kairos* 14, no. 3 (Summer 2010), 8, available at <http://kairos.technorhetoric.net/14.3/topoi/anson-neely/Anson_Neely.pdf>.

[5] David Bartholomae, "Inventing the University," in *When a Writer Can't Write: Studies in Writer's Block and Other Composing-Process Problems*, ed. Mike Rose (New York: Guilford, 1985), 144.

[6] "Plagiarism," *Research Integrity* 9, no. 2 (Fall 2005–Spring 2006), 15, available at <www.grad.msu.edu/researchintegrity/docs/ri05.pdf>.

[7] David Cromwell, "Punishing the Pen with the Sword? Colombia's New, Extreme, and Ineffective Punishment for Plagiarism," *Pacific Rim Law & Policy Journal* 22, no. 1 (January 2013), 157–177. Professor Giraldo was also fined and her civic rights temporarily restricted. While the sentence, including jail time, was ultimately suspended, the plagiarism statute was amended to punish "violators with a minimum of thirty-two months in jail and a maximum of ninety" (161–162). See also Carlos Castellanos Rubio, "Colombian's Poetic World of Authors' Moral Rights: Considerations on Imprisoning a Professor for Plagiarism," trans. David Cromwell, *Pacific Rim Law & Policy Journal* 22, no. 1 (January 2013), 141–155.

[8] J. Dempsey, "Plagiarism in Dissertation Costs German Defense Minister His Job," *New York Times*, March 1, 2011. Six months following his resignation, Karl-Theodor zu Guttenberg was appointed Distinguished (Nonresident) Statesman at the Center for Strategic and International Studies in Washington, DC.

[9] See Nina Werkhauser, "A Chronology of the Schavan Plagiarism Affair," *Deutsche Welle,* October 2, 2013, available at <www.dw.de/a-chronology-of-the-schavan-plagiarism-affair/a-16589171>. See also "Education Minister Loses Doctorate for Plagiarism," *The Local Europe*, February 5, 2013, available at <www.thelocal.de/20130205/47785>.

[10] Sarah Harrison Smith, *The Fact Checker's Bible* (New York: Anchor Books, 2004), 87. As Smith acknowledges and Richard A. Posner (*The Little Book of Plagiarism* [New York: Pantheon Books, 2007], 34) confirms, "plagiarism cannot become the basis of a lawsuit [unless] it infringes copyright or breaks the contract between author and publisher." Although wrong and a form of fraud, "plagiarism qualifies as neither crime nor tort in the United States (Posner, 38).

[11] Katie Elson Anderson and Vibiana Bowman Cvetkovic, "Teaching Intellectual Honesty in a Parodied World," in *Stop Plagiarism: A Guide to Understanding and Prevention*, ed. Katie Elson Anderson and Vibiana Bowman Cvetkovic (New York: Neal-Schuman, 2010), 4–5; Michael Nelson, "The Good, The Bad, and the Phony: Six Famous Historians and Their Critics," *The Virginia Quarterly Review* 78, no. 3 (Summer 2002), 377–394. See also Hillel Italie, "Historians Under Fire," CBS News, January 24, 2002, available at <www.cbsnews.com/news/historians-under-fire>; and "Writing History," *PBS Newshour*, January 28, 2002, available at <www.pbs.org/newshour/bb/law-jan-june02-history_1-28>.

[12] Jonathan Martin, "Senator's Thesis Turns Out to Be a Remix of Other's Works, Uncited," *New York Times*, July 24, 2014, available at <www.nytimes.com/2014/07/24/us/politics/montana-senator-john-walsh-plagiarized-thesis.html>; also see Nick Corasaniti and Jonathan Martin, "Plagiarism Raises Ethical Alarm at Military School," *New York Times*, July 25, 2014, available at <www.nytimes.com/2014/07/25/us/politics/plagiarism-raises-ethical-alarm-at-military-school.html>; and Jonathan Martin, "Plagiarism Costs Degree for Senator John Walsh," *New York Times*, October 11, 2014, available at <www.nytimes.com/2014/10/11/us/politics/plagiarism-costs-degree-for-senator-john-walsh.html>.

[13] The academic year 2014 resident class included 77 international officers representing 67 different countries. Those pursuing the master of security studies degree are subject to the same standards and academic requirements as resident U.S. students. As English is a second language for most international fellows, the writing, language, and cultural challenges they face are diverse and unique. Consequently, their writing challenges are not addressed in this article.

[14] Sergey Bukakov, Vadim Dyagilev, and Alexander Tskhay, "Protecting Students' Intellectual Property in the Web Plagiarism Detection Process," *International Review of Research in Open and Distance Learning* 13, no. 5 (December 2012), 9.

[15] Patchwriting is commonly associated in contemporaneous usage with *remix* or *mashup* where the former refers to "paraphrasing from other sources and making the content fit together seamlessly," while the latter entails "copied material from several different sources without proper citation." See "Defining Plagiarism: The Plagiarism Spectrum," *GoTurnItIn.com*, available at <http://go.turnitin.com/paper/plagiarism-spectrum>.

[16] Rebecca Moore Howard, "A Plagiarism Pentimento," *Journal of Teaching Writing* 12, no. 2 (Summer 1993), 233.

[17] Rebecca Moore Howard, "Plagiarisms, Authorships, and the Academic Death Penalty," *Journal of Teaching Writing* 57, no. 7 (November 1995), 796–797.

[18] Howard, "A Plagiarism Pentimento," 239.

[19] The "gotcha game" operates from the assumption that all students are inclined to "cheat the system [at the] risk [of] their own personal welfare" and that faculty members have a responsibility to catch them. That view is rejected at the Army War College. See G. Jay Christensen, "Plagiarism: Can It Be Stopped?" *Business Communication Quarterly* 74, no. 2 (June 2011), 204; see also Douglas E. Abrams, "Plagiarism in Lawyers' Advocacy: Imposing Discipline for Conduct Prejudicial to the Administration of Justice," *Wake Forest Law Review* 4, no. 5 (November 2012), 921–933.

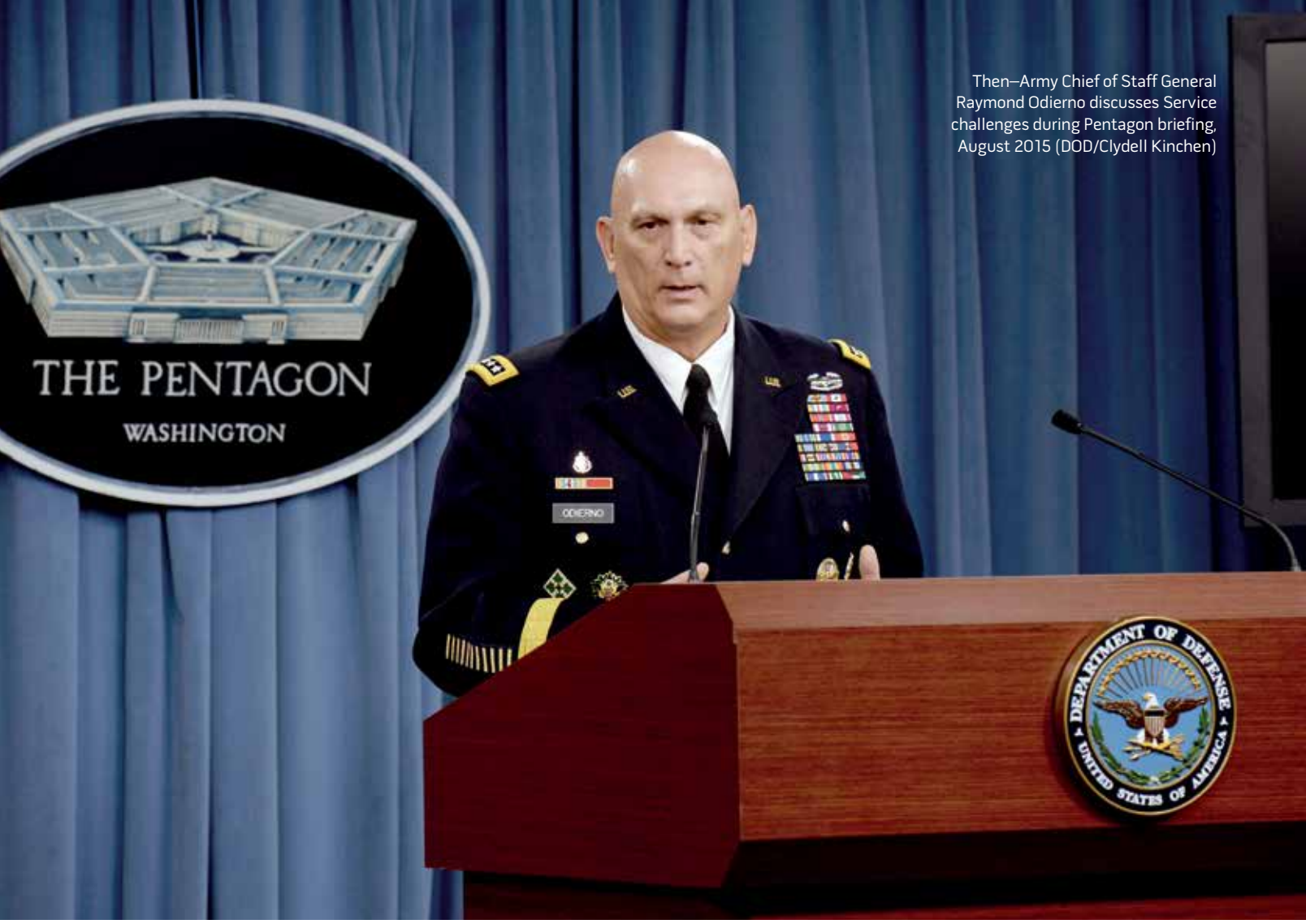
[20] Compare to Ry Rivard, "Turning on Turnitin," *InsideHigherEd.com*, April 16, 2013, available at <www.insidehighered.com/news/2013/04/16/writing-professors-question-plagiarism-detection-software>; and "2013 Resolutions & Sense of the House Motions," *NCTE.org*, available at <www.ncte.org/cccc/resolutions/2013>.

[21] Marshall Schminke, "Editor's Comments: The Better Angels of Our Nature—Ethics and Integrity in the Publishing Process," *Academy of Management Review* 30, no. 4 (October 2009), 3.

[22] Appointed by the dean, an Academic Review Board at the Army War College is composed of four faculty members who meet to investigate formal allegations of misconduct and advance recommendations.

[23] See Benson Honig and Akanksah Bedi, "The Fox in the Hen House: A Critical Examination of Plagiarism among Members of the Academy of Management," *Academy of Management Learning & Education* 11, no. 1 (March 2012), 105.

[24] Raymond T. Odierno, James F. Amos, and William H. McRaven, *Strategic Landpower: Winning the Clash of Wills* (Washington, DC: U.S. Army, U.S. Marine Corps, and U.S. Special Operations Command, May 2013).



Then–Army Chief of Staff General Raymond Odierno discusses Service challenges during Pentagon briefing, August 2015 (DOD/Clydell Kinchen)

Extending the Shelf Life of Teachers in Professional Military Education

By William G. Pierce, James E. Gordon, and Paul C. Jussel

William G. Pierce, James E. Gordon, and Paul C. Jussel are Faculty Members in the Department of Military Strategy, Planning, and Operations at the U.S. Army War College.

Over the past several years, a number of authors addressing professional military education (PME) have expressed frustration about and occasionally disdain for retired military officers who serve on the faculties of Department of Defense (DOD) senior-level colleges (SLCs).[1] In a 2011 article, Dr. George Reed, a former U.S. Army War College (USAWC) faculty member, stated, "Their [retired military on faculty] experiences have a shelf life that begins to expire on the date of retirement. They can usually be counted on to run a good seminar, but few contribute much in terms of scholarship as measured by the usual indicators of research and publication."[2] The authors are not in a position to defend those PME faculty members who have not performed well. However, it appears that the critics do not under-

Retired Admiral James G. Stavridis, dean of Fletcher School of Law and Diplomacy at Tufts University, speaks at U.S. Naval War College, December 2014 (U.S. Navy/James E. Foehl)

stand that retired military officers bring a specific body of knowledge of operational and strategic expertise to PME—in most cases acquired through years of experience.

This is a body of professional knowledge that SLC graduates must master to be effective strategic planners, advisors, and leaders. Retired military officers on a Service SLC faculty have an important role in preparing students for service at the strategic level. The faculty must know the past and current state of practice of operational and strategic planning, integrate new concepts into a continually evolving curriculum, understand the contemporary strategic environment, and convey this knowledge to a diverse student body.

The faculty, referred to here as professors of practice (PoP), are largely retired military faculty involved in teaching the professional knowledge related to theater strategy and campaign planning. This article explains the term *professors of practice* and examines some of the factors that affect how they maintain currency in the professional body of knowledge. It then describes how the changing strategic environment affects PoP currency and offers ways they can acquire and disseminate this information to students and faculty. Finally, it offers a number of actions organizations within DOD can take to support PoP more effectively.

Who Are Professors of Practice?

The USAWC School of Strategic Landpower consists of four teaching departments: the Department of Distance Education and three resident course teaching departments that roughly align to address the three "great problems" that former Secretary of War Elihu Root articulated over 110 years ago: national defense, military science, and responsible command.[3] This article focuses on those who teach military science in the School of Strategic Landpower, although many of the ideas presented also apply to those who teach other aspects of the professional body of knowledge. *Military science* is not a descriptive term, but two documents—U.S. Code Title 10 and Chairman of the Joint Chiefs of Staff (CJCS) Instruction 1800.01D, titled "Officer Professional Military Education Policy (OPMEP)"—provide some clarity on what the Service SLCs granting Joint Professional Military Education Phase II must teach. These two documents require Service SLCs to include instruction on "theater strategy and campaigning" and "joint planning processes and systems" in the curriculum.[4]

The focus of the OPMEP is clear regarding the goals of Service SLC education: "To prepare students for positions of strategic leadership and advisement; senior education focuses on national security strategy, theater strategy and campaigning, joint planning processes and systems, and joint interagency, intergovernmental, and multinational capabilities and integration."[5]

PoP Qualifications

The OPMEP addresses Service SLC faculty qualifications but with little specificity. For civilian faculty, which includes retired military, "The Services and NDU [National Defense University] determine the appropriate number of civilians on their respective college faculties. Civilian faculty members should have strong academic records or *extensive professional experience*" (emphasis added).[6] In the case of PoP, extensive professional experience is essential given that most of the subjects they must address have no analogue in civilian graduate degree programs.[7] In addition to the broad guidance in the OPMEP, faculty qualification requirements in a recent job announcement for a PoP position at the USAWC included the following: "Ability to prepare, teach, and lecture on subjects related to the theory and practice of military strategy, campaign planning, defense management, and joint and combined military operations."[8]

Factors Affecting PoP Currency

There are a number of significant differences in how PoP and teachers of other professions, such as medicine, maintain currency. These differences generally fall into two categories. The first are the challenges in generating opportunities for PoP to maintain currency in the professional body of knowledge through practice. The second relates to the changing strategic environment. Although understanding the strategic environment is not explicitly part of the body of knowledge, it is an essential aspect in planning and, as shown, is a

well-documented shortcoming in DOD planning over the past decade.

Medical school faculty members generally work in positions where they are able to practice their profession concurrent with teaching. This ability to practice would certainly help PoP maintain currency, but at a Service SLC, they do not enjoy the same opportunities for three reasons.

First, PoP are geographically separated from the offices and military organizations (for example, combatant commands and joint force headquarters) that translate national policy into executable military plans. Second, in addition to the physical separation, planning for the employment of military forces at any level requires a team approach. This team includes experts from all staff elements within the headquarters, interagency and multinational partners, and potentially nongovernmental organizations. This team establishes local procedures in addition to the guidance provided by policy and processes described in joint doctrine. While PoP have special expertise, it normally takes time for any newcomer to establish the credibility and trust essential to becoming an effective member of any high-performing team. Integrating a PoP into an engaged planning team in a timely fashion could be difficult under the best of circumstances.

Finally, there is a temporal aspect that precludes engagement by PoP through a complete contingency planning cycle. The near-term goal for developing contingency plans is 1 year, but a CJCS instruction states, "This goal assumes [as of now incorrectly] that APEX [adaptive planning and execution] planning tools and technologies has [*sic*] been fully implemented."[9] Episodic engagements by PoP with a joint headquarters during a planning cycle would certainly strengthen professional expertise, provide relevant perspectives, and help validate SLC curricula. Actual opportunities for a PoP to work through a complete planning cycle, though, are rare because of time considerations, faculty availability from teaching duties, and the cost of an extended temporary duty deployment at a joint or Service planning headquarters.

Figure 1. The Dynamic Security Environment: Selected Guidance Published Since 2001

National Law and Guidance
- Amendments to Title 10 U.S. Code (for example, addition of the Chief of the National Guard Bureau to the Joint Chiefs of Staff)
- *National Security Strategy* (2002, 2006, and 2010)
- *Unified Command Plan* (2003 with changes 1 and 2, 2005, 2006, 2008, and 2011 with change 1)

Department of Defense Guidance and Doctrine
- *Quadrennial Defense Review* (2002, 2006, 2010, and 2014)
- *National Defense Strategy* (2005 and 2008)
- *Defense Strategic Guidance* (2012)
- *National Military Strategy* (2004 and 2011)
- *Guidance for Employment of the Force* (2008, 2010, and 2012)
- *Joint Strategic Capabilities Plan* (2002, 2006, 2008, 2010, and 2012)
- Joint Publication 1, *Doctrine for the Armed Forces of the United States* (2007 with change 1, 2009, and 2013)
- Joint Publication 3-0, *Joint Operations* (2001, 2006 with change 1, 2008, and 2011)
- Joint Publication 5-0, *Joint Operation Planning* (2002, 2006, and 2011)

Figure 2. The Dynamic Security Environment: Selected Concepts Introduced Since 2001

- Rapid Decisive Operations (defunct)
- Effects-Based Operations (defunct)
- Systemic Operational Design (defunct)
- Secretary of Defense In-Process Review in Adaptive Planning (ongoing, under revision)
- Requirement for Combatant Commander Strategy and Campaign Plans (ongoing)
- Emphasis on Security Cooperation (ongoing)
- Operational Design (migrated from Army doctrine to joint doctrine)
- Air-Sea Battle (ongoing)
- Mission Command (migrated from Army doctrine to joint doctrine)
- Inclusion of Department of Defense Interagency Partners in Planning (Promote Cooperation) (ongoing)
- Regionally Aligned Forces (Army, ongoing)

Maintaining Currency

The constantly evolving national security environment in which PoP operate requires various organizations within the U.S. Government to review and, if necessary (due to world circumstances or Federal law), publish new national strategic guidance, policy, concepts, and doctrine. All of these documents are part of the PoP professional body of knowledge and affect currency and curriculum development. Two figures illustrate the scope and variety of these sources. Figure 1 is a partial list of government documents published after September 11, 2001, that PoP incorporated into curricula. Figure 2 lists doctrinal or theoretical concepts from the same timeframe. There are a number of points worth noting in these figures. Dr. Joan Johnson-Freese believes that Active-duty military with current experience should be the first choice in selecting faculty for the topics PoP address.[10] Recent operational experience is valued but is not necessarily the answer to better faculty. Figure 1 shows that some component of the professional body of knowledge changed each year between 2001 and 2013. If this trend continues, all faculty members, no matter how recent their operational experience, would have to understand and incorporate new guidance, concepts, or doctrine into the curriculum within a year or two. In figure 2, note the short shelf life of several concepts to appreciate the flux experienced by PoP. An additional challenge arises as several of these concepts were never codified in joint doctrine, yet the OPMEP requires PoP to dedicate classroom time to them even in their embryonic states.[11]

The Professional Body of Knowledge

PoP maintain currency in the professional body of knowledge through a combination of structured institutional support and significant individual effort.

The OPMEP requires the Joint Staff J7 Joint Education Branch to host a Joint Faculty Education Conference (JFEC) every year. The conference's purpose is to "present emerging concepts and other material relevant to maintaining curricula currency to the faculties of the PME and JPME colleges and schools."[12] The JFEC is held each summer, and the J7 hosts invite representatives of the PME community. DOD representatives' presentations focus on the evolving professional body of knowledge, but they also provide insight into the strategic environment.

There are numerous classified and unclassified policy and strategy documents directly related to PoP expertise (figure 1). PoP invest a significant effort to remain current. Although the faculty at Service SLCs cannot use classified documents in class because of the presence of international fellows, they serve as an important source for PoP expertise. Detailed knowledge of these documents is essential to shape the curriculum that respects security considerations while ensuring relevance to U.S. practitioners.

Articles in professional journals serve as valuable sources of PoP knowledge, both as sources of content and as vehicles for research and contributions by PoP to share new knowledge. Students invariably raise numerous topics for scholarly research such as flawed concepts, doctrinal voids, and inconsistent policies during seminar discussion. There are a number of other ways PoP maintain currency:

- Faculty development. While the PoP at the USAWC join the faculty with considerable operational and planning experience, the subject matter they address in class is so broad that no one person can be an expert on all facets of the theater strategy and campaigning curriculum (Root's "military science"). Effective faculty development programs at the institutional and departmental levels ensure all PoP have a common understanding of current strategies, concepts, doctrine, and the strategic environment. Faculty development is an opportunity for new faculty to share their recent operational experiences and for PoP to offer perspective, expertise, and instructional techniques to their new colleagues. This structured mentoring is especially valuable to new teachers who must coach SLC students in conceptual skills that will enable them to operate in the unfamiliar, uncomfortable, and complex strategic environment that is the new reality of their post-SLC studies.
- Reference handbooks. Publications that integrate current doctrine and best practices or consolidate diverse information into one document provide PoP with superb professional development references. Two examples are the USAWC *Campaign Planning Handbook* and the U.S. Naval War College's *Forces/Capabilities Handbook*.
- Inputs to joint doctrine. Inputs to doctrine contribute to the body of knowledge, and while the author is never acknowledged, changes to doctrinal publications undergo an extensive peer review process by practitioners.
- Optional lectures. Throughout each academic year there are numerous opportunities to expand professional expertise through optional lectures provided by a variety of subject matter experts on relevant topics.
- Supervise student research. PoP can maintain currency by serving as advisors for student research projects.

Understanding the National Security Environment

In addition to the professional body of knowledge, another component of PoP expertise is an understanding of the strategic environment. PoP educate students on the importance of integrating the effects of the environment when applying the professional body of knowledge to U.S. national security challenges. Two studies document the undesirable results that occur when U.S. strategic leaders failed to adequately understand the environment during planning and execution.

The first lesson, documented in a 2012 study by the Joint and Coalition Operational Analysis division of the Joint Staff J7, concerned a failure to understand the environment. The study concluded, "A failure to recognize, acknowledge, and accurately define the operational environment led to a mismatch between forces, capabilities, missions, and goals."[13] The second reference is a 2014 study by the RAND Corporation titled "Improving Strategic Competence." This study critiques the U.S. strategic effort over the past 13 years. The authors make clear one of their findings in the section titled "Military Campaigns Must Be Based on a Political Strategy, Because Military Operations Take Place in the Political Environment of the State in Which the Intervention Takes Place."[14] The study concludes the U.S. military did not adequately understand the political environment in the process of developing plans for Afghanistan and Iraq.

This requirement for environmental understanding is a recent addition to doctrine and PoP expertise. Introduced into joint doctrine in the 2011 version of Joint Publication 5-0, *Joint Operation Planning*, operational design methodology assists the commander in developing an operational approach. Three aspects of the methodology leading to an operational approach are understanding the strategic direction, understanding the operational environment, and defining the problem.[15]

In a memorandum describing the six officer-desired leader attributes for Joint Force 2020, General Martin Dempsey included the ability "to understand the environment and the effect of all instruments of national power."[16] Reinforcing General Dempsey's emphasis on this environmental understanding, Army Chief of Staff General Raymond Odierno sent a letter containing guidance to Major General William Rapp, the newly appointed commandant of the USAWC. Among other tasks, General Odierno asked Major General Rapp to ensure he understood the strategic environment to include "maintaining your current sense of the global and Washington

Graduates listen as General Dempsey delivers commencement address at National Defense University graduation ceremony in Washington, DC, June 18, 2015 (DOD/Daniel Hinton)

atmospherics."[17] In a USAWC faculty town hall meeting on September 29, 2014, Major General Rapp repeated that charge to the faculty to ensure the students also understood those aspects of the national security environment.[18]

It is fair to conclude that SLC graduates could learn what they need to know about the environment in their post-graduation assignments. However, this delay in effectiveness flies in the face of the vision for USAWC graduates as articulated by the previous commandant, Major General Anthony Cucolo. One slide in his command briefing stated:

Our primary purpose is to produce graduates who are skilled critical thinkers and complex problem solvers . . . who have rethought their professional identity for continued service at senior levels . . . and who, upon graduation, can immediately [emphasis in the original] *be value-added in an advisement or leadership role at the strategic level anywhere in the joint force or the interagency.*[19]

The need for PoP to understand and convey relevant aspects of the strategic environment to students is clear. Achieving that environmental understanding is a significant challenge for all PoP and is complicated by decisions regarding sources of information relevant to the curriculum and restrictions on disseminating environmental insight.

Achieving an Understanding of the Strategic Environment

The effort by PoP to maintain currency regarding the environment is a never-ending and time-consuming task. Fortunately, PoP do not suffer from a lack of sources regarding this aspect of the profession. On the contrary, determining what is relevant and timely for lesson development or inclusion in seminar dialogue given the multitude of unclassified information outlets is a challenge. Examples of open source information range from recently published books, journals, and blogs to unclassified daily summaries of U.S. military activity. PoP must engage in environmental scanning daily and be good team players. PoP who find open source material that provides insight into the dynamic strategic environment and supports lesson or course objectives must freely share this information with colleagues. Taken to the extreme, PoP inboxes could be overflowing with interesting but not necessarily relevant environmental insight. This is where PoP experience makes a difference: understanding what is and is not important in making critical points in class. Fortunately, sharing relevant environmental insight is something the

professionals in the authors' department have done well for years.

While open sources are an important source of environmental awareness, information from government insiders provides environmental understanding that is extremely valuable to students and faculty. However, access limitations and constraints on dissemination of this information pose a peculiar challenge for PoP and affect currency.

Over the course of the academic year, students often hear faculty and guest speakers declare that "relationships matter." For PoP, relationships are critical. Maintaining contact with former students who are in relevant operational assignments is an effective way for PoP to maintain a feel for the strategic environment.

PoP can gain an understanding of the environment through primary source interviews or interactions with senior members of DOD and interagency and multinational partners who deal with operational and strategic level challenges daily. The dedicated public servants who formulate and implement U.S. national policy are in ideal positions to provide clarity regarding the strategic environment. Unfortunately, these national security professionals are busy and do not have the time to document their observations in an effort to enlighten PME faculty.

Access to sources that have special insight is the first challenge. Relationships developed between senior government officials and PoP have served the faculty well at USAWC. These relationships, established during coincident assignments or student contacts, translate into access where PoP are able to obtain and share with faculty colleagues insights regarding current policies and practice. These relationships do not grow overnight, but once they are established, many PoP are able to tap into individual expertise that is simply not available to other faculty or the public at large. The USAWC leadership recognizes the importance of access. A qualification in a recent job announcement for a Chair of War Studies was an "extensive professional network enabling access to academic institutions, think tanks, government agencies, nongovernmental organizations, etc."[20]

The second challenge PoP face is that once acquired, dissemination of this environmental insight to a wide audience is affected, in part, by the USAWC policy regarding attribution of comments to sources.[21] Engagements with senior government officials or other subject matter experts who are not candid would not be useful to faculty or students. Source perspectives on the environment are enlightening but are often sensitive. The nonattribution policy protects those who are willing to provide insights, but this policy also limits the ability of PoP to document source insights in publicly available media. Another factor that limits dissemination of environmental perspective is the classification of the insight. Discussions with high-level sources frequently involve classified information, and there are restrictions on how this information is shared with colleagues and students.

While PoP will gain great insight from engagements with the sources described thus far, it is essential that a wider audience (for example, faculty colleagues and students) benefit from these activities. Dr. George Reed's comment regarding PoP "scholarship as measured by the usual indicators of research and publication" does not necessarily account for how PoP share environmental insight. The "usual indicators of research and publication" may not be relevant or useful in helping PoP and students understand the strategic environment.

Nonstandard Contributions to the Body of Knowledge

Scholarly articles have an important role in ensuring PoP currency, but there are a few drawbacks in relying on peer-reviewed journal articles to disseminate insight on the strategic environment. First is timeliness of an article. In a rapidly changing environment, traditional publication review and publishing processes might not keep up. As an example, Anthony Cucolo and Lance Betros authored an article for the July 2014 edition of *Joint Force Quarterly* regarding changes at the USAWC. During the peer review and publishing process, the USAWC leadership changed direction and moved away from some of the curriculum initiatives the authors presented.[22] A journal article regarding publications describes this situation:

As the rate of societal change quickens, cycle-times in academic publishing, which have lagged behind those in industry and technology, become crucial. In a world of instant communication in which 70 million blogs already exist and 40,000 new blogs come on line each day—the majority of which are not in English—academia cannot continue to rely on a venerated journal-publishing system that considers publication delays of up to two years to be both acceptable and normal.[23]

Another consideration is the need for the PME community to recognize that peer review may not apply to environmental insight. There is no doubt that peer review is a valuable tool for proposed additions to the professional body of knowledge. However, for environmental aspects of the profession, first-person accounts do not lend themselves to peer review. Washington, DC, atmospherics are about perceptions and opinions of the environment, and these opinions matter if one wants to operate effectively in the environment. When Eliot Cohen entered government service in 2007, he believed that "policy was forty percent substance and sixty percent personalities." As a result of his service in the Department of State, his view changed: he now believes government policy is "ten percent substance and ninety percent personalities."[24] Personalities change with every administration, and documented policy cannot always keep up. A recent example is the difference between the current practice regarding the Secretary of Defense campaign and contingency plan reviews and the current policy as articulated in a CJCS instruction.[25] Substantive differences such as these are important to Service SLC graduates who must operate in this environment and the PoP who must integrate these realities into the curriculum.

Trip reports, blog entries, online journals, and other nonstandard representations of new knowledge are ways PoP disseminate environmental realities to a relevant audience. These methods do not have the cachet of journal articles and may not have any enduring value. However, timely, relevant, and accurate insight into the strategic environment in any form arguably supports PoP currency and student learning.

Recommendations

A number of current policies and processes within DOD and the USAWC support the continuing education and development of PoP. However, the institution could do more if it seeks to extend PoP shelf life and leverage the years of teaching experience, context, and perspective that PoP bring to the classroom. Those responsible for PME within DOD should establish a system to disseminate critical references relevant to OPMEP requirements to the PME institutions. As noted above, PoP must have access to and integrate into the curriculum a never-ending flow of new strategic guidance, policy (classified and unclassified), concepts, and doctrine. The Joint Staff J7 Joint Education Branch could act as a clearinghouse for strategic guidance, policy, and concept documents and push them to each of the institutions involved in PME, similar to how it currently provides joint doctrine updates. This should include concepts and other strategic documents that are in draft with an anticipated date of release.

The Joint Faculty Education Conference is a great start to every academic year. It provides current insights for PoP and sets the stage for curriculum refinement. One change the J7 should consider is to conduct the JFEC in a classified forum. It is through access to classified insight and material that PoP will achieve the level of understanding of systems, processes, and concepts to shape the classes that serve the U.S. audience while respecting classification considerations.

Unfortunately, a JFEC-like conference once a year is not enough to enable PoP to maintain currency with respect to the strategic environment. Three proposals could help provide critical insight between the annual JFEC. First, J7 could host classified blogs available to those involved in policy development and planning, ranging from the Office of the Secretary of Defense (OSD) Policy to the joint force headquarters involved in operational/strategic planning. Second, J7 could develop a system similar to the server list called STRATLST that connects Army strategists via email. It has generated great participation and insight among practitioners and PoP. The one disadvantage is that the Army STRATLST operates on an unclassified network, which limits usefulness.[26]

Former Secretary of War Elihu Root (Wikipedia)

Finally, OSD Policy or the Joint Staff J5 Joint Operational War Plans Division could host a global brainstorming session on a regular basis to provide PoP with best practices among practitioners on status of policy and concepts between the annual JFEC. One of the authors recently participated in such a session unrelated to national security, but if done in a classified forum, it appears to be an ideal way to get worldwide input from practitioners on a variety of issues.[27]

There are a few other ways PME leadership can support PoP efforts to maintain currency.

- Leadership in PME must resource regular staff visits to relevant organizations and commands. These visits, while expensive, are critical in ensuring PoP currency and relevance.
- Service SLCs should actively seek and resource PoP engagements with

joint planning or policy development organizations for an extended period. This would normally be part of a PoP sabbatical. The Services, however, must support the SLCs with additional faculty to enable these extended operational support opportunities.

- Curriculum developers must engage subject matter experts who are outside of the Federal Government. These experts offer PoP and students a broader perspective leading to a better understanding of the environment.

Absent efforts to maintain currency, everyone involved in education, not just retired military officers in PME, has a shelf life. Because of the challenges outlined above, PoP will not be able to engage in their practice similar to teachers of other professions. It is not a foregone conclusion that PoP will become stale, though. With hard work, additional institutional support, and acceptance of nonstandard forms of new knowledge, there is no reason why PoP in Service SLCs cannot continue to grow professionally while maintaining an understanding of the evolving strategic environment. In fact, most competent PoP do maintain contact with their former students and others to gain that critical understanding of what is happening around the globe and how senior headquarters are adapting to changing political landscape. For officers and government civilians rising into the ranks of advisors to senior leaders and ultimately as senior leaders themselves, what could be more important in the PME environment than supporting PoP who prepare these committed professionals for years of valuable service to the Nation? JFQ

Notes

[1] Joan Johnson-Freese, "The Reform of Military Education: Twenty-Five Years Later," *Orbis* (Winter 2012), 147, 151. In a discussion of practitioners, she states, "What they [retired military officers] know tends to be an asset that declines in value the longer they are away from their area of professional activity." She goes on to say that "Active duty military officers are crucial to the PME mission, and should be the first choice to teach the courses on operational warfare, not former officers far removed from current experience."

[2] George Reed, "What's Right and Wrong with the War Colleges," *Defense Policy Journal*, July 1, 2011, available at <www.defensepolicy.org/george-reed/what's-wrong-and-right-with-the-war-colleges>.

[3] These words were part of a speech Elihu Root gave during the laying of the cornerstone of the Army War College at Washington Barracks, February 21, 1903.

[4] Armed Forces, 10 U.S.C. § 2155 (2011); and Chairman of the Joint Chiefs of Staff (CJCS) Instruction 1800.01D with Change 1, "Officer Professional Military Education Policy (OPMEP)," September 15, 2011, 1.

[5] CJCSI 1800.01D with Change 1, A-A-5.

[6] Ibid., B-3.

[7] GraduateGuide is a Web site that provides a directory of graduate schools in the United States and Canada. The site groups graduate majors into 52 broad categories. A search using several criteria showed that civilian graduate universities do not offer most of the subjects relating to "military science" that the OPMEP requires Service SLCs to address.

[8] Announcement NEDQ141197706, "Professor of Operational Art," *USAJobs.gov*, accessed at <www.usajobs.gov/GetJob/ViewDetails/379212900>.

[9] CJCS Instruction 3141.01E, "Management and Review of Joint Strategic Capabilities Plan (JSCP)-Tasked Plans," September 2011, B-15.

[10] Johnson-Freese, 147.

[11] CJCSI 1800.01D with Change 1, E-E-2. Joint Learning Area 3, Learning Objective a, states, "Evaluate the principles of joint warfare, joint military doctrine, and emerging concepts in peace, crisis, war and post-conflict."

[12] Ibid., C-3.

[13] Joint and Coalition Operational Analysis Division (JCOA), J7 Joint Staff, *Decade of War Volume 1: Enduring Lessons from the Past Decade of Operations* (Suffolk, VA: JCOA, June 15, 2012), 2.

[14] Linda Robinson et al., *Improving Strategic Competence: Lessons from 13 Years of War* (Santa Monica, CA: RAND Arroyo Center, 2014), 52–53.

[15] Joint Publication 5-0, *Joint Operations* (Washington, DC: The Joint Staff, August 2011), III-22.

[16] Martin E. Dempsey, "Desired Leader Attributes for Joint Force 2020," memorandum for Chiefs of the Military Services, Washington, DC, June 28, 2013.

[17] William Rapp, email message to authors, October 2, 2014.

[18] William Rapp, briefing, U.S. Army War College, Carlisle, PA, September 29, 2014. Used with permission.

[19] Command briefing, U.S. Army War College, Carlisle, PA, May 2, 2014.

[20] Announcement NEDQ1264682, "Chair of War Studies," *USAJobs.gov*, accessed at <www.usajobs.gov/GetJob/ViewDetails/387161800>.

[21] U.S. Army War College, "Carlisle Barracks Pamphlet 10-1: Administrative Policies and Procedures for Students, Faculty and Staff," June 2011, 2–10.

[22] Anthony Cucolo and Lance Betros, "Strengthening PME at the Senior Level: The Case of the U.S. Army War College," *Joint Force Quarterly* 74 (3rd Quarter 2014), 50–57.

[23] Nancy J. Adler and Anne-Wil Harzing, "When Knowledge Wins: Transcending the Sense and Nonsense of Academic Rankings," *Academy of Management Learning and Education* 8, no. 1 (March 2009), 72–95.

[24] Eliot A. Cohen, discussion with the U.S. Army War College Advanced Strategic Art Program during a National Security Staff Ride, Washington, DC, February 9, 2014. Used with permission.

[25] Paul Martin, "Adaptive Planning and GEF Review," lecture, Joint Faculty Education Conference, Washington, DC, June 24, 2014. Used with permission.

[26] Nathan K. Finney, email to authors, November 5, 2014: "STRATLST is a professional e-mail forum for strategists and interested individuals." Francis Park, email to authors, November 5, 2014: "Today there are 400 subscribers, with U.S. military members across all four services ranging from 1LT to general officers, as well as allied officers and civilian academics."

[27] From September 30, 2014, to October 2, 2014, Boston University School of Management hosted a business education "jam session" using IBM software (<www.collaborationjam.com>). During the session, worldwide practitioners were able to offer opinions on topics such as fostering ethical leadership, harnessing digital technology, and supporting 21st-century competencies.

President Obama and Vice President Biden hold meeting with combatant commanders and military leadership in Cabinet Room, November 12, 2013 (White House/Pete Souza)

Why War Plans, Really?

By Robert A. Gleckler

On the surface, "What are war plans for?" is a simple question. Clearly, these plans should state what we propose to do in case of war. From this point of departure, however, any further understanding of the role of war plans can diverge significantly. The fact is that war plans are used, leveraged, and cited for more than just war planning, and this carries inherent risks. The most common misuse of war plans usually stems from fundamental misunderstandings of the role of any single war plan or war plans in general and of the conceptual timeframes for their execution.

This article is not meant to explore the dark arts of operational planning. Reams of articles and terabytes of blog space on the merits or failings of existing doctrine for joint operational planning have been produced, and read almost exclusively, by practitioners. Rather, this article seeks to describe how war plans are used (and even misused) at the strategic and policy levels, often as a result of diverging interpretations of their nature and value. Pointing out these pitfalls could help current and future strategists and policymakers avoid problems in the future, thereby enriching the civil-military dialogue that should take place throughout plan development.

What War Plans Are Really Telling Us

The term *war plans* is a colloquial substitute for operation or contingency plans.[1] In addition to direct conflict, they can also address other condi-

Lieutenant Colonel Robert A. Gleckler, USA, is Deputy Chief of the Under Secretary of the Army's Strategic Initiatives Group.

During second battle of Libya, before zero hour, brigadier commanding tank units in Tobruk instruct tank commanders on operations using sand table for demonstration purposes (Courtesy Library of Congress/Official British Army photo No. BO 773 [BM 7241])

tions such as humanitarian assistance and disaster relief, defense support to civil authorities, or any other type of contingency that may call on resources from the military. Our joint operation planning framework includes the activities that combatant commanders and joint force commanders undertake to respond to contingencies and crises. Plans can serve as a basis for dialogue from the joint force to national leadership.[2] From planning guidance directed by the President, Secretary of Defense, and Chairman of the Joint Chiefs of Staff, combatant command and joint force command planners develop "campaign plans and contingency plans *based on current military capabilities* [emphasis in original]."[3] Formal planning guidance from these leaders is provided biannually in the form of the Secretary of Defense's *Guidance for Employment of the Force* and the Chairman's *Joint Strategic Capabilities Plan*.

The campaigns and contingency plans crafted in response to formal guidance documents are examples of deliberate planning. In the biannual revision of these documents, the Secretary and Chairman articulate planning requirements for specific contingencies and the level of detail required of those plans. These are the formal methods by which senior leaders tell us, "We really need to think about *X*." Crisis action planning is used for these unanticipated emergent contingencies that were not captured in formal planning guidance documents. Crisis action planning is used to address the problems that we simply did not see coming.

Understanding the timeframe for deliberate planning requirements is critical for an informed discussion on the role of war plans. Plans written by combatant commands in response to biannual formal guidance documents are expected to be developed and reviewed within the same timeframe. Though these contingencies may never transition to execution, the conceptual timeframe for potential execution is likewise within the 2-year planning cycle. Therefore, the plans must be based on current military capabilities if they are to meet the criterion of feasibility.[4] Campaign plans, though they are meant to span a 2- to 5-year timeframe, are also meant to be developed and reviewed within the 2-year window of the guidance documents. Campaigns are ongoing and at various stages of execution at any given

time. Crisis action planning addresses emergent contingencies, which are, by their nature, near term. In all the cases described herein, the plans must reflect the potential for near-term execution with the forces and resources available at the time.

To help inform planners of the realistic availability of forces in the near term, Services annually provide data in the form of apportionment tables that describe each Service's best estimate of the average availability of certain types of forces in the coming year. The data are not a perfect reflection of day-to-day availability of forces because unanticipated demands accumulate throughout the course of the year from the moment the ink dries on the annual revision. However, the estimate still provides a general picture of how many forces a Service could provide and the pace at which they could be made available in a contingency. Using this data to inform planning at the front end does not mean those are the exact forces that may be available at execution, but it should decrease the difference between what a commander expects and what a Service is able to provide at execution. Referenced early in the planning process, accurate force generation estimates may even drive a commander to have a discussion with policymakers regarding feasibility and the range of acceptable outcomes before initially embarking on deliberate planning.

What About the Future?

Given that deliberate and crisis action planning are directed at the near term—the adversary as we see him today and the forces and resources we can reasonably expect to be made available today and in the near term—how do we address the future? A planning process solely focused on near-term threats and availability of resources does not provide the impetus for long-term innovation, strategic planning, or programming. Not only will threats change over time, but our forces and resources will change as well. Within the Department of Defense (DOD) planning, programming, budgeting, and execution process, programming extends 5 years into the future, while planning extends 15 to 17 years. If plans written for today's threats with today's resources are used as the primary demand signal for future planning, programming, and strategy development, DOD could find itself constantly staring in the rearview mirror looking for hints of future demands.

This is where DOD Support for Strategic Analysis (SSA) has a major role to play.[5] Defense planning guidance that covers the 5 years of the upcoming Program Objective Memorandum (POM) is published annually and gives specific scenarios for DOD to examine. Significantly, the scenarios use forces programmed at the end of the POM rather than those available today. In parallel, assumptions about how the adversary may have changed must also be projected to the same timeframe. This is vital in avoiding the pitfall of examining today's adversary with tomorrow's force. DOD provides direction on developing scenarios to support senior leaders as they deliberate on strategy and programming.[6] In contrast to campaign and war plans, which are written by combatant commands and undergo review before being presented to the Secretary of Defense, SSA products are collaboratively developed by the Office of the Director for Cost Assessment and Program Evaluation (CAPE), Under Secretary of Defense for Policy, and Chairman of the Joint Chiefs of Staff using data provided by DOD components.[7] The scenarios can range from near to long term, but they should be based on plausible (though not necessarily the most likely) challenges and are not meant to be used in evaluating current war plans.[8]

Plausibility in the scenarios should not be overlooked. This is where DOD senior leaders can take the liberty to explore alternative futures but not stray so far from reality that the exercise is either useless or counterproductive. This somewhat obvious point was not always a given. In his history *American War Plans, 1890–1939*, Steven Ross notes that as late as 1916, the Navy General Board was still presenting plans for a naval showdown on the high seas between the United States and Germany. The plan was notably silent on the strategic question of why Great Britain—or any other belligerent—would simply stand aside and allow this to happen in the middle of World War I.[9] Today's SSA scenarios are directed to focus on the strategic level of warfare and include "threat and friendly politico-military contexts and backgrounds, assumptions, constraints, limitations, strategic objective, and other planning considerations."[10] Accounting for the strategic environment that would lead to conflict is a vital part of the civil-military dialogue associated with any future scenario.

What Are the Pitfalls?

As noted, the greatest sources for misunderstanding plans at the strategic and policy levels come from differing views on the temporal aspects of the plan (the timeframe for potential execution) and the purpose or value of the plan. Below are a few observations on the pitfalls associated with these different interpretations.

If You Build It, They Will Come. A deliberate plan, developed by a combatant command in response to formal biannual planning guidance from the President, Secretary of Defense, and Chairman, is meant to address potential near-term threats using resources that could reasonably be made available. A plan that is drafted uninformed by any consideration of available resources (that is, force availability or logistics sustainability) or transportation feasibility does not paint a realistic picture of the types of decisions and tradeoffs that senior strategic and policy-level decisionmakers would be faced with should the plan be required to transition to execution. At best, an uninformed plan shifts the assumption of risk from the author (the combatant command) to the force provider (for example, the Services, U.S. Special Operations Command, U.S. Transportation Command), or the transporter (U.S. Transportation Command) and masks potential shortfalls or lateness. At worst, it can paint a three-dimensional, overly optimistic picture that masks risk from all participants. A plan uninformed by resources becomes, "If you build it,

Soldiers plan for defense during decisive action rotation 15-02 at National Training Center on Fort Irwin, California, November 2014 (U.S. Army/Randis Monroe)

they will come." An unrealistic projection of available resources becomes, "If the balloon goes up, we're all in." And a policymaker has no idea of the tough decisions that might converge at execution, such as mobilization options, disengagement from existing priorities, overlapping requirements, authorities needed, access and overflight required, time required to meet objectives, or resources.

Ideally, these conversations happen at the genesis of planning rather than deep in the planning process when time has been squandered. Despite shortcomings in the process, one of the great values of in-progress reviews of deliberate plans and campaigns is that they can serve as a training ground for civil-military policy discussions when the stakes are not nearly as high, so that the participants are ready to have these discussions during crisis action planning. This applies not only to the dialogue between military planners and policymakers within DOD, but also to the dialogue that includes interagency and potential coalition partners.

The "New York, New York" Approach to Sustainment Planning. One common argument for unconstrained plan development is sometimes used during sustainment planning. Even when operational planners thoroughly adjust their force flow from the desired force to the realistically available force, logistics planners may stay fixated on sustaining the desired force. If the ideal, preferred force for the plan is larger than the force that could actually be generated, so the logic goes, then it is best to plan to sustain the larger force. If, at execution, a smaller force were provided, then certainly the plan would be sufficient to sustain that force as well. This is essentially the principle that "If you can make it here, you'll make it anywhere." Why risk being caught short if, by some supreme effort, the preferred force were actually generated?

The flaw in this approach is that it can lead to sub-optimized sustainment for the force that may actually arrive. Again, it is not only the size of the force, but also the timing of arrival. For example, food, fuel, or munitions could be programmed to arrive in time to sustain units that had not yet been generated, misaligning valuable cargo space for medical assets for the units that do arrive. Changes in the force flow of joint capabilities—whether based on force generation timelines or transportation timelines—do not simply extend the operational timelines of the plan; they can drastically impact the entire scheme of maneuver for the operational commander—and even result in discussions about policy implications (that is, time needed, projected casualties, international or domestic pressures, and so forth). Capabilities that had been needed early in the ideal timeline may no longer serve their purpose by arriving later. The plan that is based on the realistic generation and arrival of forces could have completely different priorities for the arrival of sustainment capabilities from the plan that is based on a desired or preferred force.

War Plans in Strategy Development

We must concede that operation and contingency plans carry a certain gravitas that SSA scenarios lack, *especially* when the former are referred to as *war plans*. After all, in the case of planning contingencies formally directed by the President, Secretary of Defense, or

Chairman, war plans are developed in response to direction from the highest levels. They are designed to meet real threats in the near term, are developed by the responsible regional combatant command, formally staffed for comment, and reviewed by the Secretary of Defense or Under Secretary of Defense for Policy. SSA scenarios, as described earlier, serve a different purpose and are developed in a process led by CAPE, often exploring the plausible—though not necessarily likely—challenges of the future. This creates a disparity in the perceived value of both products that unfortunately can carry over to the development of strategy for the future.

When exploring how DOD might meet future challenges, working groups have a strong tendency to use today's war plans, rather than SSA scenarios, to articulate what the demands might be. As described earlier, a plan that is developed for today's adversary, with today's resources, and to meet today's policy objectives may be inappropriate for exploring tomorrow's threat with the resources that we believe will be available in the future. At best, this can result in a temporal mismatch between today's needs and tomorrow's threats. At worst, this creates an incentive to distort a war plan from a feasible near-term plan to a programmatic demand signal, where desired future capabilities are shielded by the argument that "this is what the war plan calls for." The nature of the war plan thus changes from an operational approach for today to a justification for future programs. When a war plan is distorted this way, it becomes difficult to amend to meet changes in the operational environment for fear of losing a programmatic demand signal. Using today's war plans for strategy development can also lower the incentive to explore innovative schemes or resource investments to tackle the problem—or reduce its likelihood—in the future. After all, who wants to argue with the demands of a war plan that has been reviewed by the Secretary of Defense?

One of the most unsettling manifestations of this tendency occurs when strategy working groups combine existing war plans from today in an effort to get an understanding of the demands for combined execution in the future. Not only were the plans written considering today's resources for today's adversary, but they were also written independently of each other. Simply adding two plans together may not provide an accurate description of either the strategic environment or our national response to such a scenario. The strategic environment that led to conflict in each of the individual war plans might be completely different from the strategic background that would lead to simultaneous conflict with both adversaries at once. The operational approaches and the tolerance for different policy objectives and national resource availability may be completely different when the Nation is severely pressed by multiple adversaries, as compared to one at a time.

Take a Number, Please!

Plans that are tasked and developed in isolation from one another run the risk of missing the entire demand for resources that may arise during the contingency. While there is value in isolating a problem (a potential contingency) for deep examination by specific regional combatant command planners, the shortfall is that most contingencies will not be limited to a single combatant command problem. Even when planners are diligent in crafting a near-term plan informed by available resources, they may never have been formally tasked to take into account other related crises outside of their responsibility that would place competing demands on those same resources.

There is a growing acknowledgment within DOD that our approach to contingency planning needs to account for the range of demands that may be placed on the entire force during execution. A move to combine plans to understand the total demand must be more nuanced than simply adding together the requirements of several plans developed in isolation. It should lead to plans that are developed, from the outset, as collaborative approaches to a problem whose main focus may lie within one combatant command but could require supporting efforts from other combatant commands, especially those with global or functional responsibilities.

Plans that are developed collaboratively from the start will expose potential policy-level decisions that would have been masked previously. This applies not only to potential conflicts over resources but also to opportunities that can be exploited, such as placing an adversary's interests outside the local theater at risk. As General Ulysses S. Grant snapped to a panicky subordinate after a hard day's fighting during the Battle of the Wilderness in May 1864, "Go back to your command, and try to think what we are going to do ourselves, instead of what Lee is going to do."[11] A potential adversary whose threat is important enough for the national leadership to direct us to plan against it should not be addressed simply as one combatant command's problem, but as the Nation's problem. Our adversaries would not limit themselves to taking on a single regional combatant command, and we should not approach it that way either.

This holistic approach to plan development requires not only the involvement of multiple combatant commands, but also interaction with policymakers who can be exposed early on to gaps and opportunities that we may ask their help in addressing through interagency and international partners. This is especially important when trying to grasp what conditions might have existed prior to the crisis erupting.

Crisis versus Complacency

Our planning, both for war plans as well as SSA scenarios, places a heavy emphasis on the crisis portion (decisive action or Phase III) of a given contingency or scenario. War plans are often precluded by the phrase "and should deterrence fail," loosely translated as "when all hell breaks loose." Our planning construct describes contingencies as branches of the ongoing campaign plan, which is sometimes interpreted as "things were going fine, then we fell off a cliff." Our Joint Operation Planning and Execu-

tion System construct envisions triggers such as the declaration of a C-day (crisis) by the President, authorizing a whole host of force flow and mobilization activities. Our adversaries know this all too well, and they deliberately operate in the ungoverned white space of our planning construct that exists to the left of any sort of thresholds for crisis declaration.

For SSA scenarios, this crisis focus is especially problematic because it can lead to an overemphasis on the weapons systems and capabilities we may need once the sky *has* fallen. By envisioning a start point where all our efforts to set conditions between now and the beginning of a future catastrophe have been fruitless, we actually avoid some of the most substantial and informative policy-level dialogue about what we want to achieve in that ungoverned white space short of crisis between now and the future. While focusing on worst-case start points for crisis activities is important for understanding the highest bar of demand and for pushing the bounds of innovation, SSA scenarios can bring added value if they also explore alternative start points for future crises, envisioning the fruits of several years' efforts on access, overflight, availability, relationships, prepositioning, advances in medicine and technology, and so forth. Exploring alternative start points would not be intended to be unreasonably optimistic about the future but rather to actually inform ourselves, while the stakes are not as high, of the activities we may want to pursue to set better conditions should the crisis arise in the future.

In the End, It's Just a Plan

In the universe of demands placed on combatant commands, Services, and the entire DOD, war plans are simply one of many. In the midst of ongoing day-to-day operations, exercises, campaigns, and the Title 10 functions of man, train, and equip, war plans and scenarios designed to explore the future are sometimes not used or consulted.

Ironically, the further one gets from the factory floor of plan development, the more the notion of war plans seems to be placed on a pedestal. War plans, to those outside the dark arts of operational planning, seem to carry an aura of importance that can make practitioners cringe when asked about them. War planners need to display utmost caution when responding to the question "How many *X* (brigades, carriers, squadrons, and so forth) are in the plan?" Key follow-up questions should be: "Who is asking?" and "For what purpose?" Raw data, removed from the context of time (today or in the future? total demand or phased arrival?), strategic environment (in isolation or combined? start point assumptions?), or purpose (plan refinement or strategy development?) can be less than helpful. Such data can actually be counterproductive, especially when accompanied by the declaration, "That's what the plan calls for!"

We must remember that any plan, whether deliberate or crisis action, is *a* way, not necessarily *the* way, that the military instrument of national power will be applied during execution. In an ideal world, near-term plans, based on the reasonable expectation of resources, serve to stimulate the civil-military dialogue early in the process. They identify potential decision points when resources or policy aims may be in conflict, and they explore the range of acceptable outcomes before devoting valuable time and energy to developing specific courses of action. Well-developed plans, frequently reviewed for changes in the strategic environment, can help narrow the gap between expectations during plan development and the reality at execution, when time is always short and pressure is abundant.

Though war plans can certainly inform strategy development, they must be understood for what they represent: an approach for today's adversary with today's resources. To misuse war plans as a signal for future demands is to walk backward into the future. This can stifle innovative ways to approach future challenges and even distort an existing war plan from a truly operational approach for today into a holding pen for programmatic demand signals for the future. When we use SSA scenarios to explore innovative approaches to the future—even considering alternate starting conditions—we can foster a rich civil-military dialogue that captures risks and opportunities when the stakes are manageable and time is available. In understanding the roles of war plans and scenarios and their temporal contexts, DOD will be well positioned to address near-term challenges and to develop policy and strategy for the future. **JFQ**

Notes

[1] Examples of the legacy term *war plans* still in current use include the Joint Staff's Joint Operational War Plans Division in J5, Joint Strategic Plans, as well as Headquarters Department of the Army's War Plans Division, formally known as G-3/5/7, DAMO-SSW (Department of the Army, Maneuver and Operations, Strategic Studies, War Plans).

[2] Joint Publication 5-0, *Joint Operation Planning* (Washington, DC: The Joint Staff, 2011).

[3] Ibid., xiii.

[4] Chairman of the Joint Chiefs of Staff Instruction 3141.01E, "Management and Review of Joint Strategic Capabilities Plan (JSCP)-Tasked Plans," September 15, 2011, C-1: "(2) Feasibility. The assigned mission can be accomplished using available resources within the time contemplated by the plan."

[5] Department of Defense Directive 8260.05, "Support for Strategic Analysis," July 7, 2011.

[6] Ibid.

[7] Ibid.

[8] Ibid.

[9] Steven T. Ross, *American War Plans, 1890–1939* (London: Frank Cass, 2002), 64.

[10] "Support for Strategic Analysis," 6.

[11] Noah Andre Trudeau, *Bloody Roads South: The Wilderness to Cold Harbor, May–June 1864* (Boston: Little, Brown, 1989), 113.

Pilot with Task Force Medevac turns his back as UH-60 Black Hawk touches down at Eel River Conservation Camp in Redway, California, August 2015 (U.S. Army National Guard/Eddie Siguenza)

The Impact of Rising Compensation Costs on Force Structure

By Mark F. Cancian

The battle lines have been drawn: containing the growth of military personnel costs is either "a strategic imperative" or "breaking faith with those who have sacrificed so much."[1] As resources contract, the debate intensifies. Angry op-eds are exchanged, constituting the kind of high drama that attracts political and media attention.

Overlooked in this controversy are the adaptations that the Department of Defense (DOD) has already made to accommodate rising personnel costs. These are the same adaptations that businesses have made when faced with the high costs of a core workforce: reduce the number of high-cost personnel, replace full-time labor with part-time, use outside contractors where possible, substitute capital for labor, and be ready to rebuild if the need arises. With the military, these adaptations have shaped force structure and, hence, strategy. As a result, the United States has built a technological force that cannot go to war without mobilizing Reserves and employing vast numbers of contractors. This in turn shapes responsiveness to threats, the forces employed, and the level of public involvement with the military and conflict. Yet these strategic shifts have been buried in the highly charged arguments about the level of compensation.

Rising Personnel Costs

That personnel costs have risen steeply is not disputed. Since 2001, pay per Active-duty Servicemember has grown over 80 percent in 2001 dollars (about

Colonel Mark F. Cancian, USMCR (Ret.), is a Senior Advisor at the Center for Strategic and International Studies.

50 percent in constant dollars).[2] Military pay has increased 40 percent more than civilian pay since 2000, and enlisted Servicemembers are now paid more than 90 percent of their civilian counterparts with comparable education and experience (officers earn more than 83 percent of their civilian counterparts).[3] Retirement adds another $26 billion a year, and non-cash benefits tack on $39 billion, mostly for health care but also for quality of life programs such as childcare, schools, and adult education.[4]

These increased costs, often described as "unsustainable," have caused widespread alarm. Top military and civilian leaders in the Pentagon and a broad array of think tanks have called for action to curtail personnel costs lest they crowd out readiness and modernization.[5] The 2014 Quadrennial Defense Review makes compensation savings a major theme, so that funds are available "to sustain a healthy, ready and modern force into the future."[6]

So far, these efforts have had little impact. Curtailing military pay or benefits during wartime is hard. Military pay raises continued even as government civilians endured 3 years of pay freezes, though the most recent raises in fiscal year (FY) 2014–2015 were constrained to 1 percent. Repeated Obama administration proposals to introduce higher fees for TRICARE, the military healthcare system, have mostly failed in the face of ferocious lobbying by military associations. An attempt to reduce the growth of military retirement costs as part of the FY 2014–2015 budget deal was repealed a month after it was enacted.

Indeed, just holding the line on new benefits is difficult. In the last year, DOD and Congress granted benefits to same-sex partners, expanded medical stipends and transition assistance programs, allowed single parents and pregnant women to enlist, and created a special TRICARE Prime enrollment process for remote eligibles. None of these expansions are necessarily wrong, but they are moving in the wrong direction if the desire is to contain personnel costs.

Faced with this dynamic, the government took the traditional path of creating the Military Compensation and Retirement Modernization Commission. In January 2015, following extensive analyses and outreach, the commission presented a broad set of proposals for changes in health care, retirement, and benefits. Although congressional action is incomplete as of this writing, the House and Senate appear to have rejected most of the savings proposals but may modify the military retirement program to allow some benefits for personnel who leave before 20 years.

Adaptations and Their Effects

Critics of DOD efforts to reduce personnel costs argue that these expenditures have stayed constant over the last two decades and have not threatened modernization or readiness.[7] This is true; the military personnel appropriations have varied within a narrow band from 22 percent to 30 percent of the DOD budget over the last 30 years (about 33 percent when healthcare costs are included). Concerns that personnel costs will hurt readiness and eventually "consume the entire defense budget"[8] are, therefore, misplaced. However, this is not evidence of long-term fiscal sustainability, either. To accommodate higher personnel costs, DOD has made broad adaptations, which have had major strategic effects that are largely unrecognized.

Cut Expensive Personnel. The first adaptation is that, over time, DOD has cut the number of military personnel, particularly Active-duty troops, to fund higher individual compensation. For example, in 1994, $130 billion (in FY 2014 dollars) paid 1,610,000 Active-duty personnel and 998,000 Guardsmen and Reservists. In 2014, $137 billion paid 1,324,000 Active-duty personnel and 833,700 Guardsmen and Reservists. In other words, the same amount of money (slightly more, actually) was only enough to pay 450,000 fewer personnel. The Army and Marine Corps are particularly vulnerable because their budgets are so personnel-intensive (45 and 60 percent, respectively),[9] but all Services are affected. Indeed, practically every budget-cutting concept proposed by a think tank or an editorialist makes deep cuts to personnel. In one recent budget "wargame," for example, four think tanks realigned force structure and acquisition programs to fit lower future budget levels. All four teams proposed deep cuts to personnel, reducing numbers by 150,000 to 300,000. This was, they argued, the "Willie Sutton principle" applied to defense budgeting: personnel are where the money is.[10]

Rely on Part-Timers. The second adaptation has been to rely more on lower cost part-timers—that is, the Guard and Reserves. Before the Vietnam War, the Guard and Reserves comprised only 26 percent of the total force; during the draft years, Active-duty personnel were readily available, so there was less need to rely on Reserves. With the end of the draft and the announcement of the Total Force policy in the early 1970s, the proportion began to rise. By the end of the Cold War, when the full cost of sustaining the all-volunteer force had been accommodated, Guard and Reserves comprised 36 percent of the total force. In FY 2015, the proportion rose to 39 percent.[11]

To get a sense of what budget pressure might do to force structure in the future, suppose military personnel budgets hold constant (a best-case scenario for the next few years) but compensation increases at 2.5 percent per year (half the recent rate). That creates an annual bill of $3.4 billion. To pay this bill out of the personnel appropriations, the Services would have to cut 23,000 Active-duty personnel a year or shift 32,000 positions from the Active to Reserve Component.[12] Historically, the Services have done a combination of the two and cut operations and modernization as well. Cutting Reserve personnel would also save some money but only about one-quarter what is saved by cutting Active personnel. To budgeteers, the financial gain is often not worth the political and strategic cost. As a result, the number of Reserve personnel has declined less; thus, their proportion has increased.

The shift from Active to Reserve personnel has a basis in strategy as threats have diminished and required timelines for deployments have lengthened. Less sophisticated threats and longer

Airmen of 919th Special Operations Security Forces Squadron practice building-clearing techniques during annual training at Camp Guernsey, Wyoming, August 2015 (U.S. Air Force/Sam King)

deployments allow Reserve units the time needed to mobilize, train, and deploy, so more of them can be used. The Guard and Reserves have also adapted by reconfiguring themselves from a "strategic" reserve to an "operational" one. Still, the shift has introduced a degree of strategic risk as the Nation relies on forces that are inherently less ready and harder to use. The disruption of civilian communities produced by deployment of Reservists may also make military force less usable (a good or bad thing, depending on one's perspective).

A shift in power has followed the shift in personnel. In 2001, all Service Reserve chiefs received a third star to ensure their stronger participation in bureaucratic battles for resources and missions. In 2012, the Chief of the National Guard Bureaus received a fourth star and membership on the Joint Chiefs of Staff, establishing the Guard as a virtual fifth Service.

This dynamic of budget constraints and shifting power played out recently in the Air Force. In 2012, the Air Force proposed personnel cuts to both the Active and Reserve Components but more heavily to the Reserve. The Reserve Components, especially the Guard, working through their congressional supporters, had their cuts halted and a commission established "to undertake a comprehensive study of the structure of the Air Force . . . to best fulfill mission requirements in a manner consistent with available resources."[13] The commission, arguing both the ability of the Reserve Component to meet more mission requirements and the need to save money, proposed further realignment of missions from the Active to the Reserve Component so that the total force would shift from the present 69 percent Active/31 percent Reserve to 58 percent Active/42 percent Reserve.[14] In 2015, Congress, concerned about similar tensions within the Army, created the National Commission on the Future of the U.S. Army. With the methodology used by the Air Force commission as a precedent, the commission could produce a similar result.

Substitute Capital and Outside Support. DOD adaptations go beyond the personnel accounts. A further adaptation is the classic substitution of capital for labor. Businesses have done this as labor costs have risen (note the large number of robots in modern factories), and DOD has done the same. Unmanned aerial vehicles (UAVs), for example, now constitute a large proportion of the aviation inventory. Expensive new equipment such as the Navy's *Ford*-class carrier is justified in part by reduced personnel requirements. Over time, procurement spending per Servicemember has increased, from $37,000 in 1994 to

$71,000 in FY 2014 (all in FY 2014 constant dollars).[15] More broadly, the U.S. Armed Forces are more capital-intensive than the militaries of other countries. U.S. equipment spending runs about 25 percent of the total budget; our North Atlantic Treaty Organization (NATO) Allies are only at 14 percent (as NATO measures equipment spending).[16]

This approach has had some success. The liberation of Kuwait in 1991 and the overthrow of Saddam Hussein in 2003 were accomplished quickly and with few casualties. But the insurgencies in Iraq and Afghanistan could not be subdued despite the application of unprecedented levels of technology, from UAVs and sensors to long-range strike and the Internet battlefield. There is a whole literature exploring the impact of technology on warfare, and the U.S. focus on technology has roots beyond just the high cost of personnel—for example, in a democracy's concern about casualties and a national fascination with technology. Nevertheless, the military is not exempt from the laws of microeconomics; high personnel costs drive organizations to substitute capital for labor.

Substituting capital for labor has had other limits, as the Navy and Air Force found out in the 2000s. Coming out of the procurement holiday in the 1990s and not getting procurement money in war funding as the Army was able to do, the Navy and Air Force needed a way to recapitalize. Even as the Army and Marine Corps were expanding, the Navy and Air Force cut personnel, planning to put the savings into modernization. Because of rising personnel costs, however, the savings went instead into expanded personnel compensation and benefits.

Another adaptation has been the expanded use of contractors both at home and on the battlefield, which shifts higher cost and permanent military personnel out of routine support functions. During the Iraq War, for instance, Americans and commentators were surprised to learn that contractors were the largest "coalition" partner. At the height of the war in 2007, there were 165,000 troops in country and the same number of contractors (U.S., third-country nationals, and locals) supporting the war effort.[17] This growth mirrored expanded use of contractors at home where many base functions, and some headquarters functions, had been turned over to outsiders. There were solid strategic reasons for both. Contractors at home and on the battlefield took over routine tasks that did not require military personnel, such as food service and base maintenance. When the war or task ended, the contractors could easily be discharged. This paralleled the practice in business of focusing core personnel on core tasks and contracting other tasks out.

But this new reliance on contractors raised a host of concerns. Initially, these concerns were focused on financial issues—waste and unethical business practices. They prompted congressional hearings, new contracting structures, and a major investigating commission, the Commission on Wartime Contracting in Iraq and Afghanistan.

On a deeper level, many commentators worried about the strategic effects of depending on for-profit entities in national security. At home, contractors seemed to have taken over inherently governmental functions such as intelligence analysis and writing military doctrine. Overseas, the widespread and unprecedented use of contractors, particularly as they moved out of support roles and into the direct application of violence, raised concerns about "conduct[ing] wars with less political debate . . . undermining the legitimacy of counterinsurgency efforts and damaging the perceived morality of the war effort." Indeed, some observers worried that contractors "endanger the basic tenets of the military profession" by blurring the line between civilians and military.[18] Despite these concerns, the rising cost of military personnel and their declining numbers will push force planners to rely even more on contractors in the future.

Expand in Wartime. The final adaptation has been the need to rapidly expand the force in wartime because the peacetime force would be too small to handle large conflicts. This approach was remarkably successful in Iraq and Afghanistan, where the Army and Marine Corps were able to quickly add over 100,000 personnel during an increasingly unpopular war and without resorting to conscription. The risk is in timing—making the difficult political decision to expand when needed. The Iraq expansion did not begin until the end of 2006. It should have started years earlier before the force was strained by repeated deployments, but it took several years for the political apparatus to acknowledge so publicly that the wars would be long and hard. Thus, future force structures might only be viable if an early decision could be made to expand them. The Army is at greatest risk here, followed closely by the Marine Corps. Without rapid expansion, these Services will be stretched on the battlefield and stressed by long and frequent deployments.

Labor Economics versus Moral Obligations

Why can we not just settle on an objective formula for compensation that avoids these tough structural tradeoffs? The reason is that there are fundamentally different views on the nature and purpose of compensation. On one side are the labor economists—that is, people who argue that compensation should be set at a level adequate to recruit and retain the numbers and quality of personnel an organization needs. Cindy Williams, formerly an economist at the Congressional Budget Office, came to symbolize this approach when she testified in 1995 that all objective measures of compensation fairness were badly flawed and that, ultimately, "in a volunteer environment, the best indication of how well the military can compete as an employer is the overall picture of the services' success in recruiting and retention."[19] Therefore, military compensation could be assessed like other occupations and vary based on the state of recruiting, retention, and the economy. When unemployment is low and the force is expanding, compensation needs to rise to be competitive. Thus, compensation grew rapidly in the 2000s. However, when the force is shrinking (as it is today), compensa-

tion can decline. This view also held that compensation should be adjusted for personnel quality, with higher skilled personnel paid more than lower skilled personnel as happens in the broader economy.

On the other side are those who argue that there is a moral obligation to pay workers a "fair" wage. This view has roots as diverse as Karl Marx's socialism and Catholic social teaching, from Pope Leo XIII in the 19th century to Pope Francis today ("Not paying a just [wage], focusing exclusively on financial statements . . . goes against God").[20] Applied to the military, this approach argues that the Nation owes generous compensation to the 1 percent who serve on behalf of all. The military is not a job; it is a calling or a profession (to use the words of Charles Moskos, the late dean of military sociologists), and it deserves compensation on a moral basis, not an economic one.[21] This perspective is also egalitarian; all those who serve should be honored and treated equally, consistent with the rank structure. These arguments often take a moral tone. As General Gordon Sullivan, USA (Ret.), head of the Association of the U.S. Army, stated, cuts to compensation "demonize our troops as unworthy of the benefits they receive while ignoring the challenges, sacrifices, and hardships military personnel and their families face."[22]

The debate is not limited to the military. It has parallels at universities regarding payment of a living wage for low-skilled workers and in national debates about the level of the minimum wage. It does mean, however, that agreement on military compensation has been elusive. What one side regards as "reasonable adjustments," the other side regards as "betraying a commitment."

Some commentators have proposed conscription as a way out of this conundrum of high costs and adverse strategic consequences. Conscription seems to offer lower costs, abundant personnel, and a feeling that "everyone is in this together." In fact, experience from the Vietnam War indicates that of these goals, only abundant personnel are likely achievable and even then at a high cost to morale, effectiveness, and public regard. Whatever conscription's benefits might be, however, politicians, the military leadership, and the American people all oppose its reinstitution. Therefore, little more needs to be said about it as a solution.

New Jersey National Guard Soldier from 50th Infantry Brigade Combat Team launches RQ-11 Raven unmanned aerial vehicle during joint exercise, Warren Grove Gunnery Range, New Jersey, June 2015 (U.S. Air National Guard/Matt Hecht)

The Strategic Dimension

So the debate continues. Many commentators complain about the structural trends. Rachel Maddow criticizes "relying on a pop-up army . . . of greasy, lawless contractors." Andrew Bacevich laments "the large gap between the military and society." Bernard Rostker warns about the risks in overreliance on "unready" Reservists.[23] These concerns may or may not have merit, but they are essentially irrelevant. Unless the approach toward military compensation changes, the prospect is more of the same—a shrinking force, greater reliance on Reservists, contractors as a permanent element of the military force structure, capital substituting for labor, and rapid force expansion when wartime demands exceed what the peacetime force can handle.

And that is the element missing in discussions about military compensation. It is about more than what military personnel deserve or whether the costs are "affordable." It is about the adaptations the military establishment has made to accommodate the higher personnel costs. These adaptations have had profound strategic effects—effects that no Quadrennial Defense Review or strategy document discusses. The key strategic decision, then, is whether the military structure that the compensation structure produces supports the strategy the Nation wants, with risks and costs that are acceptable. The United States has backed into the existing structure without a lot of thought. As compensation discussions renew, the debate going forward ought to be broadened to include these strategic effects. **JFQ**

Notes

[1] "Strategic Imperative," from Posture Statement of General Martin E. Dempsey, Chairman of the Joint Chiefs of Staff, Senate Armed Services Committee, Fiscal Year 2015 Department of Defense Budget, March 5, 2014, available at <www.armed-services.senate.gov/download/dempsey_03-05-14>; Steve Strobridge, "Spare Us the 'Keeping Faith' Blather," *MOAA.org*, March 15, 2012, available at <www.moaa.org/main_article.aspx?id=9412>.

[2] Robert Hale, Testimony to the Senate

Armed Services Committee, March 28, 2012, available at <www.defense.gov/news/newsarticle.aspx?id=67743>. Calculations vary depending on treatment of accruals for TRICARE and retirement, the mobilization of Reservists, and personnel costs in war funding, but all methods show large cost increases.

[3] Comparison with civilian compensation from *Report of the Eleventh Quadrennial Review of Military Compensation (QRMC), Main Report* (Washington, DC: Department of Defense [DOD], June 2012), 31. The increase of 40 percent compared to civilian compensation has been cited repeatedly by DOD; for example, see Secretary of Defense Chuck Hagel, *FY 2015 Budget Preview*, February 24, 2014.

[4] *Interim Report of the Military Compensation and Retirement Modernization Commission* (Washington, DC: Military Compensation and Retirement Modernization Commission, June 2014), 15, § 6.2. DOD costs only.

[5] For example, on June 3, 2012, 25 experts from 10 think tanks wrote an open letter to senior Members of Congress and the Secretary of Defense recommended "curb[ing] the growth in military compensation costs, as well as reductions to bases and shrinking the civilian workforce." The think tanks spanned the ideological spectrum from the libertarian Cato Institute to the liberal Center for American Progress to the conservative American Enterprise Institute. For a sample of individual statements, see Leon E. Panetta, Testimony before the Defense Subcommittee of the Senate Appropriations Committee, June 13, 2012; Robert Gates, Remarks at the Eisenhower Center, Abilene, KS, May 8, 2010, which included his famous comment, "Health-care costs are eating the Defense Department alive," available at <www.defense.gov/speeches/speech.aspx?speechid=1467>; Chuck Hagel, "FY15 Budget Preview," The Pentagon, February 24, 2014, available at <www.defense.gov/Speeches/Speech.aspx?SpeechID=1831>; Dempsey.

[6] *Quadrennial Defense Review 2014* (Washington, DC: DOD, March 4, 2014), 39, 48–51.

[7] The Military Officers Association of America did the original analysis, which has been picked up by many others. See, for example, *A Bargain, Not a Liability* (Alexandria, VA: Military Officers Association of America, 2014), 3. This calculation excludes non-cash benefits and veterans' benefits, both of which have increased steeply in recent years.

[8] For example, David R. Segal and Lawrence J. Korb, "Manning and Financing the Twenty-First Century All-Volunteer Force," in *The Modern American Military*, ed. David M. Kennedy (New York: Oxford University Press, 2013), 127; Paul K. MacDonald and Joseph M. Parent, "The Banality of Retrenchment," *ForeignAffairs.com*, March 9, 2014, available at <www.foreignaffairs.com/articles/united-states/2014-03-09/banality-retrenchment>.

[9] Military personnel appropriation as a percentage of total service FY14 budget. Excludes war funding (overseas contingency operations funding). Total personnel compensation, with health care and benefits, is substantially larger. The Marine Corps percentage is unusually high because its aviation procurement and operations are mostly funded by Navy appropriations.

[10] *Joint Think Tank Event: Alternatives to the QDR and FY15 Defense Budget, Comparison Across Teams* (Washington, DC: Center for Strategic and Budgetary Analysis, February 5, 2014), available at <www.csbaonline.org/2014/01/28/joint-think-tank-event-alternatives-to-the-qdr-and-fy15-defense-budget/>. The teams were from the Center for Strategic and Budgetary Assessments, Center for Strategic and International Studies, Center for a New American Security, and American Enterprise Institute. Willie Sutton was a bank robber who apocryphally stated that he robbed banks "because that's where the money is."

[11] Office of the Under Secretary of Defense (Comptroller)/Chief Financial Officer, *United States Department of Defense Fiscal Year 2015 Budget Request Overview* (Washington, DC: DOD, March 2014), A2, A3.

[12] Author calculation using data from FY14 DOD budget materials and Eleventh QRMC. This calculation is consistent with a detailed Active/Reserve Component cost comparison conducted by the Reserve Forces Policy Board, *Eliminating Major Gaps in DOD Data on the Fully Burdened and Life-Cycle Cost of Military Personnel: Cost Estimates Should Be Mandated by Policy* (Washington, DC: Reserve Forces Policy Board, January 7, 2013), 5. The study calculated that "the [Reserve Component] per capita cost ranges from 22% to 32% of their [Active Component] counterparts' per capita costs, depending on which cost elements are included."

[13] *National Defense Authorization Act for Fiscal Year 2013*, Public Law 112-239, January 2, 2013, Subtitle G, § 363 (a)(1).

[14] *Report to the President and Congress of the United States* (Washington, DC: National Commission on the Structure of the Air Force, January 30, 2014), 36.

[15] Office of the Secretary of Defense (Comptroller), *National Defense Budget Estimates for FY 2014*, May 2013, tables 6-8, 7-5, available at <comptroller.defense.gov/Portals/.../defbudget/fy2014/FY14_Green_Book.pdf>. Excludes war funding.

[16] Calculated from data in *Financial and Economic Data Relating to NATO Defense* (Brussels: NATO Public Diplomacy, February 24, 2014).

[17] Moshe Schwartz and Jennifer Church, *Department of Defense's Use of Contractors to Support Military Operations: Background, Analysis and Issues for Congress*, R43074 (Washington, DC: Congressional Research Service, May 17, 2013), 25. For an expanded discussion of contractors on the battlefield, see Mark F. Cancian, "Contractors: The New Element of Military Force Structure," *Parameters* (Autumn 2008), 61–77.

[18] Strategic concerns from T.X. Hammes, "Private Contractors in Conflict Zones: The Good, the Bad, and the Strategic Impact," *Joint Force Quarterly* 60 (1st Quarter 2011), 26–32; Gary Schaub, Jr., and Volker Franke, "Contractors as Military Professionals?" *Parameters* (Winter 2009/2010), 101.

[19] Cindy Williams, Testimony on Military Pay before the Senate Armed Services Committee (Washington, DC: Congressional Budget Office, March 16, 1995), 14. This testimony hit the Internet as an example of attacks on military benefits and made Dr. Williams well known.

[20] Karl Marx, *Critique of the Gotha Programme* (1875); Pope Leo XIII, *Rerum Novarum* (*Rights and Duties of Capital and Labor*), 1891; Pope Francis, "Speech to Workers in Cagniliarca, Sardinia," September 23, 2013, cited in John Coleman, "Pope Francis on the Dignity of Labor," *America Magazine*, November 20, 2013, available at <http://americamagazine.org/content/all-things-/pope-francis-dignity-labor>.

[21] Charles C. Moskos, Jr., "The All-Volunteer Military: Calling, Profession, or Occupation?" *Parameters* (Winter 2010/2011), 23–31.

[22] Gordon Sullivan, "Don't Cut Troops' Pay and Benefits," letter to the editor, *Washington Post*, January 6, 2014.

[23] Rachel Maddow, *Adrift: The Unmooring of American Power* (New York: Crown Publishing, 2012), 186–187; Andrew J. Bacevich, *The Limits of Power: The End of American Exceptionalism* (New York: Metropolitan Books, 2008), 122–123, 131, 152–156; Bernard Rostker, *Rightsizing the Force: Lessons for the Current Drawdown of American Military Personnel* (Washington, DC: Center for a New American Security, June 2013), 5–11.

Guided-missile cruiser USS *Lake Erie* (CG 70) launches SM-3 Block 1B interceptor during Missile Defense Agency test and successfully intercepted complex short-range ballistic missile target off coast of Kauai, Hawaii (DOD/U.S. Navy)

The Case for the Joint Theater Air and Missile Defense Board

By S. Edward Boxx and Jason Schuyler

Consider this possible scenario: *A rogue nation threatens to fire ballistic missiles at the United States and its regional allies. In response, a forward-deployed U.S. Army radar transitions to high alert and continually scans the stratosphere, intending to detect and track the adversary's ballistic missiles. U.S. Navy and partner nation Aegis ships armed with missile interceptors depart their home ports and steam toward prearranged operating areas. Meanwhile on land, missile defense convoys disperse near air and sea bases, activate their radars, and raise their launchers skyward. At multiple operations centers, Airmen plan attack operations against the enemy's command*

Colonel S. Edward Boxx, USAF, is Chief of the Space and Integrated Air and Missile Defense Division at U.S. Pacific Command. Lieutenant Colonel Jason Schuyler, USA, is assigned to the Joint Staff J7 Future Joint Force Development Division.

and control and missile defense units. These joint missile defense movements require a sophisticated response, but what should the mechanism be to socialize, synchronize, and recommend these actions within a geographic combatant command? The answer: that mechanism would include inputs from the land, maritime, and air commanders (along with supporting agencies), yet present a holistic, inclusive, and effective missile defense response from the joint force commander.

Planning and executing a layered missile defense using the assets mentioned in the scenario requires coordination and integration among the land, maritime, and air components as well as subunified and regional missile defense partners. Not surprisingly, these resources for integrated air and missile defense will continue to be limited, as recognized by the Chairman of the Joint Chiefs of Staff in his *Joint Integrated Air and Missile Defense: Vision 2020*.[1] Missile defense systems are complex, expensive, and limited in number, and the lack of affordable interceptors gives potential adversaries a cost advantage as it is cheaper and easier to launch ballistic missiles than to successfully intercept them. Navy Aegis ships, the Army Terminal High Altitude Area Defense (THAAD) system, and Patriot PAC-3 systems have proven and impressive intercept records.[2] Yet these systems are finite in number, cost millions of dollars, and are in high demand across the combatant command's (CCMD's) area of responsibility (AOR). In short, integrated air and missile defense (IAMD) is an inherently joint and increasingly multinational and cross-CCMD mission area. How the geographic combatant commander or joint force commander (JFC) orchestrates these multi-Service and international missile defense operations requires a joint mechanism that is responsive and linked to the CCMD's battle rhythm.

One solution is to operationalize the CCMD staff through the Board, Bureau, Center, Cells Working Group (B2C2WG) process with a dedicated and collaborative air and missile defense board—akin to the well-known and practiced joint targeting coordination board or the joint collection management board. A missile defense coordination forum does not exist in joint doctrine, yet a joint theater air and missile defense (JTAMD) board, fed by a supporting JTAMD working group, could provide the much needed joint IAMD planning and coordination support capability to the theater area air defense commander (AADC) and the joint force commander.

B2C2WG Defined

The hierarchal Napoleonic system of "J-codes" has of course been used by military organizations for centuries and continues to align commanders and their staffs. But CCMDs and staffs have searched for responsive processes to function more effectively in a diverse, complex, and ever-changing geopolitical environment.[3] The B2C2WG template offers a possible solution and has been embraced by U.S. Pacific Command (USPACOM) during its transition to an *operationalized* headquarters. In the past, CCMD headquarters relied on subordinate task forces as the operational sinew for the theater; now, however, the USPACOM directorates fulfill the operational as well as traditional strategic responsibilities. So instead of completely eliminating the 200-year-old system, USPACOM maintains the J-code system as a recognizable CCMD staff structure, but distinguishes the need to coordinate laterally through the vertically aligned staffs. Therefore, the B2C2WG process has been adopted as the mechanism to interconnect combatant command J-coded directorates and assimilate planners, operators, intelligence agencies, and stakeholders while simultaneously connecting with the functional component commands. The B2C2WG process has enabled traditional organizations to more effectively integrate and synchronize the battle rhythm process, in both peacetime and crisis. In November 2013, Operation *Damayan* (the coordinated theater-wide response to a massive typhoon that struck the Philippines) validated this methodology. It illustrated the ability of the USPACOM staffs, subordinate task forces, partner nations, and interagency teams to rapidly employ a productive and sustainable battle rhythm during a crisis.

The same responsiveness demonstrated in the *Damayan* relief efforts needs to be applied to missile defense and should be included in the USPACOM B2C2WG process. North Korea's missile arsenal remains a worrisome threat to U.S. and allied security and in fact continues to grow, as evidenced by the 2014 firing of ballistic missiles into the sea toward Japan. Successive USPACOM commanders continue to describe North Korea's nuclear and missile capabilities and its proliferation of weapons of mass destruction and associated technologies as the major challenge to stability in the region.[4] The enormity of the region (the USPACOM AOR covers half the Earth, contains over three billion people, and includes the world's three largest economies and one-third of all U.S. trade) also epitomizes missile defense challenges. The obligation to multiple subunified commands and treaty obligations further strain the demand for limited missile defense resources. Of the seven total security treaties signed by the United States, five reside in the USPACOM AOR with Australia, Japan, the Philippines, South Korea, and Thailand. Each represents differing missile defense capabilities, and further exemplifies the need for a doctrinally recognized, theater-wide JTAMD board.

Northeast Asia, and in particular the potential battlespace between the Korean Peninsula and the Japanese archipelago, illustrates the complexity of missile defense in the USPACOM AOR and the need for the JTAMD board. For example, the Republic of Korea's navy employs *KDX-III*-class Aegis destroyers and Patriot PAC-2 missile batteries, while nearby Japan uses *Kongo*-class Aegis ships and Patriot PAC-2/3 interceptors. In and around both countries, U.S. forces (possessing similar Patriot and Aegis assets) must be able to complement the regional defense architecture while protecting the homeland from intermediate and intercontinental ballistic missiles targeting Guam and the United States. Sensors such as AN/TPY-2 and SPY-1

General James D. Thurman, United Nations Command, Combined Forces Command and United States Forces Korea commander, and General Kwon Oh Sung, Combined Forces Command deputy commander, brief Republic of Korea President Park Geun-hye on status of Ulchi Freedom Guardian exercise, August 22, 2013 (U.S. Army/Brian Gibbons)

radars and Japanese and Korean sensors can cue other systems, greatly reducing the time required to compute firing solutions. Concepts such as "launch on remote" and "engage on remote" via datalinks are significantly extending the range of missile intercepts—meaning a successful ballistic missile defense (BMD) kill chain (sensors, shooters, command and control) must overcome regional and political boundaries. For instance, a U.S. Aegis ship positioned between South Korea and Japan could impact missile defense for either country. With an overlapping defense framework, ships and ground-based units are assigned primary defense responsibilities such as those found in the defended asset list (DAL). But if coordinated and planned, these systems can also assist one another as a "backup" shooter and, in some cases, serve as the tertiary defense. It is imperative that these efforts are synchronized because of the finite numbers of Patriot, THAAD, and SM-3 interceptors and the multirole mission requirement to provide an air defense capability within the AOR.[5] To effectively manage these limited assets, the JFC and the AADC staffs must have an adaptable coordination mechanism to rapidly plan across vertically stovepiped organizational hierarchies. The theater AADC certainly retains the prerogative to engage the JFC in all air and missile defense issues at any time. However, due to the complex relationships among partner nations, other U.S. agencies, and CCMDs, the JTAMD board's ability to plug into the CCMD commander's battle rhythm could hasten theater and cross-AOR missile defense coordination.

Currently in U.S. Army doctrine, a theater air and missile defense (TAMD) coordination board (formerly known as a reprioritization board) led by the deputy AADC exists primarily to recommend changes to the DAL, a JFC-approved list of protected assets connected to a specific operations plan.[6] The joint TAMD board would build upon this framework, open the aperture to other topics besides DAL prioritization, and include other members. Coalition participation early in the C2B2WG process could facilitate faster allied approval and collaboration on proposed operations. In addition to multinational participation, other JTAMD board members/observers should also include subunified commands such as U.S. Forces Korea (USFK) and U.S. Forces Japan (USFJ). An IAMD functional representative from the CCMD or JTF headquarters and, in some instances, other missile defense organizations would also attend. The Missile Defense Agency (MDA), the U.S. Strategic Command (USSTRATCOM) Joint Force Functional Component Command for Integrated Missile Defense, and the

U.S. Soldiers perform pre-launch checks on Patriot missile launcher as part of field training exercise on Kadena Air Base, Japan (U.S. Air Force/Maeson Elleman)

Joint Integrated Air and Missile Defense Organization already provide liaison officers to USPACOM, and their participation would allow the vital contributions of those supporting organizations. As a case in point, the MDA Sea-Based X-Band radar, normally used for testing, could augment an operational layered missile defense, but would require inter-CCMD coordination. Other JTAMD board observers would include the global force management and the J4 munitions divisions in order to facilitate requests for forces and expedite replenishment of high-demand replacement missiles.

In an attempt to mimic and codify the success of the staff response during Operation *Damayan* and other B2C2WG achievements, USPACOM AADC and CCMD officers explored ways to improve missile defense integration with the goal of a collaborative problem-solving process. Subsequently, during Exercise Keen Edge 2014, the deputy AADC expanded the U.S. Army's process to include joint participants such as USFJ, the Japanese Self-Defense Forces, and CCMD officers. Additionally, during Exercise Ulchi Freedom Guardian, USFK and the theater deputy AADC further refined the joint process with Republic of Korea forces. Both exercises demonstrated the success of an inclusive JTAMD board by improved allied involvement during planning, and significantly aligned the staffs in supporting the missile defense weight of effort. With further improvements to the JTAMD process, continuing development of IAMD officers, and additional changes to joint doctrine, missile defense could become even more effective.

Recommendations

First, the JTAMD planning process should be adopted as a joint IAMD planning capability and must be exercised regularly and continually refined. Combatant commands need to adopt a coordinated and integrated approach to missile defense training scenarios that include all elements, from tactical units (sensors and shooters) all the way to national command authorities. Air and missile defense must be considered early in exercise development, and all training, testing, and evaluation events should dovetail into an overall tactical-operational-strategic "pathway to victory" road map. The deputy AADC-led JTAMD board should offer a forum to formulate and provide timely adjudicated solutions not only for DAL priority, but also for interceptor resupply, requests for additional forces, cross-CCMD coordination, and changes to regional defense and readiness postures (alert states). Complex missile defense systems are increasingly no longer just regional, but impact multiple commands, and thus maintenance requirements for long-range radars such as the AN/TPY-2 need an operation-

ally focused venue. Additionally, the USPACOM AOR, which includes the MDA Reagan Test Site in Kwajalen Atoll and the Pacific Missile Range Facility in Hawaii, conducts one of the most complicated and intricate missile defense tests in the world. A JTAMD process would serve as a conduit to strengthen warfighter and MDA efforts such as combining real-world missile tests with operator training at every opportunity. Previous MDA tests have included realistic scenarios with multiple engagements of Patriot, Aegis BMD SM-3, and THAAD missiles against live targets, and recently demonstrated the successful first firing of the Aegis Ashore weapons system. Therefore, to better leverage these singular live events, the JTAMD board (supported by a JTAMD working group chaired by a captain or colonel) should be instituted and practiced to inculcate the collaborative process and render it routine.

Second, as Joint Publication 3-01, *Countering Air and Missile Threats*, undergoes revision, more of its content should be devoted to the development of joint air and missile defense officers and intra- and inter-CCMD coordination. Although USPACOM currently holds the distinction of being the only geographic combatant command to conduct both regional and homeland missile defense, other regional AADCs and JFCs will be required to routinely coordinate across combatant command boundaries as the air and missile threats to the Nation and its regional partners continue to mature and proliferate.

Last, in August 2012, the Deputy Secretary of Defense designated USSTRATCOM as the joint lead for integrating and synchronizing joint BMD training in coordination with the CCMDs and the military departments.[7] However, there is currently no joint organization in the Defense Department tasked with the responsibility of training and developing joint IAMD planners. More must be done to cultivate and track qualified and experienced joint IAMD officers, as their experience is crucial to joint layered missile defenses. CCMD and Service personnel managers currently are unable to adequately identify experienced joint IAMD planners to fill billets. A better way to manage human capital would be to establish a joint air and missile defense skill identifier, that is, a military occupational specialty or Air Force specialty code. Whether an Airman, surface warfare officer, or air defender, these officers epitomize jointness, as they understand not only their Service-specific weapons systems, but also component interdependencies and enablers. Initiatives such as regional IAMD centers in U.S. Central Command, U.S. European Command, and the emerging USPACOM efforts are to be commended for filling the joint IAMD training void. But a more formalized joint training pipeline is necessary to train and track qualified joint IAMD-qualified personnel.

The JTAMD board would not be the panacea to complex missile defense planning and execution, but it would allow for deliberate and crisis-action planning processes to shape missile defense strategy in all phases of conflict. Much like the better known joint targeting coordination board and joint collection management board, the JTAMD board needs to mirror its importance in joint doctrine. The board has the potential to act as a leveler to bring the many facets of missile defense across the Defense Department and partner-nation staffs together. During peacetime operations, the JTAMD board should meet regularly; however, during exercise or contingency operations such as a North Korean provocation cycle, it could convene daily. In sum, the JTAMD board could serve as a much needed "nonmaterial" enabler for expensive air and missile defense systems to make them more complementary and effective. **JFQ**

Notes

[1] Martin E. Dempsey, *Joint Integrated Air and Missile Defense: Vision 2020* (Washington, DC: The Joint Staff, 2013).

[2] As of time of publication, records were as follows: Terminal High Altitude Area Defense (THAAD) had 13 tests/11 attempts/0 misses; Aegis had 29 tests/31 attempts/25 hits/6 misses; and Patriot PAC-3 had 24 tests/25 attempts/21 hits/4 misses.

[3] For more information on the Board, Bureau, Center, Cells Working Group process lessons learned, see Gary Luck, Mike Findlay, and the Joint Warfighting Center Joint Training Division, *Joint Operations Insights & Best Practices*, 2nd ed. (Norfolk, VA: U.S. Joint Forces Command, July 2008), 22.

[4] Andrew Feickert, *The Unified Command Plan and Combatant Commands: Background and Issues for Congress*, R42077 (Washington, DC: Congressional Research Service, January 3, 2013), 47.

[5] THAAD and Patriot (PAC-2 and PAC-3) conduct terminal defense (intercepting an inbound missile in the last phase of flight). The Patriot system intercepts ballistic missiles at endoatmospheric and exoatmospheric altitudes. Aegis ballistic missile defense ship and Aegis Ashore SM-3 missile intercepts occur solely exoatmospherically and are generally considered mid-course defense capabilities.

[6] Field Manual 3-01.94, *Army Air and Missile Defense Command Operations* (Washington, DC: Headquarters Department of the Army, April 2005), 3–9.

[7] Ashton Carter, Joint Ballistic Missile Defense Training Memorandum, August 26, 2012.

General Dempsey hosts question-and-answer session with Peter W. Singer, director of Center for 21st Century Security and Intelligence, in Washington, DC, June 2013 (DOD/Daniel Hinton)

Expanding Combat Power Through Military Cyber Power Theory

By Sean Charles Gaines Kern

We need a theory for cyberspace operations that will allow us to understand the implications of employing cyberspace capabilities at the tactical, operational, and strategic levels.[1]

—Major General Brett T. Williams, USAF

Military theory is a primary component of operational art. Early military theorists such as Alfred Thayer Mahan, Giulio Douhet, and B.H. Liddell Hart reasoned about the maritime, air, and land domains respectively, generating frameworks, models, and principles for warfare. Today, these theories help strategists and planners think about, plan for, and generate joint combat power. Unfortunately, no standard military theory for cyberspace operations exists, although elements for such a theory do. If a codified theory for military cyber power existed, it would greatly aid the joint force com-

Lieutenant Colonel Sean Charles Gaines Kern, USAF, is assigned to U.S. Cyber Command.

mander (JFC) in integrating cyberspace operations with joint operations, resulting in expanded combat power.

Although JFCs have many years of practical experience and military education in employing joint forces, they are not as experienced with cyberspace operations.[2] There is a lack of shared cyberspace knowledge and an agreed operational approach to link cyberspace missions and actions and place them in the larger context of joint operations.[3] Military cyber power theory is the foundation for such knowledge.

The JFC requires a cyberspace component commander who, through education and experience, has developed the requisite expertise to apply military cyber power theory at a level equivalent to his or her peers in the other domains. However, joint doctrine does not describe such a leadership role. Without the equivalent of a joint force cyberspace component commander (JFCCC), it is unlikely that the JFC would be able to effectively integrate cyberspace operations within the construct of joint operations. This results in a perpetual adjunct role for cyberspace operations and suboptimal combat power, as the Chairman of the Joint Chiefs of Staff himself noted as a key operational problem in the *Capstone Concept for Joint Operations: Joint Force 2020*.[4]

Toward a Preliminary Theory

The most challenging aspect of developing cyber operational art is devising a military theory for cyber power, which is essential for assessing the operational environment and making predictive judgments that will then guide strategy and plan development. By viewing the operational environment through the lens of military cyber power theory, the JFCCC will be in the position to provide his or her best military advice to the JFC, resulting in integrated cyberspace operation and expanded combat power.

A framework advances understanding and provides a basis for reasoning about the current and potential future environment by incorporating a number of elements. The framework identifies and defines key terms and structures discussion by categorizing the elements of the theory. It explains the categorized elements by summarizing relevant events and introducing additional frameworks and models. It allows the members of the cyber community to connect diverse elements of the body of knowledge to comprehensively address key issues. Finally, the predictive nature of the framework will enable the practitioner to anticipate key trends and activities to test the validity of the theory.[5] Although Major General Brett Williams called for a theory of cyberspace operations that addresses cyberspace operations at the strategic, operational, and tactical levels, the focus here is at the strategic and operational levels since the JFCCC's responsibility will be to translate strategic direction into operational plans.

Early cyber power theorists generally identified and defined three key terms: *cyberspace*, *cyber power*, and *cyber strategy*. Under the guise of military cyber power theory, this author offers four additional terms: *military cyber power*, *military cyber strategy*, *key cyber terrain*, and *military cyberspaces*.

Military cyber power is defined as the application of operational concepts, strategies, and functions that employ cyberspace operations (offensive cyberspace operations [OCO], defensive cyberspace operations [DCO], and Department of Defense [DOD] information network [DODIN] operations) in joint operations to expand combat power for the accomplishment of military objectives and missions.[6]

Military cyber strategy is defined as the development and employment of operational cyberspace capabilities integrated with other operational domain capabilities to expand combat power and accomplish the military objectives and missions of the JFC. These definitions reflect an emphasis on cyberspace operations mission areas and their contributions to joint operations and joint force combat power.

Given the pervasive and ubiquitous nature of the cyberspace domain and the fact that the military relies heavily on the commercial sector for interconnectivity, the concept of key terrain becomes especially critical in the context of military cyber power theory. *Key cyber terrain* forms the foundation from which the joint force preserves and projects military cyber power and represents the attack surface that adversaries would likely target. It is defined as any physical, logical, or persona element of the cyber space domain, including commercial services, the disruption, degradation, or destruction of which constricts combat power, affording a marked advantage to either combatant.

Defining cyberspace as a global domain suggests a homogeneity that does not exist in reality. There is not one cyberspace, but many cyberspaces.[7] These cyberspaces are in most cases interconnected by privately owned infrastructure. DOD has over 15,000 networks, or cyberspaces, interconnected by commercial infrastructure that the department does not own or control. This has two significant implications. First, unlike in other domains, the joint force is not solely capable of generating its required military cyber power; it relies on commercial services. Second, not all key cyber terrain will be under control of the joint force. For example, there is no current equivalent in cyberspace to the way in which the United States fully militarized its airspace immediately following the 9/11 terrorist attacks. Thus, *military cyberspaces* are defined as networks or enclaves wholly owned and operated by DOD, interconnected by means that are outside the control or direct influence of DOD.

With key terms identified and defined, military cyber power theory must conceptually consider the relationships of these terms as well as other relevant domain characteristics. The JFCCC must consider his or her efforts in the context of the three layers of cyberspace: physical, logical, and persona layers.[8] Figure 1 depicts the relationships between the terms (left) and the relation of the cyberspace layers in the context of the overall friendly or adversary attack surface (right).

Based on these relationships, the JFCCC can then conceptualize the weighted effort of the cyberspace operations mission areas. These operations comprise the ways and means for the JFCCC's cyber strategy and planning.

Figure 1. Elements of Military Cyber Power Theory and Cyberspace Domain Layers

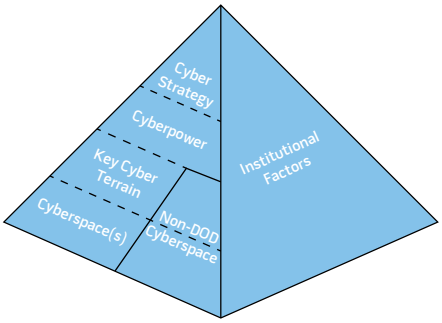


Figure 2. Weighted Effort for Cyberspace Operations

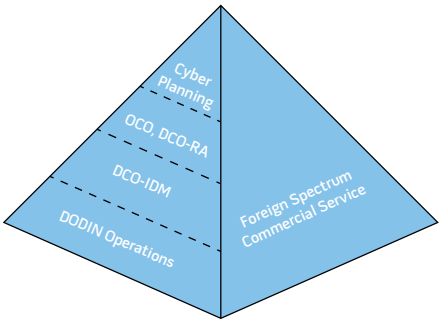


Figure 3. Cyber Adversary Characterization

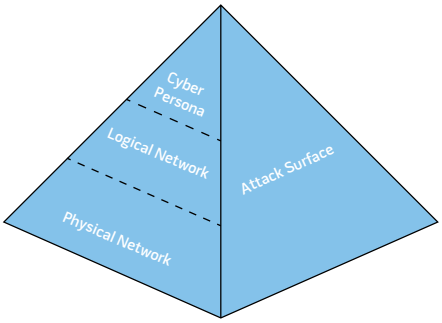
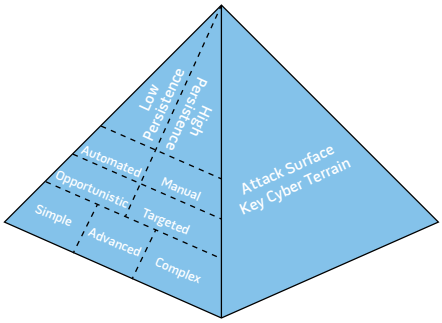


Figure 4. Cyber Kill Chain



The weighted effort, in priority order, would be DODIN operations, DCO–Internal Defense Measures (DCO-IDM), DCO–Response Actions (DCO-RA), and OCO (see figure 2).

The joint force conducts cyberspace operations, like all joint operations, with the adversary in mind. This leads to a final structured discussion to characterize cyberspace adversaries and conceptualize adversarial operational planning and execution. Ultimately, this discussion gives the JFCCC the framework to assess risks associated with generating combat power.

The JFCCC and staff assess cyberspace adversaries similar to adversaries in other domains in terms of intent and capability. It takes two types of capabilities in the cyberspace domain to conduct cyberspace operations: technical and analytical. *Analytical capability* refers to the ability to analyze a potential target to identify its critical nodes and vulnerabilities and potentially its connections to other targets. *Technical capability* refers to knowledge of computer software and hardware, networks, and other relevant technologies.[9] The JFCCC can further categorize cyber adversaries as simple, advanced, and complex, based in part on the scope and scale of operations and potential effects achieved.

In addition to being simple, advanced, or complex, military cyber power theory categorizes adversary operations as either opportunistic or targeted. The former is usually cybercrime-related, automated, and rarely attempts to maintain persistent presence. Targeted attacks are oriented against friendly key cyber terrain and are likely to be persistent and stealthy. In targeted attacks, cyber operators may be manually interacting with target systems. These categories are not mutually exclusive, as opportunistic attackers may gain access to high-value systems and in turn seek to sell access to these systems to adversaries seeking targeted access (for example, the nexus of cybercrime and state-sponsored cyber operations). Figure 3 shows the relationships among adversary capability, targeting type, and level of persistence.

Cyberspace adversaries share common strategic and operational concepts with adversaries in other domains, one of which is the concept of a kill chain. Conceptualizing a cyber kill chain enables the JFCCC to understand how the adversary plans and conducts cyber operations. The cyber kill chain depicted in figure 4 provides an excellent framework for the JFCCC to develop the appropriate strategy and corresponding operational plans to mitigate the adversarial threat. The ultimate goal is to detect and defend against the adversary as early as possible in the chain, ideally at or prior to the adversary developing access.

Military Cyber Power Principles

A theory of military cyber power includes principles that would inform the JFCCC's operational art. The true test of a theory is how well these principles hold over time. The principles examined here are not exhaustive and should serve as a foundation for future expansion of military cyber power theory.

Stealth and Utility. A cyberspace capability is effective as long as it can go undetected and exploit an open vulnerability. If the adversary detects the cyber capability or mitigates the targeted vulnerability, the cyber capability is perishable. These characteristics may drive the timing of cyber operations based on the perceived utility.[10]

Convergence, Consolidation, and Standardization. In peacetime, efficiency is valued over effectiveness. Core services are converging to Internet Protocol technologies. Smaller bandwidth network interconnections are converging to fewer massive bandwidth interconnections. DOD is consolidating data centers and Internet access points, resulting in streamlined, consolidated service architectures. DOD is also standardizing hardware and software. Convergence, consolidation, and standardization create an efficient, homogenous military cyberspace environment that reduces the DOD attack surface overall and better postures cyber defenders to preserve combat power. However, these efforts reduce system redundancy, limit alternative routes, and increase the number of chokepoints, making it easier for an

Joint Service and civilian personnel concentrate on exercise scenarios during Cyber Guard 2015 (DOD/Marvin Lynchard)

adversary to identify and target friendly key cyber terrain.

Complexity, Penetration, and Exposure. Systems are becoming increasingly complex by almost every measure. Higher complexity begets a growth in vulnerabilities. Internet penetration is expanding in terms of people and devices connected to cyberspace. People and organizations are integrating an increasing number of services delivered through cyberspace into their daily lives and operations, creating significant cyberspace exposure. Complexity, penetration, and exposure increase the attack surface by creating broader and deeper technical and process vulnerabilities, putting joint combat power at risk.

Primacy of Defense. History shows that militaries are prone to favor offensive operations.[11] Yet Colin Gray, Brett Williams, and Martin Libicki argue that DCO, not OCO, should be the JFC's primary effort in cyberspace. Since the joint force constructs cyberspace, Gray contends that cyberspace operators can repair the damage. Each repair hardens the system against future attacks. Offense can achieve surprise, but response and repair should be routine. Cyberspace defense is difficult, but so is cyberspace offense.[12] As systems are hardened, an attacker must exploit multiple vulnerabilities to achieve the same effect as compared to prior attacks that only required a single exploit.[13]

Speed and Global Reach. Cyberspace exhibits levels of speed and reach uncharacteristic of the other domains. Like other domains, cyberspace operations, especially offensive ones, require significant capability development, planning, reconnaissance, policy, and legal support prior to execution. However, once the JFC decides to act, cyberspace effects can be nearly instantaneous. The global cyberspace domain relegates geography to a subordinate consideration.

Arranging Operations. The *Joint Operational Access Concept* states that the critical support provided by cyberspace operations generally must commence well in advance of other operations as part of efforts to shape the operational area. Even in the absence of open conflict, operations to gain and maintain cyberspace superiority will be a continuous requirement since freedom of action in cyberspace is critical to all joint operations.[14] Chris Demchak offers a cautionary consideration, suggesting that if kinetic operations eventually take place, the United States may see the results of several decades of cyber "preparation of the battlefield," ranging from tainted supply chains to embedded malware.[15]

Resilience. Resilience is the ability to continue operations in a degraded cyber environment while mitigating quickly the impact of any attack. Much like the Quick Reaction Force construct in the physical domain, cyberspace operations require

robust DCO-IDM capacity oriented in support of friendly key cyber terrain to respond quickly to mitigate the effects of adversarial cyberspace operations. In concert with these DCO-IDM efforts, the total force will need to implement people, process, and technology measures, such as network minimize procedures or increasing bandwidth capacity, to continue to operate in the degraded environment.

Cyber-Physical Interface. To gain efficiencies, critical infrastructure owners and operators have increasingly connected their once-closed systems to the Internet. As a result, industrial control systems and supervisory control and data acquisition systems are increasingly easy to exploit. These systems are the two primary means for cyber adversaries to achieve direct physical effects through cyberspace.

Decision Integrity. Assuring integrity of operational information is essential to maintaining trust and confidence in the quality of decisionmaking, since making decisions based on wrong information could degrade joint combat power. Without a baseline of what is normal, it is impossible to discern if an adversary has made unauthorized changes to operational information. As Charles Barry and Elihu Zimet observe, "The possession of accurate and timely knowledge and the unfettered ability to distribute this as information have always been the sine qua non of warfighting."[16]

Speed, Not Secrets. Ninety-eight percent of all information is digitized.[17] Adversaries have proved adept at compromising and extracting information from closed networks. In this environment, how long is it reasonable to expect secrecy? The days of having a high degree of confidence that secrets will remain secure are fleeting. Overclassification exacerbates this problem and negatively affects key cyber terrain analysis. The joint force should place value on the ability to make decisions before the adversary compromises key information.

Strategic Attribution. From a strategic perspective, it may be more important to know "Who is to blame?" than "Who did it?"[18] This shift in perspective changes focus from technical attribution, which is difficult, to one of assigning responsibility to a nation-state—more pointedly, to national decisionmakers—for either ignoring, abetting, or conducting cyberspace operations against the United States, its allies, and key partners.

Increase Security, Decrease Freedom of Movement. In other domains, increased security usually implies greater freedom of movement and action. This same concept is not true for cyberspace since increased cybersecurity usually restricts options in cyberspace.

Scope and Scale of Effects. The most sophisticated cyber adversaries have the means to create a regional disturbance for a short period or a local disturbance for a sustained period.[19] The intelligence functions should continually assess the intent and capabilities of potential adversaries to predict the potential scope and scale of effects.

Increased Reliance on Commercial Services. U.S. Central Command's March 2014 posture statement noted the command is "heavily reliant on host nation communications infrastructure across the Central Region."[20] Whereas a JFC can easily partition and militarize the other domains into internationally and nationally recognized contiguous operational areas, cyberspace largely exists via private sector Internet service providers connecting national and military network enclaves.[21] The JFCCC will have to consider this dynamic when attempting to define his cyber joint operational area.

Perpetual, Ambiguous Conflict. Cyberspace is in a perpetual state of conflict that crosses geographic boundaries. Unlike the other domains where one can physically discern unambiguous threat indications and warning, operations in cyberspace are inherently ambiguous. Ambiguity can make war more or less likely. Timothy Junio suggests this is the case because ambiguity "may lead states to overestimate their potential gains, overestimate their stealth, and/or underestimate their adversary's skill."[22] Demchak warns that actions by nonstate actors could lead to unintended escalation as one state misinterprets the action or uses it as cover for its own actions.[23]

Cyber Intelligence. Cyber intelligence—scanning for things that just do not look right by sifting through chatter to discern patterns of intelligence—can become close to police work.[24] When DCO operators detect an adversary, it is difficult to assess adversarial intent. Is the adversary conducting reconnaissance, exfiltrating information, or instrumenting the network for a follow-on operation? A JFCCC must be able to assess cyber situational awareness beyond the joint operational area to understand fully the scope and scale of cyber risks to the theater of operations.

Centralized Control, Centralized Execution. Because any point in cyberspace is equidistant to any other, cyber forces are capable of deploying and surging virtually without the required mobilization time and physical proximity to theater operations. This characteristic is a contributing factor to the centralized control, centralized execution model employed by U.S. Cyber Command. This model affects the development of cyberspace experience across the joint force.

Precedence. There are currently no universally accepted norms of behavior in cyberspace. As such, employment of a cyberspace capability may result in a de facto precedence that other nation-states and nonstate actors may use as a barometer for how they may choose to act in cyberspace. Currently, some senior leaders view offensive cyberspace operations as a last resort, restricting the ability to develop cyberspace experience.

Uncertainty. Whereas the physical characteristics of the other domains are well understood and defined, cyberspace is a constantly changing, dynamic domain that is difficult to model due to its ubiquity and complexity. Unlike the precision of kinetic weapons, there is a level of doubt regarding the use of cyber capabilities in terms of understanding what effects cyber forces can achieve in cyberspace and assessing the success of cyberspace operations. This uncertainty is compounded by a lack of cyber experience and education in the senior ranks, thus creating a circle of uncertainty, reluctance to employ, and lost opportunities

Soldiers training with first fully immersive virtual simulation for infantry at 7th Army Joint Multinational Training Command in Grafenwoehr, Germany, December 2013 (U.S. Army/Markus Rauchenberger)

to gain cyber experience, leading to even greater uncertainty.

The combination of key terms, frameworks, and principles serves as a foundation for an evolving military cyber power theory, which serves as a building block to enhance both the explanatory and predictive power of the JFCCC's recommendations to the JFC. Application of the theory improves the soundness and timeliness of these recommendations. With expert understanding and application of this preliminary military cyber power theory, the JFCCC will be better prepared to provide the JFC recommendations to integrate cyberspace operations in joint operations to preserve and project joint combat power.

Cyberspace Operations as Combat Power

Practitioners validate military theory through application. A successful military theory expertly applied should result in increased combat power for the practitioner. Given the lack of cyberspace operations experience and education in the joint force, it may be difficult to consider how cyberspace operations could contribute to combat power. It does not help that joint doctrine is silent regarding the direct relationship between cyberspace operations and combat power.

Joint Publication (JP) 1-02, *Department of Defense Dictionary of Military and Associated Terms*, defines *combat power* as the total means of destructive and disruptive force that a military unit or formation can apply against an opponent at a given time.[25] The two key words are *destructive* and *disruptive*. Although JP 3-12(R), *Cyberspace Operations*, does not refer to combat power, it implies it by describing direct denial effects achieved through cyberspace attack, which include, in part, the ability to destroy and disrupt adversary targets. The primary doctrinal source for combat power is JP 3-0, *Joint Operations*, in which the JFC is the central focus.

The JFC seeks decisive advantage using all available elements of combat power to seize and maintain the initiative, deny the enemy the opportunity to achieve its objectives, and generate a sense of inevitable failure and defeat in the enemy.[26] Joint doctrine leaves the reader with a sense that there is a bias to operations and effects in the physical domains. For example, JP 3-0 discusses the relative combat power that military forces can generate in terms of delivering forces and materiel. It describes the roles of long-range air and sea operations as effective force projection when timely or unencumbered access to the area of operations is not available. It also

Vice Admiral Jan E. Tighe, commander of Fleet Cyber Command and commander of U.S. 10th Fleet, right, discusses educational requirements for cyber and course matrices that support those requirements (DOD/Javier Chagoya)

discusses combat power in the context of mass, maneuver, economy of force, and surprise. Like JP 3-12(R), JP 3-0 does not reference cyberspace operations in relation to combat power, although it does note that cyberspace superiority may enable freedom of action throughout the operational area. There is clearly an opportunity to link cyberspace operations and combat power in joint doctrine.

In addition to doctrinal references to combat power, the Chairman also publishes operational concepts that provide broad visions for how joint forces will operate in response to specific challenges. For example, the Chairman's *Joint Operational Access Concept* (JOAC) calls for cross-domain synergy to overcome emerging antiaccess/area-denial (A2/AD) challenges. Cross-domain synergy seeks to employ complementary capabilities in different domains such that each enhances the effectiveness and compensates for the vulnerabilities of others.[27] To this end, the JOAC specifically addresses the need for greater and more flexible integration of cyberspace operations into the traditional land-sea-air battlespace. It identifies two combat power–related tasks required to gain and maintain access in the face of armed opposition. The first is overcoming the enemy's A2/AD capabilities through the application of combat power. The second is moving and supporting the necessary combat power over the required distances. Cyberspace operations play a critical role in accomplishing both of these tasks. Fifteen of the 30 capabilities required in the concept are either directly or indirectly associated with the conduct of cyberspace operations, with significant requirements in command and control, intelligence, and fires capabilities. The A2/AD challenge is an excellent operational problem to validate and expand the preliminary military cyber power theory discussed herein.

Conclusion

Stanley Baldwin asserted in 1932 that the "bomber will always get through." History has shown that he was wrong. However, the adoption of this theoretical airpower perspective did drive acquisition, organization, and doctrine leading into World War II. Cyberspace operations share some similarities with the interwar years. Much remains undetermined about the role of cyberspace operations in joint operations and their impact on joint combat power. Yet there are historic examples, key trends, and operational problems that call for increased attention to the need for a military cyber power theory and, consequently, the need for updates to doctrine, organization, and education to inculcate the military cyber power principles presented here.

The Joint Staff should update doctrine to reflect the growing importance of effectively integrating cyberspace operations in joint operations to expand joint combat power. It should update JP 3-12(R) to reflect the need for a JFCCC and incorporate aspects of the preliminary military cyber power theory presented here. Likewise, the Joint Staff should update JP 3-0's description of combat power to broaden and deepen the relationship between cyberspace operations and combat power. Moreover, professional military education and advanced studies programs should include military cyber power theory in the curricula and challenge students to conduct research to evolve the theory.

Organizationally, the JFC should designate a JFCCC for most task force operations. However, depending on the forces assigned, it may be difficult for the JFC to identify a JFCCC candidate that has the preponderance of cyber forces and the best means to command and control those cyber forces. Furthermore, organizations that must address A2/AD in their strategies and operational plans should conduct extensive exercises with a heavy emphasis on cyberspace capabilities.

With expert understanding and application of military cyber power theory, the JFCCC is poised to develop strategic and operational recommendations for the JFC to integrate and synchronize cyberspace operations in joint operations and achieve expanded combat power. The need for integrated cyberspace operations and its contribution to joint combat power is clearly illustrated in one of the most significant operational challenges the joint force will likely face in the future, which is gaining and maintaining operational access in the face of enemy A2/AD capabilities.

The *Joint Operational Access Concept* notes three trends in the operating environment that will likely complicate the challenge of opposed access, one of those being the emergence of cyberspace as an increasingly important and

contested domain. The implication is that the JFCCC and his staff are becoming ever more central in assisting the JFC in generating combat power to disrupt, degrade, and defeat enemy A2/AD capabilities. If the joint force is going to be successful in future advanced A2/AD operations, the JFC must fully integrate cyberspace operations into joint operations. A prerequisite for success is the designation of a JFCCC with the requisite professional development, to include expert understanding of and experience applying military cyber power theory. JFQ

Notes

[1] Brett T. Williams, "The Joint Force Commander's Guide to Cyberspace Operations," *Joint Force Quarterly* 73 (2nd Quarter 2014), 12–20.

[2] Brett T. Williams, "Ten Propositions Regarding Cyberspace Operations," *Joint Force Quarterly* 61 (2nd Quarter 2011), 11–17.

[3] Williams, "The Joint Force Commander's Guide."

[4] *Capstone Concept for Joint Operations: Joint Force 2020* (Washington, DC: The Joint Staff, September 10, 2012), 7, available at <www.dtic.mil/doctrine/concepts/ccjo_jointforce2020.pdf>.

[5] Stuart H. Starr, "Toward a Preliminary Theory of Cyberpower," in *Cyberpower and National Security*, ed. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Washington, DC: National Defense University Press/Potomac Books, Inc., 2009), 43–90.

[6] Adapted from Elihu Zimet and Charles L. Barry, "Military Service Overview," in *Cyberpower and National Security*, 285–308.

[7] Colin Gray, *Making Strategic Sense of Cyber Power: Why the Sky Is Not Falling* (Carlisle Barracks, PA: U.S. Army War College, April 2013).

[8] Joint Publication (JP) 3-12(R), *Cyberspace Operations* (Washington, DC: The Joint Staff, February 5, 2013).

[9] Irving Lachow, "Cyber Terrorism: Menace or Myth?" in *Cyberpower and National Security*, 437–464.

[10] Robert Axelrod and Rumen Iliev, "Timing of Cyber Conflict," *Proceedings of the National Academy of Science* 111, no. 4 (January 28, 2014), available at <www.pnas.org/content/111/4/1298.abstract>.

[11] Timothy J. Junio, "How Probable Is Cyber War? Bringing IR Theory Back into the Cyber Conflict Debate," *Journal of Strategic Studies* 36, no. 1 (February 2013).

[12] Gray.

[13] Kim Zetter, *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon* (New York: Crown Publishing, 2014).

[14] *Joint Operational Access Concept* (Washington, DC: The Joint Staff, January 17, 2012).

[15] Peter Dombrowski and Chris C. Demchak, "Cyber War, Cybered Conflict, and the Maritime Domain," *Naval War College Review* (April 2014), available at <www.readperiodicals.com/201404/3271362101.html>.

[16] Zimet and Barry.

[17] Joel Brenner, *America the Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare* (New York: Penguin Press, 2011).

[18] Jason Healey, *Beyond Attribution: Seeking National Responsibility for Cyber Attacks*, Issue Brief (Washington, DC: The Atlantic Council, 2011), available at <www.fbiic.gov/public/2012/mar/National_Responsibility_for_CyberAttacks,_2012.pdf>.

[19] Armed Forces Communications and Electronics Association 2013 Spring Intelligence Symposium, available at <www.afcea.org/events/globalintelforum/13/welcome.asp>.

[20] *Commander's Posture Statement* (Tampa, FL: U.S. Central Command, March 5, 2014), available at <www.centcom.mil/en/about-centcom-en/commanders-posture-statement-en>.

[21] *Capstone Concept for Joint Operations.*

[22] Junio, 125–133.

[23] Chris Demchak and Peter Dombrowski, "Cyber Westphalia: Asserting State Prerogatives in Cyberspace," *Georgetown Journal of International Affairs* (Special Issue 2013).

[24] Mark Lowenthal, *Intelligence: From Secrets to Policy*, 5th ed. (Washington, DC: Sage Press, 2013). This is adapted from Lowenthal's description of the intelligence challenge posed by terrorism.

[25] JP 1-02, *Department of Defense Dictionary of Military and Associated Terms* (Washington, DC: The Joint Staff, November 15, 2014).

[26] JP 3-0, *Joint Operations* (Washington, DC: The Joint Staff, August 11, 2011).

[27] *Joint Operational Access Concept, Version 1.0* (Washington, DC: Department of Defense, January 17, 2012), foreword.

British battleship HMS *Irresistible* abandoned and sinking, having been shattered by explosion of floating mine in Dardanelles during attack on Narrows' Forts, March 18, 1915 (Royal Navy/Library of Congress)

The Gallipoli Campaign

Learning from a Mismatch of Strategic Ends and Means

By Raymond Adams

World War I began on July 28, 1914, 1 month after the assassination of Archduke Franz Ferdinand, heir-apparent to the Austro-Hungarian throne.[1] Most Europeans expected the conflict to be short—"over by Christmas" was a common refrain—and relatively inexpensive in terms of blood and treasure. Almost immediately, however, the combatants faced each other in a long line of static defensive trenches. The Western Front quickly became a killing ground of unprecedented violence in human history: combined British, French, and German casualties totaled 2,057,621 by January 1915.[2]

The character of war had changed. Armies had not changed their battlefield tactics in response to new, highly destructive weapons, resulting in massive casualties. Rising calls from British political leaders, the media, and the public demanded action to break the stalemate. British strategists responded by opening a new front in the east with two strategic objectives: drive Turkey out of the war by attacking Constantinople, and open a route to beleaguered ally Russia.[3] The decision to open a second front in the

Lieutenant Colonel Raymond Adams, USMCR, is a student at the National War College.

east in 1915 ultimately failed to achieve Britain's strategic objectives during the first full year of World War I. British leaders pursued short-term, politically expedient military objectives in Turkey that were both ancillary to their military expertise and contrary to achieving the overall ends of winning the war by defeating Germany. This article examines the disastrous results of the attempt to open a second front and the disconnect between Allied strategic ends and means.

Genesis of the Dardanelles Decision

With combat in France and Belgium characterized by hopeless direct assaults on entrenched enemy positions, British strategists began planning for a new direction.[4] First Lord of the Admiralty Winston Churchill contemplated amphibious operations in the North Sea to increase pressure on Germany. He proposed a joint Anglo-French amphibious assault along the Belgian coast designed to outflank German positions on the Western Front, liberate the port of Zeebrugge, and prevent Germany from using Zeebrugge and Ostende as submarine bases.[5] Ultimately, the British failed to convince the French to participate, effectively scuttling Churchill's North Sea plan.

British political and military leaders next focused attention on Turkey and the possibility of military operations to seize the Dardanelles,[6] attack Constantinople, and open a line of communication to Russia. Secretary of the War Cabinet Maurice Hankey, Chancellor of the Exchequer David Lloyd George, and Churchill advocated military operations against Turkey on the Gallipoli Peninsula.[7] They agreed that the Ottoman Empire was weak and that "Germany [could] perhaps be struck most effectively, and with the most lasting results on the peace of the world through her allies, and particularly through Turkey."[8] Thus, within weeks of the outbreak of war, British attention turned east.

At the end of August 1914, Churchill formally requested that Secretary of State for War Field Marshal Herbert Kitchener organize a group of naval and military officers to plan for the seizure of the Gallipoli Peninsula, "with a view to admitting a British Fleet to the Sea of Marmara" and eventually knocking Turkey out of the war.[9] Representatives of the War Office and the Admiralty met and concluded that an attack on the Gallipoli Peninsula was not a militarily feasible operation.[10] Director of Military Operations Major General Charles Callwell[11] presciently observed that a campaign in Gallipoli was "likely to prove an extremely difficult operation of war."[12] He proffered that an operation in the Dardanelles would require a force of not less than 60,000, with strong siege artillery, echeloned into Turkey in two large waves.[13] Kitchener also disagreed with opening a second front, but for different reasons. He was reluctant to divert troops from the continent, which he viewed as the primary focus of effort for the British.

A dichotomy of opinion thus emerged: the politicians advocated for a second front on the Gallipoli Peninsula, while senior military officers argued against intervention in Turkey.[14] The debate continued into winter. The dynamic changed on January 1, 1915, when Russia formally requested a "naval or military demonstration against the Turks to ease the pressure caused by the Turkish offensive driving through the Caucasus Mountains."[15] British decisionmakers debated the Russian request and the larger issue of the future strategic direction of the war effort during a series of War Council meetings in early January.[16] The council decided that the British would continue to fight side by side with France on the Western Front, and the Admiralty would, commencing in February 1915, prepare operations "to invade and take the Gallipoli Peninsula, with Constantinople as its objective."[17]

Bureaucratic maneuvering and negotiation were thus necessary to reach a decision to launch the operation. The next major task for senior British leaders was designing the strategy to implement the War Council's decisions. The final plan would call for a combined force of six British and four French battleships, accompanied by a substantial naval escort, to push through the Dardanelles and fight to Constantinople.[18]

Flawed Assumptions Underpinning the British Strategy

The British designed their Dardanelles plan on a series of faulty assumptions. Political leaders and military planners alike assumed the Turks were deficient in martial skill, grit, and determination.[19] Churchill displayed unbridled confidence in the ability of naval bombardment to destroy land targets.[20] British war planners assumed that the battle fleet would easily breach the enemy's coastal defenses, float directly to Constantinople, and seize the straits without requiring a landing force. Kitchener assumed that, once through the straits, with naval guns pointing at Constantinople, the fleet would "compel Turkey's capitulation, secure a supply route to hard-pressed Russia, and inspire the Balkan states to join the Allied war effort and eventually to attack Austro-Hungary, thereby pressuring Germany."[21]

Kitchener further assumed that once news of the arrival of the British fleet reached Constantinople, the entire Turkish army in Thrace would retreat, leaving Turkey to British control.[22] Sir Edward Grey, Secretary of State for Foreign Affairs, argued that once the fleet moved through the Dardanelles, "a *coup d'état* would occur in Constantinople, whereby Turkey would abandon the Central Powers and join the Entente."[23] All of the foregoing assumptions proved false, and their cumulative effect foreordained the Dardanelles operation to disaster.

Naval Operations in the Dardanelles

British naval forces shelled the forts at the entrance of the Dardanelles on November 1, 1914, well before the formal commencement of the Gallipoli campaign. The purpose of the attack was more to punish Turkey for siding with the Triple Alliance than an attempt to secure the strait. The shelling had a more pernicious effect, alerting the Turkish defenders that a future military operation in the Dardanelles by the British was likely. Mustafa Kamal

Australian troops charging near Turkish trench, just before evacuation at Anzac, ca. 1915 (U.S. National Archives and Records Administration)

Attaturk, overall Turkish commander at Gallipoli, and Otto Liman von Sanders, a German general and military advisor to Turkey, focused on fortifying the Dardanelles after the British attack of November 1.[24] The Anglo-French naval force attacked the Dardanelles in force on March 18, 1915. The battle initially favored the attackers. Naval bombardment in the days preceding the assault successfully destroyed several Turkish defensive positions at the entrance to the straits.[25] By midday, the British fleet neutralized most of the Turkish mines at the mouth of the Dardanelles, leaving nine more mine belts in the approach to Constantinople.[26] The Clausewitzian concept of chance in war then emerged. The fleet approached an undetected line of 20 mines, which a Turkish steamer had laid just 10 days earlier.[27] Three Allied warships struck mines and sank; a fourth suffered severe damage and was unsalvageable.[28] The assumption that the Turks would surrender on sight of the British naval force was incorrect, and the prospect of a collapse of the Ottoman Empire by means of a naval assault alone died on March 18. The setback caused the British War Council to delay further naval action immediately.

The council charted a new course and called for landing troops in a beach-hopping campaign from the Aegean to the Sea of Marmara, eventually attacking Constantinople.[29] However, 38 days would pass before British commanders were able to embark, transport, and land military forces on the peninsula. In the interim, the enemy seized the initiative. Turkey deployed six divisions, some 500 German advisors, and civilian labor units in a hurried effort to strengthen Gallipoli's defenses in anticipation of the next round of fighting.

Amphibious Landings on Gallipoli

The British did not reassess their strategic objective of defeating Turkey and opening a line of communication with Russia after the failure of the naval attack. In fact, the historical record shows just the opposite: British leaders redoubled their efforts, eventually committing nearly 500,000 Allied forces to the Gallipoli operation. Kitchener appointed General Sir Ian Hamilton as the overall commander of a combined force of British, Australian, New Zealander, and French troops. Hamilton faced a challenge of epic proportions. His task was to conduct the first opposed amphibious landing in an era of high-powered defensive weapons that included innovations such as the machine gun and highly accurate artillery firing a new generation of high explosives.[30]

At dawn on April 25, 1915, British, Dominion, and Allied forces waded ashore onto six landing beaches at Cape Helles.[31] Amphibious operations continued for 8 months, but the Allies never gained more than a foothold on the peninsula. The campaign to outflank the stalemate on the Western Front ironically began to resemble the fighting in France and Belgium, although on a much smaller scale, with Hamilton committing his troops against an entrenched and forewarned foe at Gallipoli.[32] Although Kitchener and Hamilton recognized that a central assumption about the Turks—that they were a second-rate fighting force that did not stand a chance against British arms—was clearly wrong, they did not change course.[33] In fairness to British military commanders, a major reason for continuing the operation was political expediency.[34] David Fromkin observes, "Constantinople and the Dardanelles, because of their world importance for shipping, and eastern Thrace, because it is in Europe, were positions that occupied a special status in the minds of British leaders."[35] As Churchill further argued, "the line of deep water separating Asia from Europe was a line of great significance, and we must make that line secure by every means within our power."[36]

Despite the perceived importance of the region to British war aims, the Allies withdrew from the peninsula on January 9, 1916, dashing hopes of defeating Turkey and reaching the Russians. British, Australian, New Zealander, and French casualties totaled 130,000, yet the operation achieved none of the goals set by British political leaders.

Mismatch of Ends and Means

The British experience in the Dardanelles is a cautionary tale that highlights the flaws inherent in a strategy charac-

terized by improperly aligned ends and means.[37] The initial plan—a navy-only effort to forcibly enter the Dardanelles, navigate the peninsula while destroying land-based targets with surface fires, and force the capitulation of Constantinople—is perhaps the classic example of imbalanced ends and means in World War I. Naval gunfire in 1915 was generally ineffective against land-based artillery and even static targets without ground-based spotters.[38] Although the fleet had limited success in the opening days of the naval operation, decisively defeating Turkish defensive positions in the 35-mile-long strait with naval guns alone was not feasible. Furthermore, ships are by definition incapable of taking land and occupying terrain. In fact, neither Kitchener nor Hamilton had any sustainable plan to seize and hold terrain in March 1915.

Another example of mismatched ends and means occurred in the minesweeping phase of the first attack in Gallipoli. The Allied fleet "applied its least capable set of assets, that of fishing trawlers turned minesweepers manned by civilian crews, against the most difficult part of the campaign, that of clearing mines under fire."[39] Even the amphibious landings of April 25 lacked properly balanced ends and means. A total of five British, French, and Commonwealth divisions landed at five separate beaches against entrenched defenders expecting an Allied attack.[40] Although the number of forces in action in the Dardanelles consistently grew during the evolution of the operation, the fact remains that the Allies never successfully held a beachhead for an extended period, largely due to the lack of means, that is, ground forces.

Another imbalance in the ends-means paradigm was evident in British command and control. Inadequate command and control

handicapped Hamilton throughout the campaign, but was especially evident during the first, crucial days of the landing. Hamilton monitored the landing from aboard the Queen Elizabeth. . . . [However]*, the* Queen Elizabeth *was not configured as a headquarters for an amphibious task force. As a result, Hamilton's staff, what could be fitted aboard the* Queen Elizabeth*, was squirreled away throughout the ship.*[41]

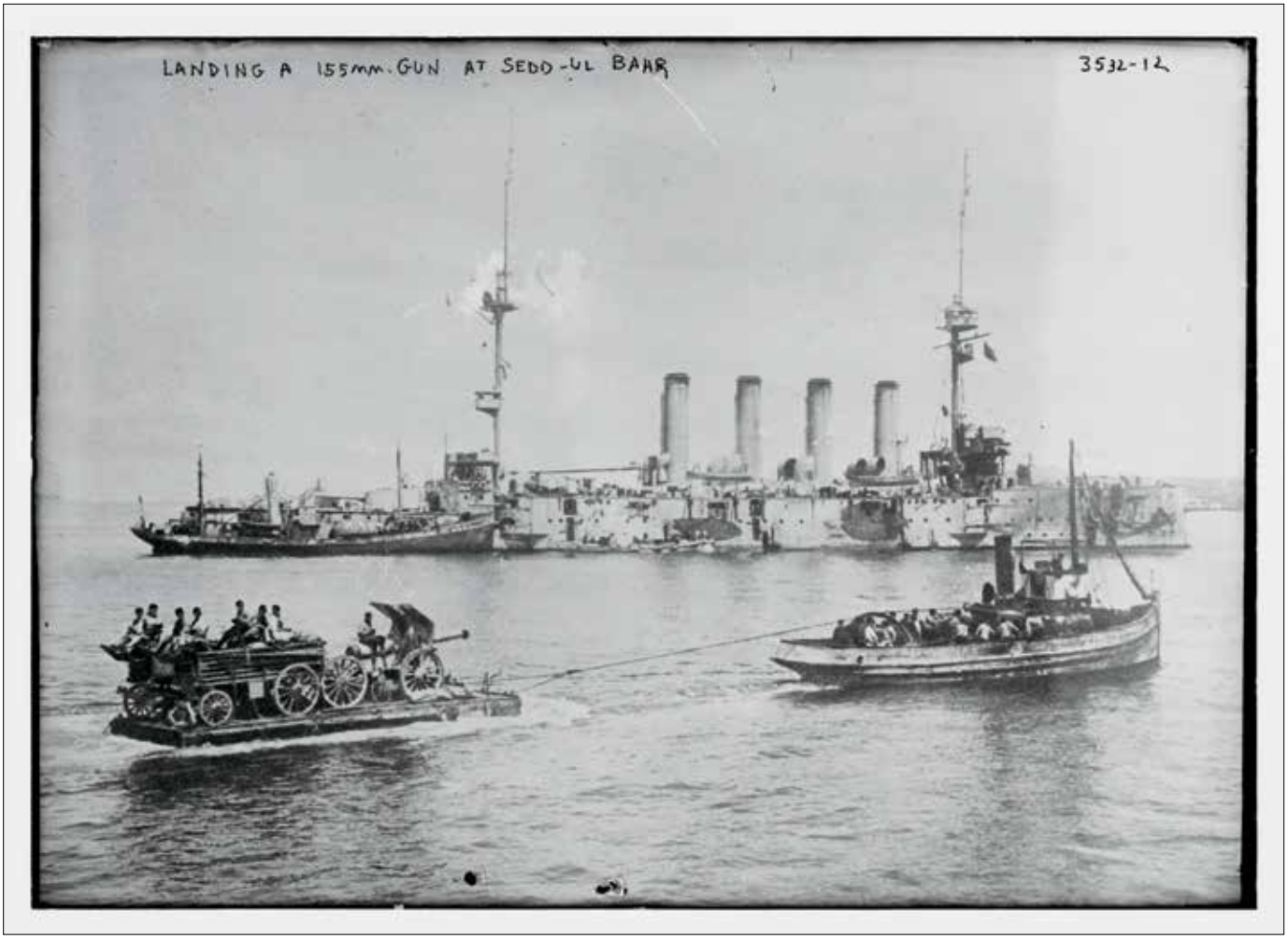
Ottoman soldiers and guns during Gallipoli campaign (Library of Congress)

The commander of one of the largest, most complex amphibious assaults in history was thus virtually powerless to exert his will over his own forces, let alone those of the enemy. Without the means to command and control a complex military operation, the ends were all but unattainable.[42] A lack of two further means—amphibious doctrine and previous army-navy joint training—also hindered Hamilton's ability to orchestrate the landings.[43] The Clausewitzian concept of friction, compounded by the lack of command and control, amphibious doctrine, and previous army-navy training, took effect on the battlefield almost immediately. The historical record is replete with first-hand accounts of problems exacerbated by weak command and control. An Australian soldier succinctly described a frustrating scene undoubtedly unfolding for thousands of men during the Gallipoli campaign: "Battalions dissolved into separated groups of men, some making marvelous progress but without possibility of any support. It was this and the strengthening Turkish resistance which led to the disturbing lack of confidence by commanders, who felt that the men should be evacuated."[44]

Helmuth von Moltke the Elder, chief of the Prussian General Staff from 1857 to 1887, observed, "Strategy can direct its efforts only toward the highest goal that the available means make practically possible."[45] British means in the Gallipoli campaign did not support British strategy. The imbalance between ends and means in the naval and ground campaigns in the Dardanelles doomed the overall effort to failure.

Conclusion

The changing character of war, embodied in the deadly intersection of 19th-century tactics and 20th-century weapons, created a staggering number of casualties in 1914. The carnage prompted British leaders to seek a new front to break the European stalemate. Strategists looked east to open a new theater of war. The plan to conduct operations against Turkey and open a route to Russia suffered from flawed assumptions, which led first to an ill-advised, naval-only attack in the Dardanelles. Six weeks later, this time without the element of surprise, the Allies attacked again. The second round



Warships near Gallipoli Peninsula landing 155-mm gun at Sedd-ul Bahr (Library of Congress)

featured a larger naval fleet with an embarked landing force of five divisions. A series of amphibious landings over the next 8 months, however, failed to gain anything more than a foothold for the Allies. The British lacked the means to achieve the desired ends in the Dardanelles, particularly in the command and control, doctrinal, training, and manpower realms. The Allies ultimately failed in their attempt to seize the Dardanelles, force Constantinople's surrender, and open a link with their Russian ally. In the final analysis, a flawed strategy, poorly executed, did not achieve Allied ends.[46]

Coda: Lessons Learned on Amphibious Assault

The Dardanelles campaign was a disaster for Great Britain. Amphibious assaults against defended beachheads, among the most challenging of military operations, were widely considered impossible after the failed Gallipoli landings. The seemingly overwhelming challenges presented by amphibious assaults—in command and control, amphibious operations doctrine (or lack thereof), interservice coordination, and maintaining a beachhead after landing—convinced military and political leaders of the futility of operational maneuver from the sea. However, as Clausewitz observed, "Historical examples clarify everything and also provide the best kind of proof in the empirical sciences. This is particularly true in the art of war."[47]

During the interwar years, military planners and theorists validated the Clausewitzian concept of the value of studying history. Planners and theorists analyzed the reasons for the failure in the Dardanelles and developed doctrine, conducted exercises, and structured forces to overcome the problems associated with successfully assaulting fortified coastal defensive positions. A generation after Gallipoli, the Allies successfully landed tens of thousands of troops on beaches defended by entrenched and well-equipped German and Japanese forces. Allied amphibious operations in North Africa, Europe, and the Pacific were instrumental in the combined effort to defeat Nazism and Japanese imperialism.

Another lesson to emerge from Gallipoli, despite failure there, was the importance of the indirect approach, which factored heavily into British strategy during World War II. Churchill favored amphibious operations against Germany in the North Sea in 1914 in an effort to bypass the main line of resistance on the Western Front. Less than three decades later, Churchill opposed

the U.S.-favored Operation *Roundup*, a cross-channel attack planned for mid-1942. The prime minister instead advocated for operations in North Africa, Italy, and the Balkans—presumably softer targets than Adolf Hitler's Atlantic Wall—before a cross-channel assault against Fortress Europe.

Finally, Churchill personifies the greatest legacy of the Gallipoli campaign. A primary architect of the Dardanelles disaster, he managed to salvage his reputation and career after Gallipoli, and emerged as one of the most effective war leaders in history during World War II. The lessons of Gallipoli, learned at great cost in blood and materiel, were thus not in vain. **JFQ**

Notes

[1] Germany, Austria-Hungary, and Italy forged the Triple Alliance in May 1882. France, Britain, and Russia formed the Triple Entente in 1907 in an attempt to balance the growing German threat as Berlin's economy and military grew in the early 20th century. Members of the Triple Alliance were bound to defend each other through force of arms; Triple Entente members had a "moral obligation" to defend each other. A critical event occurred on August 2, 1914, when the Ottoman Empire signed a secret treaty joining the Triple Alliance. See Hew Strachan, ed., *The Oxford Illustrated History of the First World War* (Oxford: Oxford University Press, 2000), 10–11; U.S. Department of State, *Catalogue of Treaties: 1814–1918* (Washington, DC: Government Printing Office, 1919), 11; "The Road to War: The Triple Entente," BBC Schools, available at <www.bbc.co.uk/schools/worldwarone/hq/causes2_01.shtml>.

[2] *Statistics of the Military Effort of the British Empire during the Great War* (London: His Majesty's Printing Office, 1922), 237–252.

[3] Russia suffered stinging losses soon after the outbreak of hostilities, particularly in the Battle of Tannenberg against Germany. The British feared a Russian collapse and thus sought to relieve pressure on the tsar by attacking through the Dardanelles to reach Russia.

[4] David Fromkin, *A Peace to End All Peace: The Fall of the Ottoman Empire and the Creation of the Modern Middle East* (New York: Henry Holt and Company, 1989), 124.

[5] Ibid.

[6] The Dardanelles Strait is 35 miles in length. The entrance is 2.5 miles wide. It extends for 4 miles in a northeasterly direction, widens to a maximum width of 4.5 miles, and then narrows to less than a mile. The narrows extend for 4 miles, then widen again to 3 miles. They continue for another 20 miles before entering the Sea of Marmara. This geographic information is from Victor Rudenno, *Gallipoli: Attack from the Sea* (New Haven: Yale University Press, 2008), 27.

[7] Fromkin, 125.

[8] Ibid.

[9] Graham T. Clews, *Churchill's Dilemma: The Real Story Behind the Origins of the 1915 Dardanelles Campaign* (Westport, CT: Praeger, 2010), 44.

[10] Ibid.

[11] Charles E. Callwell was an influential military theorist. He published a seminal work on counterinsurgency titled *Small Wars: Their Principles and Practice* (London: His Majesty's Stationery Office, 1899).

[12] Trumbull Higgins, *Winston Churchill and the Dardanelles: A Dialogue in Ends and Means* (New York: Macmillan, 1963), 57.

[13] Ibid.

[14] Fromkin, 127, observes, "The doctrine of the generals was to attack the enemy at his strongest point; that of the politicians was to attack at his weakest." This "politicians' predilection" for attacking at the enemy's weakest point would surface again in World War II.

[15] Peter Hart, *Gallipoli* (New York: Oxford University Press, 2011), 14.

[16] Ibid., 16.

[17] As quoted in ibid.

[18] Martin Gilbert, *A History of the Twentieth Century, Volume One: 1900–1933* (New York: Avon Books, 1997), 63.

[19] Hart, 22.

[20] Clews, 37.

[21] Gilbert, *A History of the Twentieth Century*, 363.

[22] Ibid.

[23] Ibid.

[24] Rudenno, 12–13.

[25] Martin Gilbert, *The First World War: A Complete History* (New York: Henry Holt and Company, 1994), 136.

[26] Gilbert, *A History of the Twentieth Century*, 365.

[27] Gilbert, *The First World War*, 136.

[28] Clews, 275.

[29] Gilbert, *A History of the Twentieth Century*, 365.

[30] Hart, 171.

[31] Fromkin, 157. The historical record is replete with accounts of heroism and suffering on both sides. However, a detailed account of the fighting at the tactical level is not within the scope of this article.

[32] Ibid., 561.

[33] The concept of sunk cost applies in the Gallipoli campaign. The theory behind the sunk cost concept is that in a failing endeavor, such as Gallipoli, the decisionmaker justifies continued expenditure in an effort to recoup past losses.

[34] British decisionmaking in the Gallipoli campaign is a classic example of the Rubicon theory of war. Under this theory, "when people believe they have crossed a psychological Rubicon and perceive war to be imminent, they switch from what psychologists call a 'deliberative' to an 'implemental' mind-set, triggering a number of psychological biases, most notably overconfidence." This theory helps explain why, even when the commanders realized their central assumptions about Gallipoli were wrong, British political and military leaders made no change in the overall course of the Dardanelles strategy. Information concerning the Rubicon theory of war is from Dominic D.P. Johnson and Dominic Tierney, "The Rubicon Theory of War: How the Path to Conflict Reaches the Point of No Return," *International Security* 36, no. 1 (Summer 2001), 7–40.

[35] Fromkin, 548–549.

[36] As quoted in ibid., 549.

[37] Carl von Clausewitz devoted a significant amount of discussion to the importance of properly linking ends and means in strategy. See Carl von Clausewitz, *On War*, trans. and ed. Michael Howard and Peter Paret (Princeton: Princeton University Press, 1984), 127–147, et seq.

[38] Jonathan Schroden, "Strait Comparison: Lessons Learned from the 1915 Dardanelles Campaign in the Context of a Strait of Hormuz Closure Event," Center for Naval Analyses, September 2011, available at <www.history.navy.mil/research/library/online-reading-room/title-list-alphabetically/s/strait-comparison-lessons-learned-from-1915-dardanelles-campaign.html>.

[39] Ibid.

[40] Philip J. Haythornthwaite, *Gallipoli, 1915: Frontal Assault on Turkey*, Osprey Military Campaign Series 8 (London: Osprey, 1991), 45.

[41] Gregory A. Thiele, "Why Did Gallipoli Fail? Why Did Albion Succeed? A Comparative Analysis of Two World War I Amphibious Assaults," *Baltic Security and Defence Review* 13, no. 2 (2011), 139.

[42] The ends were successful penetration of the Dardanelles, landing and sustaining assault forces on well-defended beaches, and forcing the surrender of the capital city of an empire.

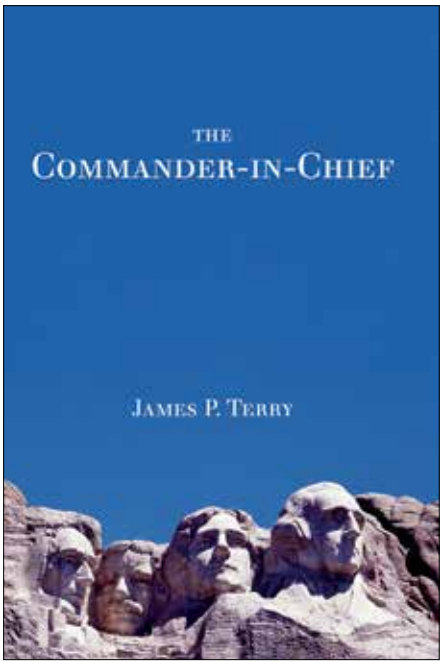
[43] Thiele, 150.

[44] Peter H. Liddle, *Gallipoli 1915: Pens, Pencils and Cameras at War* (London: Brassey's Defence Publishers, Ltd., 1985), 45.

[45] Grand [German] General Staff, trans. A.G. Zimmerman, *Moltke's Military Works: Precepts of War* (Newport, RI: U.S. Naval War College, 1935), Part II, 1.

[46] Churchill lost his post as the First Lord of the Admiralty and Hamilton lost his command in the aftermath of Gallipoli. The conclusions of the Gallipoli Commission, which inquired into the circumstances of the failed military operation, are available at <www.nationalarchives.gov.uk/ pathways/firstworldwar/transcripts/battles/dardanelles.htm>.

[47] Clausewitz, 170.



The Commander-in-Chief

By James P. Terry
Carolina Academic Press, 2015
204 pp. $40
ISBN: 978-1611636710
Reviewed by Alice A. Booher

James P. Terry long wore the mantle of being one of the most prolific writers in the areas of security and international law. In 2013 and 2014, his books *The War on Terror* and *Russia and the Relationship Between Law and Power* were recognized as providing articulate, extraordinary analyses of both subjects. *The Commander-in-Chief* is certainly equal to these two works and, in some ways, is better than both. Terry's lifelong body of work was a product reflective of extraordinary academic credentials, hands-on service in the Marine Corps, both on the ground and as Legal Counsel to the Chairman of the Joint Chiefs of Staff, and senior leadership roles at the Departments of State and Veterans Affairs. At the time of his death on December 12, 2014, Terry, a Senior Fellow in the Center for National Security Law at the University of Virginia, had signed off on this book, which was published posthumously.

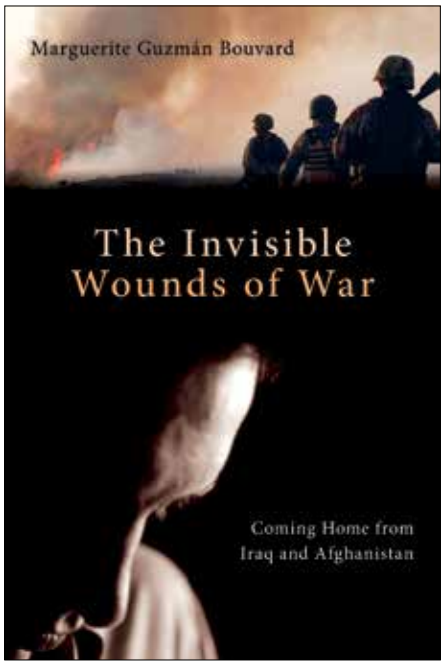
The Commander-in-Chief is a honed, expanded version of Terry's article "The President as Commander in Chief," which was published in the *Ave Maria Law Review* (2009). There is generous citing of independent collateral sources as well as of Terry's 30 years of earlier scholarly works, making broadened references easily accessible. The index and particularly the extensive bibliography and sources sections are immensely productive.

Terry's fundamental initial focus is the constitutional source of Presidential authority found in Article II with incremental expansion and limitations thereof guided by the Presidents themselves and the specific exigencies in which they discovered themselves, within and sometimes without the added dictates and directives of Congress and the courts. With text addressing both authority and execution, the fully comprehensive yet concise discussion of the warfighting Presidents in the aggregate is contained in the first five chapters, followed by foci on Presidential powers used in response to terrorism, humanitarian crises, United Nations peacekeeping, and in defense of U.S. nationals abroad in chapters 6 through 9.

Terry next gives consideration to Presidential powers in "protecting critical infrastructure" in circumstances such as electrical blackouts, protection of water supply, and actions post-9/11, post–Hurricane Katrina, and so forth, including establishment of the Department of Homeland Security and the strengthened review on cyber security. A final discussion relates to arms control. Each President and impacting elements and actions are addressed with remarkable objectivity in a context virtually absent any political "spin" other than learned analyses.

A eulogy written by national security expert Professor Robert Turner noted that James Terry "improved the lives of those around him through his willingness to share his knowledge and his genuine compassion for everyone." That assessment would appear to be fulfilled in this worthwhile and final volume, which, as Turner states, is "to be read by students, policymakers and interested members of the public for generations to come." Historians, scholars, and other readers can only hope for someone as astute and scholarly to carry on that legacy. **JFQ**

Alice A. Booher, JD, a former Foreign Service Reserve Officer and Counsel to the Department of Veterans Affairs, Board of Veterans Appeals (1969–2011), is well published in national media on numerous subjects. She is editor of and contributing author to *Glimpses of the New Veteran: Changed Constituencies, Different Disabilities, Evolving Resolutions* (Carolina Academic Press, 2015).



The Invisible Wounds of War: Coming Home from Iraq and Afghanistan

By Marguerite Guzmán Bouvard
Prometheus Books, 2012
254 pp. $18
ISBN: 978-1616145538
Reviewed by David F. Eisler

Each of us who has come home from war has experienced the return in our own way. Some were embraced by a loving family; others were alone. Some were respected by friends, while others were feared by neighbors. Many adjusted quickly to the comparative peace of their previous

lives, while some never adjusted at all, tormented by the demons of combat and post-traumatic stress disorder (PTSD). It is on this latter group of soldiers that Marguerite Bouvard focuses her attention in *The Invisible Wounds of War* through individual stories that, though incredibly moving, perpetuate many of the sensationalized stereotypes that have plagued the veteran community.

In the last few years, there have been a number of books intended to open a window into the experience of the modern soldier and combat veteran, including David Finkel's *Thank You for Your Service* (Sarah Crichton Books, 2013), Yochi Dreazen's *The Invisible Front* (Crown, 2014), and Howard Schultz and Rajiv Chandrasekeran's *For Love of Country* (Knopf, 2014). Bouvard's book, published in 2012, predates all of these and even anticipated many of the issues that have made recent headlines, including military sexual assault, controversy within the Department of Veterans Affairs (including a story of one veteran who received an appointment for trauma counseling 3 weeks after he committed suicide), as well as the philosophical issues associated with maintaining an all-volunteer force. In that regard, it is worth reading to see how these themes have evolved over time and to get a personal sense of how they affected real people.

Much of the book, though, is written in an anecdotal tone of hearsay, with many needless citations given for banal details, while wild claims are neither put into context nor supported with evidence. Because these stories are strung together without pausing to consider the context of the situation, the book misses the chance to connect with the larger conversation about military veterans. In many cases, the author is unable to distance herself from her subject, veering too often into the political and seemingly selecting her samples to confirm her convictions. In the chapter on mothers, a subject about which the author has written several books, it is somewhat surprising that every single mother was upset when her child decided to join the military. Several mothers even try to talk their children out of it.

The book's biggest issue is its propagation of numerous negative stereotypes about veterans. Bouvard contends that "returning soldiers harbor a grief that is not widely understood" and that "they can't come home [because] . . . these memories will never go away. When soldiers drive down a highway or a road in Illinois, Nevada, New York, Colorado, or any other place, they look at rooftops and overpasses to make certain there are no enemies waiting with rifles." But her conclusions and narrative are driven by a few interviews with select individual veterans and family members and then told as if representative of the entire population—everyone in this book suffers from PTSD.

In a few cases, Bouvard evokes dangerous sensationalism. "Veterans return in combat mode," she writes, "which gives them the ability to respond instantly with deadly force. They are in perpetual mobilization for danger, endurance, and hyper-arousal." And in a later paragraph, she claims, "because soldiers have to distance themselves from emotions suffered during a horrific war, their feelings often flare up at unexpected times after returning to civilian life." If the book is meant as a way to engage civilians in understanding the emotions of war veterans, how will they come away thinking about them?

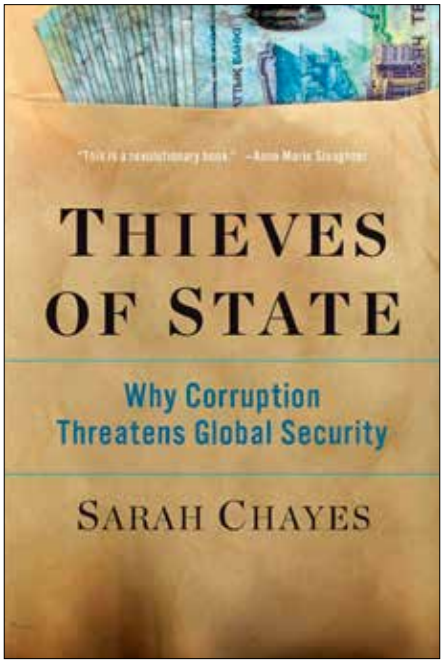
Even with these problems, much of the book is poignant and excellent, such as her description of soldiers walking long distances and waiting in lines just to get a few minutes on the phone to call their wives or families. The author is at her best when writing about the emotions and reactions of an individual person rather than making generalizations about all veterans. Her expert description of how families grieve and mourn their loved ones, whether lost in combat or to suicide, is some of the book's best material. It is easy to let those we have lost as a country become a set of faceless numbers, but Bouvard refuses to allow that. She also captures the complex emotions of coming home and readjusting to civilian life, including the feelings of dissociation

from others so familiar to those of us who have gone through it ourselves.

The book may be designed to spur readers to action, to force them to spring from their comfortable lives outside these wars and immediately find the closest veteran and shower him or her with care and affection. If you take the message too literally, though, you might come away with the impression that everyone who has served in the military is suffering and that the only way to ease their pain is to pity them.

Bouvard should be commended for her attempt to reach out, even if too much of her book is based on clichés and the unfortunately common philosophy of thinking that veterans have a monopoly on suffering that civilians cannot understand. She writes, "Living in the present, civilians have the luxury of managing their memories. We all have both good and difficult memories, but we are able to turn them off if we wish." But a person who has had a friend killed in a car crash or lost a relative to an unexpected disease—or who experiences any of the feelings of grief central to the human existence—can sympathize, if not empathize. We should not try to single out veterans as the owners of traumatic loss, but rather use that loss as a starting point to form bonds with others who have felt the same. Each side in the civilian-military conversation would benefit from sharing their stories with each other, as well as listening to the stories of their counterparts. **JFQ**

David F. Eisler is the Program Manager for Words After War and a Research Associate at the Institute for Defense Analyses in Alexandria, Virginia.



Thieves of State: Why Corruption Threatens Global Security

By Sarah Chayes
W.W. Norton, 2015
262 pp. $26.95
ISBN 978-0393239461
Reviewed by William H. Waggy II

Spring in Afghanistan brings the annual renewal from winter's snowmelt, as rivers threaten their banks and bring much-needed water to the country's valleys. This year, spring brought the onslaught of another seasonal occurrence: the annual evidence of rampant corruption in Afghanistan. March brought a story from *Stars and Stripes* that highlighted the Kabul market for gaudy mansions constructed over the last decade with no small assistance from foreign aid. April was no different, as a $100 million fuel contract scandal garnered attention in the Afghan press. Later that same month, the Special Inspector General for Afghanistan Reconstruction released a report on the oversight of personnel and payroll data that showed deficient control mechanisms allowing personnel to be paid regardless of attendance.

Sarah Chayes, a historian and award-winning PBS correspondent who later became a high-level advisor to former Chairman of the Joint Chiefs of Staff Admiral Michael Mullen, lived in the midst of Afghan corruption beginning in 2002. Originally sent to Kandahar on a reporting assignment following the U.S. overthrow of the Taliban, Chayes decided to stay in Kandahar as part of a nonprofit venture. She provides her first-hand knowledge of the payoffs, bribes, and embezzlement seemingly entrenched in southern Afghanistan during that time period. Corruption has never gotten better, but Chayes's perspective has changed. Later brought into the highest policy circles of the U.S. military, she advised multiple International Security Assistance Force commanders in the late 2000s including Admiral Mullen.

Corruption has long been on the mind of national advisors. In an early chapter, Chayes surveys so-called mirror literature, tracks from the Middle Ages that provided advice to future rulers. Though Niccolò Machiavelli's *The Prince* may be the most famous example, such advice transcends cultures and empires. She persuasively shows that writers across the centuries warned rulers of the dangers of corruption, some actually pointing to corruption as a source of weakness and instability in their kingdoms.

Chayes expands on the idea that corruption causes instability and applies it to Afghanistan. In this respect, she admirably contributes important ideas to conversations about Afghanistan security and stability. Chayes convincingly explains how unchecked corruption causes instability, national frustration, and ultimately violence. Corruption should not be viewed as merely a by-product of weak national governments or an inherent problem of insecurity. Rather, corruption erodes any support for governmental institutions, breeds cynicism throughout the population, and pushes people toward violent and puritanical solutions.

As governments fail to contain predatory impulses, the population looks for solutions that promise fairness. Looking across several countries, Chayes shows

that Islamic radicals seize upon this frustration and pledge to end corruption. Just as the Taliban promised to end the depredations of the warlords, so too do Uzbek radicals pledge relief from the vilely corrupt government in Tashkent. Liberal reformers typically lose in this popular battle, as the ideas that they advocate are inexorably linked to U.S. support for corrupt regimes. With liberals discredited, religious reformers gain the upper hand in this war of ideas.

Chayes offers a host of recommendations to fight corruption, although many of her suggestions are vague and nebulous. She advocates that intelligence analysts should study corrupt networks and develop models for understanding them. A functioning government takes in revenue that it passes through the bureaucracy to the population in the form of benefits, social welfare, and physical projects. A corrupt network reverses the flow of money in the government, taking in revenue from the population and passing the revenue up through the bureaucracy, with members at each level siphoning their cut of the money.

A comparison to a Mafia-style organization is telling. Calling the Afghan government a vertically integrated criminal network, low-level government officials skim money from the population and pass the money up the chain. The high-level officials receive the preponderance of the loot and in exchange promise protection from prosecution. Illustrating how the system works, Chayes tracks the case of a corrupt "two-bit border police buffo" arrested over stealing funds. Despite a seeming chasm separating this official from proper Kabul, bureaucrats up to then–Interior Minister Hanif Atmar frustrated the investigation, prevented his replacement, and ominously warned of unrest if a prosecution unfolded. The corrupt system took care of its own.

Though only associated with the military late in her career, Chayes effectively captures the military jargon and often irreverently highlights contradictions within the military's response to corruption. Easily readable, *Thieves of State* should sound a warning about allowing corruption to take root. Corruption undermines the institutions we develop in Afghanistan. Less a necessary evil and more just an evil, corruption feeds insurgency and provides legitimacy to religious zealots. Chayes does not provide all the solutions to this problem, but the first step will always be to admit that there is a problem. **JFQ**

Major William H. Waggy II, USA, is currently serving with Special Operations Joint Task Force–Afghanistan.

USS *George Washington* (CVN 73) Sailors load relief supplies onto MH-60R Seahawk for transport to local villages during Operation *Damayan* in response to aftermath of Super Typhoon Haiyan/Yolanda in Philippines (U.S. Navy/Chris Cavagnaro)

Interorganizational Cooperation

Part I of III: The Interagency Perspective

By James C. McArthur, William D. Betts, Nelson R. Bregón, Faith M. Chamberlain, George E. Katsos, Mark C. Kelly, E. Craig Levy, Matthew L. Lim, Kimberly K. Mickus, and Paul N. Stockton

In 2012, the Chairman of the Joint Chiefs of Staff directed the Armed Forces to expand the envelope of interagency cooperation.[1] His edict inspired a profusion of Department of Defense (DOD) literature cataloging the challenges of working with non-DOD organizations. This article is part one of a three-part series that features the other side of the story: interorganizational cooperation from interagency perspectives. Over the course of this series, authors from U.S. Government, intergovernmental, nongovernmental, and treaty-based organizations argue that broader inclusion of non-DOD perspectives into joint doctrine encourages the identification and propagation of much-needed interorganizational best practices.

This installment features perspectives from U.S. Federal executive departments and agencies (hereafter referred to as *organizations*). We address many differences among our organizations that can disrupt the planning and execution of interagency agreements. This article argues that better awareness of such

Lieutenant Colonel James C. McArthur, USMC, is Chief of the Joint Staff J7 Joint Doctrine Division. Lieutenant Colonel William D. Betts, USAF, is the DOD Terminologist. Mr. Nelson R. Bregón is an Associate Assistant Deputy Secretary at the Department of Housing and Urban Development. Lieutenant Colonel Faith M. Chamberlain, USA, is a Civil-Military Affairs Officer at the Department of State. Colonel George E. Katsos, USAR, is a Doctrine Strategist at the Joint Staff J7 Joint Doctrine Division. Dr. Mark C. Kelly is a Pentagon Planner at the U.S. Agency for International Development. Mr. E. Craig Levy is a Supervisory Emergency Management Specialist at the Federal Emergency Management Agency. Captain Matthew L. Lim, USN, is a Senior Policy Advisor at the Department of Health and Human Services. Ms. Kimberly K. Mickus is a Senior Liaison Officer at the Department of Energy. Dr. Paul N. Stockton is the Managing Director at Sonecon LLC.

issues among organizations—especially a recognition of which differences offer opportunities for compromise—would foster improved interagency negotiation and unity of effort throughout whole-of-government endeavors. The following sections sort the differences into three broad categories: *purpose* (goals and objectives), *process* (methods of work and decisionmaking), and *people* (attitude and communication). The sections below address each category in order of increasing potential for compromise. The examples demonstrate that organizations do not willingly budge on purpose-based differences, while process differences offer some room for negotiation. People, however, appear the most malleable in that small efforts yield high payoffs throughout planning and execution.

Differences in Purpose

Joint Publication 1, *Doctrine for the Armed Forces of the United States*, defines *unity of effort* as "coordination and cooperation toward common objectives, even if the participants are not necessarily part of the same command or organization."[2] By definition, common objectives or shared purpose are a prerequisite for unity of effort. Naturally, governmental organizations were created to fulfill different functions. For example, the Department of State considers diplomacy the art and practice of conducting negotiations and maintaining relations between nations, while DOD provides for the security of the United States and its interests. When two or more organizations cooperate, their divergent high-level purposes could naturally cascade into opposing objectives at lower organizational levels. This divergence could be exacerbated by three differences: interpretation of higher level guidance, geographic areas of responsibility, and time horizons.

Interpretations of Higher Level Guidance. Competing objectives are often the result of U.S. agencies interpreting the same strategic guidance in different ways. The National Security Strategy contains general guidance and prioritization. In the absence of more specific comprehensive direction, organizations tend to define their objectives along organizational lines. Early U.S. Government in-fighting in Afghanistan was partially due to the George W. Bush administration's cancellation of a detailed Presidential policy directive for managing complex contingencies.[3]

Additionally, blurred congressional jurisdiction contributes to different interpretations of higher level guidance. Co-chairs of the 9/11 Commission report, for instance, related this problem as it pertained to the Department of Homeland Security, stating that "the jurisdictional melee among scores of Congressional committees has led to conflicting and contradictory tasks and mandates for DHS."[4] Unfortunately, congressional jurisdiction is not the only blurred line causing competing purposes.

Geographic Areas of Responsibility. A well-documented difference between organizations is the misalignment of their areas of responsibility. There is a notable disparity between DOD, State, and the United States Agency for International Development (USAID) boundaries in North Africa and Southwest Asia. Each organization has valid reasons for its own convention that support organization-specific purposes. Some agencies group countries based on cultural, historical, or economic connections. DOD deliberately separates India and Pakistan to foster discrete military relationships, while State combines them to address issues that pervade the entire region.[5] The geographic mismatch can also be challenging when a country is clustered with lower priority nations under one organization but grouped with higher priorities in another. Such mismatches precluded comprehensive strategies for countering terrorism and piracy in Africa.[6]

Organizations also tailor their boundaries with inconsistent sizes and scopes. DOD prefers larger, continent-sized groupings, while State and USAID favor smaller subdivisions. USAID has challenges operating within the wide aperture of DOD's combatant command planners because the vast majority of USAID's strategic planning occurs within the respective host countries. USAID's bottom-up, country-specific approach to strategic planning allows it to better involve host-country governments and local civil societies in solving their own issues, leading to more sustainable and effective solutions.

Despite clear benefits in doing so, organizations are not open to changing their geographic alignment. In a 2012 audit conducted by the Government Accountability Office (GAO), State and USAID stated that the improved geographic alignment associated with the standup of U.S. Africa Command improved cooperation among the three organizations. Despite this acknowledged success, significant objections to a wider alignment of world regions remain. State raised concerns that adjusting its regional bureaus to look like combatant commands would signal a "militarization" of diplomacy, unnerving partners and allies. The Department of Health and Human Services echoes this sentiment, stating that many Americans do not realize the mere fact that the organization represents the U.S. Government can affect relationships in unpredictable ways. Whereas in some relationships this fact is likely to open doors, in others there may be resistance to assent to U.S. wishes for the sole reason that opposition to the United States is a domestic political necessity. Other organizations, such as the Department of Justice and Department of Commerce, cited different reasons, including the burdens of retraining and relocating personnel. Additionally, all agencies professed a need to retain the authority to change their boundaries to adapt to changing mission requirements. All of these factors led GAO to conclude that a government-wide geographic alignment is unlikely, and thus the resulting disagreements over priorities and objectives will endure.

Time Horizons. Finding a common purpose may also take extra effort when different time horizons are involved. A U.S. military civil affairs officer in Afghanistan spoke plainly to a USAID official in Afghanistan, stating, "Our objective is to fight and kill al Qaeda and the Taliban. Your objective is to build a democratic central government. Right

U.S. Army veterinarian trains local Afghans as part of joint effort including Provincial Reconstruction Team Farah, 438th Medical Detachment Veterinary Services, and Special Operations Task Force–West to promote public health in Farah Province (U.S. Navy/Matthew Stroup)

now, our objective is number one, and the consequences of our actions will be your problem in six months."[7] Many organizations agree that this type of difference, which may generate inconsistent planning benchmarks with subsequent effects, is not uncommon. While State and USAID perspectives on relationships and programmatic results can stretch into decades, DOD outlooks tend to be much shorter. Thus, viewpoints on downstream effects can be valid yet dissimilar. In extreme instances, DOD may be the first U.S. implementer of civic engagement in an area. As such, these interactions can shape the environment and set expectations of local groups for other governmental organizations, even undermining access for humanitarian partners.

When DOD-USAID coordination is absent, DOD activities may lead local groups to develop unrealistic goals for future governmental interactions, leading to disappointment, resentment, and possible anger toward the United States. It can also undermine many of the tools USAID uses to motivate populations to engage in solving their own problems. For example, early in Operation *Enduring Freedom*, the U.S. military was incentivized to achieve "quick wins" in civic and humanitarian assistance activities. As a result, commanders spent large sums of money quickly often without considering the downstream effects. One unintended consequence of cash infusion on Afghanistan's agrarian economy was a change in consumer behavior for veterinary services. While USAID had been conducting long-term livelihood training for veterinarians and vet technicians in the country, the military's free veterinary services completely undercut the ability of USAID-trained veterinarians to make a living. As a result, farmers chose not to pay for local services because they could wait and receive free civic services from military programming.[8] A contemporary USAID official eloquently summarized that spending money quickly in unstable areas usually means unstable results.[9]

Best Practice: Finding Shared Purpose. Different interpretations of higher level policy usually only see resolution at the highest level. The National Security Council (NSC) staff can settle such disparities by issuing clarifying guidance in the form of Presidential policy directives that clearly state goals and responsibilities for a particular mission.[10] Another possible mechanism to encourage shared purpose is a congressionally mandated review to include national security. Although the State Department and USAID 2010 Quadrennial Diplomacy and Development Review is not congressionally mandated, it identified the need to turn to other governmental agencies for experience and expertise in performing international functions. Both Homeland Security and Justice viewed this recognition as positive. Given

that congressionally mandated reviews may better instigate change, the U.S. Government could benefit from mandated reviews for all Federal executive departments or those departments only participating in the NSC system.[11] A single comprehensive Quadrennial Security Review for those departments under the NSC system also could be beneficial.[12]

But not all interagency friction occurs at a level that warrants NSC or congressional attention. At the operational and tactical/field level, organization officials have to work through challenges. Organizations may have varying functions, but those do not prevent a shared purpose for a portion of the mission. "Promote Cooperation" is a DOD forum in which combatant commanders request input and feedback on their plans from non-DOD counterparts. Simulations and workshops can help organizations find common ground that previously did not exist. In geographic combatant commands, military planners determined that there was a need to track, integrate with, and support efforts with State Department activities to preclude the need for a noncombatant evacuation operation executed by the military. The functional combatant commands also embed civilian organization liaisons into their command structures.[13] Even if objectives cannot align, the liaisons and humanitarian advisors can look one or two organizational levels down to identify opportunities of mutual interest, for instance. Homeland Security and the Federal Emergency Management Agency (FEMA) also benefit with embedding DOD liaisons in their organizations, which can prevent late resource requests that end up in unfilled requirements.

With respect to differing time horizons, organizations with a longer view can seek short-term cooperative opportunities with partners who have less time available. These opportunities, if taken, may overcome unintended consequences toward government efforts. Because unity of effort requires common objectives, when there is no obvious shared purpose the organizations must actively seek common ground. The idea is not to force an unnatural cooperation but rather to find the hidden symbiotic relationship that provides mutual benefit. A shared purpose is the first step toward a framework of cooperation: a shared process.

Differences in Process

Once interagency participants share a purpose, they can plan the shared process to achieve it. U.S. Government organizations typically codify mutually beneficial arrangements in the form of a general memorandum of understanding (MOU) or a detailed, more binding memorandum of agreement (MOA).[14] An example of a successful shared process is the Homeland Security National Response Framework (NRF).[15] This off-the-shelf plan establishes roles and responsibilities for orchestrating the government's comprehensive domestic disaster response. An example of how process differences preclude a much-needed agreement is in the stalled International Response Framework (IRF).[16] The current Federal system for foreign disaster response, led by USAID, is effective for normal disasters. However, complex overseas catastrophes involving infrastructure collapse (for example, Haiti) or radiological events (such as in Fukushima), especially in developed or big modern cities, beg for an international response capability comparable to the NRF. Such complexities aggravate the process difference of would-be participants. To arrive at a shared process such as an MOA or MOU, U.S. Government organizations must first compare the processes—namely, decisionmaking and methods of work—of their individual organizations.

Decisionmaking. Many organizations view DOD as overly bureaucratic. The department's sheer size and complexity can make liaison and cooperation difficult for other organizations. For starters, DOD's enormity can cause a resource and power disparity. Smaller organizations may be reluctant to cooperate for fear of their efforts being co-opted and/or losing turf and resources.[17] Other organizations do not have the manning or time to participate in planning events or other settings to the extent that DOD does or might expect. Similarly, the broad mission set and needs of DOD make it difficult for civilian agencies to find points of contact that can speak with finality.

Each organization has its own decisionmaking habits and may employ command structures that are more flexible and fluid than those of DOD. Staffing decisions for a special project or specific incident may be based more on individuals' subject matter expertise than on their rank, grade, or position. This facilitates application of the best resources to a given problem, but it may also cause temporary changes to traditional chains of command or result in coordination points that reside at different levels within each respective organization. Some organizations may also take a different approach to managing an incident. While DOD manages largely through individuals within a rank structure, the Department of Housing and Urban Development (HUD) manages disaster response through an internal committee known as the Disaster Management Group. So while action officers in DOD may only need the approval of an individual, action officers within HUD may need the approval of an entire committee.

Methods of Work. While DOD is accustomed to global connectivity, it is easy to forget that sharing data with interagency partners may not be as easy. Much of the information that DOD possesses is classified, and the rationale for many decisions requires access to classified material. The inability to quickly declassify this information so it can be shared with non-DOD and U.S. Government organizations hinders effective engagement by many DOD senior leaders and action officers. Additionally, the lack of linguistic expertise and cultural sensitivity on the part of many DOD members is a hindrance to effective cooperation.

Some organizational cultures are diametrically opposed to that of DOD. The military's strict chain of command and requirement to unquestioningly follow lawful orders are foreign to organizations such as the Department of Energy (DOE) and its need to challenge and question, which are hallmarks of good science. Other practices such as addressing everyone, other than the most

senior leadership, by first name may be mistaken by DOD as disrespectful, while non-DOD meeting attendees are often mystified when everyone leaps to their feet when a general walks in. Working hours can be another contrasting trait. Although many organizations maintain a constant high operational tempo, some operate according to "traditional business hours." This can create challenges during time-sensitive operations such as disaster response. Although organizations such as DOD, DOE, or FEMA may be able to vet and approve actions quickly, including at night and over weekends, traditional hour operations may have staff working extra hours in support of an incident. The reachback of these other organizations to headquarters or leadership for technical assistance may be delayed during non-work hours because the organization is not structured or staffed to maintain its full suite of capabilities 24/7.

Best Practice: Compromise for Shared Process. DOD has learned in the last decade that trying to predict a partner's reaction to a situation can be clouded by a common tendency known as mirror-imaging: assuming the other side will act in a certain way because that is how you would act under similar circumstances. In recent conflicts, mirror-imaging has led to poor assumptions and offended partners. Without awareness of a partner's organizational culture, mirror-imaging can also be a problem in interagency cooperation. By improving organizational cultural awareness, U.S. Government organizations can compare their processes to find room for compromise. The resulting interagency plan will reflect not only a vetted shared purpose but a shared process as well: one that incorporates decisionmaking mechanisms and methods of work compatible for all participants. For example, under the NRF, several organizations that are accustomed to leading have yielded in the name of a shared purpose and process. FEMA is designated as the supported organization and a host of governmental organizations, including DOD, are in appropriate supporting roles. As FEMA assigns missions to meet specific assistance requirements, it also tells DOD what is needed, where to take it, and how that assistance will be integrated into the larger Federal support operation. Complex overseas catastrophes involving chemical or radiological events, such as Fukushima, reinforce the need for a comparable IRF. Additionally, DOD information-sharing obstacles facing non-DOD personnel during time-sensitive operations underpin the need for more efficient ways of doing business.

It is important for DOD representatives to remember that organizational process differences are just that: differences. There is not a right or wrong organizational culture—just one that best suits the purpose of the organization. Avoiding the tendency to mirror-image will prevent poor assumptions and temper expectations. Each organization should clearly articulate its needs, resources, abilities, authorities, and, most importantly, its constraints. Many issues arise from one party making assumptions about another party based on its own way of doing things. Clear communication of requirements and timelines upfront affords the opportunity to mitigate missed connections down the line. To reinforce positive communication among organizations, MOAs and MOUs are good foundations for a shared process, and an accessible DOD central repository would enhance awareness on how the department interacts with interagency partners.

People: Communication Makes Workarounds Work

People actively search for a common purpose. People compromise to forge a common process. People make decisions, and people do the work—with other people from other organizations. U.S. Department of Agriculture (USDA) representatives reported that their ability to work effectively with interagency partners in Iraq and Afghanistan depended almost entirely on developing positive interpersonal relationships based on trust.[18] There are three types of communication differences that have stalled personal relationships in the past: terminology, information-sharing, and attitude.

Terminology. Anyone who has experienced a DOD meeting knows the military speaks a unique language peppered with jargon, acronyms, and high-tech PowerPoint lingo. But a unique language has evolved at other organizations as well, and each side is often unaware that a common word has a different meaning to the other. One well-known example is the word *intelligence*; while in fairly common use (as in "medical intelligence") on both the military and civilian sides, it can cause difficulties in other settings when it may be interpreted as a form of espionage. Many organizations echo this sentiment. Without prior knowledge, DOD partners can also read a more militaristic intent into innocuous DOD terms such as *targeting* when, in fact, a DOD author may only be referring to selectivity and focus with no context of violent action whatsoever. While militaristic terminology can make interagency players question DOD's intentions, withholding information can cause longstanding issues of trust.

Information-sharing. Often the military is required to withhold information out of operational necessity. However, what looks like a clear operational necessity to DOD will not always appear as clear-cut to other organizations. A senior civilian State official expressed his frustration at his organization's lack of awareness of DOD special operations missions: "None of us knew in many cases what they [DOD] were doing until an operation had already taken place. There was one really bad issue where Special Forces killed the wrong guys, and [the country team] had to explain it all to [Afghan president Hamid] Karzai without even having known such an operation would take place."[19] DOD is not expected to curb this practice, only to ensure the decision to withhold information is a calculated one because even justified instances can erode trust.

Even more damaging cases of withheld information are those due to negligence. Another senior civilian was more incredulous when DOD withheld mission results long after a mission went bad: "They bombed a wedding party; we heard about it way after the fact. If we had heard sooner, we could have helped mitigate the effects."[20]

Attitude. Organizational cultures also affect how individuals act and treat

U.S. military humanitarian assistance capabilities support emergency relief efforts at Fukushima Daiichi Nuclear Power Plant (U.S. Air Force/Shane A. Cuomo)

others. Mirror-imaging was shown to lead to poor assumptions about decisionmaking practices and methods of work used in organizations. The same concept can apply to individuals with equally damaging results. Differences in organizational attitude are merely unjustified perceptions—that is, stereotypes. Even though a person works for an organization with a certain reputation, uniform, rank, or grade, there are, quite often, more similarities than expected. A senior USAID official relayed his change of heart about working with military officers in Afghanistan:

Ambassador Khalilzad asked a bunch of military planners to come in and do planning. The idea among USAID . . . staff that we'd have five colonels working with us to do our planning . . . was uncomfortable. But the more we got to know them, the more we respected their talent, skill, hard work. . . . We realized we were on the same team. They pushed us, challenged us, made us think. Most USAID people never work with the military, so this whole experience was new.[21]

Another USAID official explained a progressive experience in Afghanistan: "At one point I [told senior officials in Washington] that I thought we had a hell of a lot in common with the uniformed military, which was rebellious to say and stunned them. I said that they are operational, mission oriented, have a command and control structure and chain of command, plan well and do strategies well, and we [at] USAID do all the same."[22]

Best Practice. Cross-organizational communication fundamentals are an easy fix with huge payoffs throughout the planning and execution of an interagency endeavor. Given enough time, U.S. Government representatives learn that people from other organizations are not as different as they assumed. If DOD personnel can avoid the prescribed missteps and get off on the right foot, they can build vital interpersonal relationships without struggling to earn respect over many months or years. More frequent personal interaction will only accelerate the process and build trust. For example, USAID encourages DOD field personnel to reach out directly to USAID country staff in both tactical and strategic planning. At the same time, USAID strives to educate its own staff as to why DOD may be engaging in activities that could be considered within USAID's purview and how to productively interact with such activities. USAID continues its DOD outreach to build on cooperative efforts with its new policy on cooperation with DOD.[23]

One aspect of this policy is already proved. Interagency collocation was widely recognized as a best practice in Afghanistan. Collocation at multiple levels of decisionmaking made possible regular joint analysis and planning and facilitated relationship development and mutual learning.[24] Almost immediately after Lieutenant General David Barno,

USA, took command of the combined forces in Afghanistan in 2003, he moved his headquarters to the Embassy compound. Barno and Ambassador Zalmay Khalilzad saw each other for a few hours every morning and every evening. The Ambassador emphasized the benefits of collocation: "Being . . . so close facilitated more frequent interaction, not only by telephone. . . . We made a commitment that what was important was the mission, that we were a single team."[25] Collocation helps mitigate all three identified categories of differences. Neighbors learn each other's language, they feel obliged to share information as much as possible, and they give respect and trust where it is due.

Perhaps practice makes perfect. The more opportunities organizations have to collaborate in more detail on a recurring basis, the better prepared they will be to collaborate during a crisis. Increasing the number of contact points and collaborative projects among agencies will bring greater familiarity for each of the others. It is the relationships fostered on a continual basis that will facilitate efficiency when time is of the essence.

More interaction in force development venues will also allow subject matter experts to better identify and proliferate much-needed best practices. Although war college students will read lessons learned such as from the State Department and USDA, the other 90 percent of the military will not look for those perspectives. DOD joint force development continuously grows in importance due to the acknowledgment that no single military Service can win a war on its own. In Iraq and Afghanistan, the United States learned that no single governmental organization could stabilize a war-torn region alone. A similar theme emerged at Fukushima and in Haiti. If DOD continues to be asked to support executive decisions in nontraditional military operations and complex catastrophes, which are likely callings for DOD in the years to come, then interagency force development at the strategic, operational, and tactical levels must be cultivated.

This article raises awareness on U.S. Government organizational purpose, process, and people differences. By presenting non-DOD perspectives, we aim to facilitate DOD interagency cooperation through improved awareness of negotiation pitfalls. By definition, unity of effort requires unity of purpose. Partners may have different purposes for the task at hand, but comparing objectives across time, space, and organizational level can unearth commonalities. Once a shared purpose is found, comparing process differences will identify friction points that must be negotiated before codifying a shared process. Where purpose and process differences present significant structural barriers to compromise, interpersonal relationships just take a little effort and are widely recognized as the most important facilitator in interagency cooperation. As new interagency differences and best practices emerge, broader inclusion of interagency perspectives into joint doctrine ensures these updates are captured throughout the continuous cycle of joint doctrine revision. It broadens the audience and truly expands the envelope of interagency coordination per the Chairman's remit. The second installment of the Interorganizational Cooperation series expands the envelope further beyond the U.S. Government with perspectives from intergovernmental, nongovernmental, and treaty-based organizations. **JFQ**

Notes

[1] Martin E. Dempsey, *Chairman's Strategic Direction for the Force: Strengthening Our Relationship of Trust with the Nation* (Washington, DC: The Joint Staff, February 6, 2012), 5.

[2] Joint Publication (JP) 1, *Doctrine for the Armed Forces of the United States* (Washington, DC: The Joint Staff, March 25, 2013), GL-13. JP 3-08, *Interorganizational Coordination During Joint Operations* (Washington, DC: The Joint Staff, June 24, 2011), which is traditionally the one-stop shop for non-DOD and nongovernmental entities to enter into the joint doctrine hierarchy, is presently under revision with an expected signature date in 2016.

[3] Andrea Strimling Yodsampa, *Coordinating for Results: Lessons from a Case Study of Interagency Coordination in Afghanistan* (Washington, DC: IBM Center for the Business of Government, 2013), 13. In an effort to capture institutional lessons from complex operations, the Clinton administration issued Presidential Policy Directive 56, *Managing Complex Contingency Operations*, in May 1997. The Bush administration replaced it in 2005 with the issuance of National Security Presidential Directive 44, *Management of Interagency Efforts Concerning Stabilization and Reconstruction*.

[4] Frederick M. Kaiser, *Interagency Collaborative Arrangements and Activities*, R41803 (Washington, DC: Congressional Research Service, May 31, 2011), 16.

[5] John H. Pendleton and Jacquelyn L. Williams-Bridgers, *Interagency Collaboration: Implications of a Common Alignment of World Regions among Select Federal Agencies*, GAO-11-776R (Washington, DC: Government Accountability Office, July 11, 2011), 17.

[6] Ibid., 6.

[7] Yodsampa, 14.

[8] Ibid., 27.

[9] Ibid., 21.

[10] Richard A. Best, Jr., *The National Security Council: An Organizational Assessment*, RL30840 (Washington, DC: Congressional Research Service, December 28, 2011).

[11] Presidential Policy Directive 1, *Organization of the National Security Council System* (Washington, DC: The White House, February 13, 2009).

[12] Alan F. Mangan, *Planning for Stabilization and Reconstruction Operations without a Grand Strategy* (Carlisle Barracks, PA: U.S. Army War College, March 18, 2005), 14.

[13] Pendleton and Williams-Bridgers, 26.

[14] DOD Instruction 4000.19, "Support Agreements," April 25, 2013, 28.

[15] *National Response Framework* (Washington, DC: Department of Homeland Security, January 2008).

[16] *Independent Review of the U.S. Government Response to the Haiti Earthquake: Final Report* (Washington, DC: U.S. Agency for International Development [USAID], March 28, 2011), 86; *Quadrennial Diplomacy and Development Review* (Washington, DC: Department of State, July 2009), 140.

[17] Yodsampa, 9.

[18] Bernie Carreau, "Lessons from USDA in Iraq and Afghanistan," *PRISM* 1, no. 3 (June 2010), 144.

[19] Yodsampa, 14.

[20] Ibid.

[21] Carreau, 144.

[22] Yodsampa, 19.

[23] Alfonso E. Lenhardt, *USAID Policy on Cooperation with the Department of Defense* (Washington, DC: USAID, June 2015).

[24] Yodsampa, 35.

[25] Ibid., 16.

Thunderbirds pilot banks right over Rocky Mountains after refueling in flight by KC-135 Stratotanker from McConnell Air Force Base, Kansas, May 21, 2015 (U.S. Air Force/Zach Anderson)

Lessons about Lessons

Growing the Joint Lessons Learned Program

By Jon T. Thomas and Douglas L. Schultz

There is no decision that we can make that doesn't come with some sort of balance or sacrifice.

—Simon Sinek

Brigadier General Jon T. Thomas, USAF, is Commander of the 86th Airlift Wing and former Deputy Director for Future Joint Force Development, Joint Staff J7. Douglas L. Schultz is a Lessons Learned Analyst in the Joint Lessons Learned Division, Joint Staff J7.

Lessons learned programs are traditionally used to improve organizational performance. As such, in a very true sense, these programs are "leader's programs" or top-down leadership tools. But at the same time, there is another equally important aspect that sometimes gets overlooked. In a large organization, with many distinct suborganizations, a lessons learned program is also intended to support organizational learning—many times from the bottom up—through the sharing of information about common problems and solutions throughout a community of practice. Lessons learned and shared across the larger organization enable all to learn from others' experiences with the aim of avoiding the waste and redundancy of repeating the same mistake.

U.S. Marine Corps officers assigned to Company A, The Basic School, listen to confirmation brief for field training exercise at Marine Corps Base Quantico, Virginia, April 16, 2015 (U.S. Marine Corps/Ezekiel R. Kitandwe)

The U.S. military, with its various Services, staffs, and support agencies, clearly falls into the category of a large organization with many suborganizations. Within this large and diverse grouping, effective commanders and leaders instinctively do their best to ensure that those under them learn from mistakes to avoid repeating them, while also seeking out best practices to give them an edge against likely opponents. In this sense, lessons learned "commander's programs" have been around since people first organized into groups to fight one another. Yet the other side of lessons learned does not come so naturally in a military setting, where hierarchy is firmly established and competitiveness abounds. While members serving within the same command or Service usually have no problem sharing with their compatriots, it can be a different story with outsiders. Military organizations often find it difficult to readily share failures for the sake of group learning. But especially in a dynamic environment characterized by evolving threats and tight fiscal constraints, finding a way to balance the need for a commander's program with the need for timely sharing of knowledge across the enterprise is an absolute imperative.

This article discusses how the Armed Forces have gone about this balancing act since the inception of a formalized Joint Lessons Learned Program (JLLP) following passage of the Goldwater-Nichols Department of Defense Reorganization Act of 1986. This article maps the growth of the JLLP from nascent efforts to the current broad program of today with particular focus on the significant transformation that occurred by virtue of transition to a single system of record. The story of this program, as it sought to meet and balance the needs of the large organization that is the U.S. military, as well as its individual suborganizations, may offer some lessons about lessons to any large organization faced with similar challenges.

1986–2006: Initial Attempts to Develop a Joint Process

Goldwater-Nichols was Congress's way of saying that the Armed Forces had become too competitive with each other at the expense of the taxpayer and that change was no longer optional. In addition to many other legislated changes, the Chairman of the Joint Chiefs of Staff was tasked with improving interoperability of the Services to conduct more effective and efficient joint operations. One important implication of this task was to improve the sharing of joint lessons and best practices across Service lines. Prior to Goldwater-Nichols, joint lessons learned activities were almost entirely a commander's program carried

out independently by the Services as well as the unified and specified commands. Since the Joint Chiefs of Staff did not have authority to direct actions across Service lines, the need for sharing lessons and best practices went almost unaddressed despite two General Accounting Office (GAO) reports criticizing the Department of Defense (DOD) for failing to do so. The first report, in 1979, found that "systems for identifying, analyzing, and following up on exercise lessons learned and putting the results to use were not effective" and recommended that DOD develop a universally available database where lessons could be stored and retrieved.[1] The second report, in 1985, recognized efforts undertaken since 1979, but still found significant interoperability problems and noted the lack of any progress on developing the lessons learned system previously recommended. The 1985 report identified three fundamental elements that should be present and well integrated in any successful lessons learned program: capturing and reporting observations and issues, recording and sharing this information, and providing a venue to ensure issues identified were being resolved.[2]

Goldwater-Nichols was enacted the following year, bringing the debate about "jointness" to a close. The authority of the Chairman was expanded to better address continuing joint interoperability issues. By enacting these changes into law, the intent was to "improve the functioning of the joint system and the quality of joint military advice."[3]

In response, the Chairman reorganized the Joint Staff and established three additional directorates: the J6 (Command, Control, and Communications Systems), J7 (Operational Plans and Interoperability), and J8 (Force Structure, Resources, and Assessment). The Director of the Joint Staff (DJS) provided specific guidance to the new Director of the J7 (DJ7) to establish a "high level, single focal point for functions of force interoperability to include war planning, joint/combined doctrine, JTTP [joint tactics, techniques, and procedures], readiness, joint exercises and training, and the remedial action program."[4] Partly in response to GAO criticism, and partly because of the increased authority to do so, the DJS specified a task to the new J7: stand up a Joint Center for Lessons Learned (JCLL).[5] This marked the first recorded effort in DOD to institutionalize a means to balance the commander's program approach with a knowledge-based learning capability.

While the Chairman was reorganizing the Joint Staff, the Services and combatant commands (CCMDs) made their own independent adjustments to improve their use of lessons learned. The first to formalize and expand its program was the Army with the establishment of the Center for Army Lessons Learned at Fort Leavenworth for the purpose of "collection, analysis, archiving, and dissemination of observations, insights, and lessons; tactics, techniques, and procedures; after action reviews; operational records; and lessons learned from actual Army operations, experiments, and training events . . . to sustain, enhance, and increase the Army's preparedness to conduct current and future operations."[6]

At the same time, the Air Force established its own formal lessons learned organization under the Studies, Analyses, and Assessments directorate (A9) of the Air Staff, eventually known as the A9L. This group was tasked to support "operations, exercise, and wargame after action reports as well as other [lessons learned] activities."[7] The Marine Corps also established a service-level lessons learned program under its Training and Education Command in Quantico, Virginia, the Marine Corps Center for Lessons Learned.[8]

On the JLLP front, several of the unified and specified commands also established staff-level lessons learned capabilities. The programs at U.S. European Command and U.S. Readiness Command were cited in the 1985 GAO report. All of these programs were initially known as Remedial Action Programs (RAPs), reflecting the primary emphasis on addressing shortfalls rather than on sharing knowledge of lessons learned. Even on the Joint Staff, despite the JCLL title, one of the two guiding policy directives was the Remedial Action Project Program.[9]

The JCLL was expected to contribute significantly to the J7's overall responsibility "for evaluating the preparedness and effectiveness of the unified and specified commands to carry out their assigned missions."[10] Three basic elements of lessons learned, identified in the 1985 GAO report, were brought together within one organization. Observations and issues would be captured through inputs to the Joint After Action Reporting System (JAARS). This information would be recorded and made widely available through the Joint Universal Lessons Learned System (JULLS). So while the RAP process continued to reflect the imperatives of a commander's program, the JAARS and JULLS processes became the underpinning for the sharing of lessons and best practices across the U.S. military.

In 1991, Operation *Desert Storm* provided the first large-scale operational test of the jointness legislated by Goldwater-Nichols. *Desert Storm* was widely viewed as a resounding validation of training to operate together as a joint force. However, interoperability problems still lingered and were documented during subsequent joint operations such as the Hurricane Andrew disaster response in Florida and Operation *Restore Hope* in Somalia. This led to renewed interest from GAO and initiation of another report in 1995, which focused specifically on how the potential to use lessons learned was not being realized.[11]

Despite the establishment of formal lessons learned programs in most of the headquarters (including the Joint Staff), GAO assessed that DOD was still failing to solve significant joint interoperability problems. The report concluded:

Despite lessons learned programs in the military services and the Joint Staff, units repeat many of the same mistakes during major training exercises and operations. Some of these mistakes could result in serious consequences, including friendly fire incidents and ineffective delivery of bombs and missiles on target. As a result, the services and the Joint Staff cannot be

assured that significant problems are being addressed or that resources are being used to solve the most serious ones.[12]

Even before the 1995 GAO report was published, the J7 staff recognized the need to improve the program. In 1994–1995, J7 launched the Better Lessons Learned campaign and undertook a series of visits to combatant command headquarters, soliciting feedback on what needed to be fixed. The feedback fell into four broad categories: develop and field state-of-the-art software, provide online capability, develop an analysis program, and focus on and correct significant problems.[13]

Work on the two nontechnical categories began right away. Using the Chairman's RAP process, the J7 argued successfully for creating an actual center at the Joint Warfighting Center (JWFC) that would provide the missing lessons learned analytical capability and thus the ability to identify and focus on correcting significant problems. The JWFC, established in 1993 as a Chairman-controlled activity, was located in the Hampton Roads area of southeastern Virginia. It already provided extensive support to the joint exercise and joint doctrine programs, so it seemed a sensible choice for this new task. The JWFC commander and DJ7 formalized a JCLL Implementation Plan in early 1997, which split joint lessons learned program responsibilities between their two organizations, with production and analysis concentrated in the JWFC while leaving policy and oversight of the program in the Pentagon with the J7. JWFC would also be responsible for maintaining the JULLS/JAARS database, which would theoretically give it direct access to analyze all joint lessons learned data.[14]

Developing user-friendly software and providing online access proved to be a much harder nut to crack. Although work started on a prototype Windows-based JULLS, it was suspended before the end of fiscal year 1997 to apply all available funding to develop the Joint Training Information Management System. After that, the joint community again was left to its own devices to either borrow one of the Service systems or to develop something in-house for local use.[15]

The new JWFC/JCLL organization operated as intended, even after the JWFC was transferred to U.S. Joint Forces Command (USJFCOM) in 1999 as part of a defense reform initiative seeking efficiencies within the Pentagon staff. In August 2000, the new roles and functions were clarified as part of a rewrite and re-titling of Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 3150.25. The new version, CJCSI 3150.25A, bore the title "Joint Lessons Learned Program," in recognition of the increased scope of the program beyond the report-centric Joint After Action Reporting System. During the subsequent year, this arrangement appeared to function reasonably well, with the JCLL beginning to broaden the scope of its efforts to perform trend analysis on JAARS data for potential un- or under-reported issues throughout the joint force. We will never know how the relationship would have matured because on September 11, 2001, its future was altered dramatically along with that of the rest of the Nation by the terrorist attacks on the World Trade Center and the Pentagon.

One of the first tasks that followed the attacks came in the form of a question from the Secretary of Defense, asking what lessons had been learned in the preceding years by U.S. forces combating terrorism. The initial response was developed from data gathered from the JAARS/JULLS database, supplemented with information received as a result of a force-wide data call. The resulting product was delivered approximately 3 months later, but it was not considered adequate.[16]

Over the next year (2001–2002), the JCLL found opportunities to explore the benefits of actively collecting observation data first at the request of the commander of Task Force 160 (Guantanamo Bay Detainee Operations), and later with the Army's 10th Mountain Division in Operation *Enduring Freedom*. At the same time, the Service lessons learned programs were beginning to send personnel forward to conduct active observation and lesson collection in theater.

As planning for Operation *Iraqi Freedom* (OIF) neared completion in early 2003, the USJFCOM commander knew immediately that the task of active data collection would be well beyond the capability and means of the 1 government civilian and 10 contractors assigned to the JCLL. On February 3, 2003, he tasked the USJFCOM J7 and the JWFC to build the necessary collection team, drawing resources from across the command. The resulting Joint Lessons Learned Collection Team (JLLCT) numbered over 30 Active, Reserve, and National Guard officers, and was led by then–Brigadier General Robert Cone, USA. To provide reachback analytical support, USJFCOM also formed a JLLCT-Rear element consisting of approximately 24 civilian analysts working in the JWFC.[17]

Embedded within U.S. Central Command's (USCENTCOM's) forward headquarters, the JLLCT was able to witness, record, and analyze operational-level lessons first-hand and to coordinate their efforts with Service collection teams. To receive the necessary level of access, the USJFCOM commander had to assure the USCENTCOM commander that the team's sole purpose was to support USCENTCOM and that there would be no collection efforts tied to a hidden agenda. In effect, this reinforced the commander's program approach and provided great value to USCENTCOM, although perhaps at the expense of broader sharing with, for example, other commands supporting USCENTCOM. Despite the limitations on sharing, the arrangement was considered successful enough to be enclosed within the next version of CJCSI 3150.25 as a generic Terms of Reference template for future active collection efforts.[18]

Once approved for release outside USCENTCOM, the JLLCT report on OIF Lessons Learned (LL) was extremely successful in garnering top leadership support to resolve larger issues beyond the USCENTCOM commander's authority or capability to resolve. In May 2003, the Joint Staff directors held an offsite to discuss and coordinate an OIF LL action plan. In October 2003, this Joint Staff–wide effort was formalized

U.S. Army Rangers assigned to 2nd Battalion, 75th Ranger Regiment, fire 120-mm mortar during tactical training exercise at Camp Roberts, California, January 30, 2014 (U.S. Army/Nathaniel Newkirk)

as the OIF LL General Officer Steering Committee (GOSC), tasked to conduct quarterly reviews of progress on the OIF LL action plan. The LL GOSC was chaired by the DJS and attended by the vice directors from across the staff, reviving and elevating the Chairman's RAP process as a forum for moving validated issues into the correct issue resolution processes. This approach would later be formalized in the 2005 revision to the JLLP's guidance directive, CJCSI 3150.25B.

In October 2003, the Chairman expanded the scope of USJFCOM's JLLCT, requesting that they "aggregate key joint operational and interoperability lessons reported by combatant commands, Defense agencies and Services derived from OIF and the War on Terrorism and initiate analysis of those lessons."[19] In response to the Chairman's guidance, USJFCOM identified funding requirements[20] and proceeded to formalize the JLLCT as a permanent entity that would later become known as the Joint Center for Operational Analysis (JCOA).[21]

In December 2003 and March 2004, DOD published two major lessons learned reports. The first, a report by the Defense Science Board's Lessons Learned Task Force, was an independent, classified, strategic-level view of lessons learned during OIF, but it also contained observations and insights on the JLLP itself. The second report, commissioned by the Office of the Under Secretary of Defense for Personnel and Readiness, focused on the status of the JLLP and how it might be enhanced to better support a project to overhaul the Joint Training System called the Training Transformation Initiative.[22]

Both reports recommended that USJFCOM continue in its role as the primary operational-level lessons learned activity, based on the JLLCT's strong performance. They both recommended that Services and agencies continue to concentrate their efforts at the tactical level. But they both also recommended that more emphasis be placed on strategic-level lessons learned with more formalized integration with planning, programming, budgeting, and execution processes to institutionalize change across DOD instead of at just one command.

2006—Present: Establishing a Better Balance Through a Single System of Record

While JCOA continued to perform well supporting the commander's program aspect of the JLLP, the Joint Staff J7 lessons learned element worked largely behind the scenes in 2005–2006 to lay the groundwork for a new Web-based, universally accessible automated support

Blue Angels fly over Safeco Field before Mariners baseball game in Seattle, Washington, July 29, 2015 (U.S. Navy/Michael Lindsey)

tool for sharing of lessons, the Joint Lessons Learned Information System (JLLIS). When fully developed and fielded, this system was intended to improve the balance between supporting the commander and sharing lessons across the force.

In April 2006, after examining several existing lessons learned systems, the Joint Staff J7 announced that the U.S. Marine Corps Lesson Management System had been chosen as the starting point for development of the new system. In April 2007, the Joint Staff J7, Marine Corps Center for Lessons Learned, and JCOA signed a memorandum of agreement that codified responsibilities for establishing JLLIS, with MCLL providing the baseline system, JCOA providing help with integration, and J7 providing system requirements and executive sponsorship. After 2 years of development, integration, and testing, JLLIS reached initial operational capability and was ready for launch in January 2008. The Chairman signed out a CJCS Notice on January 22 establishing JLLIS as "the DoD system of record for the JLLP."[23] This notice was quickly followed in October 2008 by an out-of-cycle revision to the JLLP instruction, CJCSI 3150.25D, institutionalizing the decision.[24] The directive was clear in communicating the intent to make JLLIS a centerpiece of the JLLP, but actual adoption of this new tool by the greater DOD lessons learned enterprise would take some time. The greatest challenge to overcome was the existence of over 30 lessons learned systems that had proliferated throughout DOD since the mid-1980s.

Issuance of a directive did not bring about immediate compliance, but the campaign to bring others onboard gathered momentum. By August 2008, the initial baseline JLLIS had been installed in all 10 CCMDs, the four Services, and three combat support agencies (CSAs). Of these DOD organizations, about 50 percent were actively using JLLIS to some degree. Additionally, JLLIS had been installed but was not yet being used at the Department of State.[25] As successive versions of the JLLIS software were released, the number of participating organizations continued to grow, as did the number of observations entered in the system.

In addition to supporting the sharing and learning part of the JLLP, JLLIS was equipped with a capability to support an issue resolution process. This new capability was recognized in the 2009 revision to the JLLP guidance directive, CJCSI 3150.25D, with the addition of language referring to CCMD level issue resolution processes, especially USJFCOM issue resolution processes.

When USJFCOM was disestablished in 2010, the planners recognized that the command provided several major functions that had to continue. Follow-on organizations were identified to transition these functions without

interruption of service. JCOA had been providing one of those necessary functions. Given Joint Staff J7's policy and oversight role in the JLLP, it made sense to reunite the two parts of the JLLP under one organizational lead. JCOA remained physically in Suffolk, Virginia, presenting the challenges of physical and cultural separation to the balancing effort. JCOA continued to operate under its commander's program paradigm, while the J7 Pentagon element, the Joint Lessons Learned Branch (JLLB), continued to support and expand the use of JLLIS, enhancing the knowledge management and learning aspect of the program. When the first CJCS manual was published for the JLLP in February 2011 (CJCSM 3150.25), the role of the JLLB included supporting a Joint Staff Issue Resolution Process (IRP), which had emerged to support the activities of the LL GOSC. Eventually, both elements would be placed under a single general officer (Deputy Director for Future Joint Force Development), as separate divisions, each led by an O6, enabling a more active approach to balancing the two sides of the JLLP without taking away from either. Successive revisions to CJCSI 3150.25E/F and CJCSM 3150.25A in 2013–2015 would further refine roles and responsibilities for gathering, developing, and disseminating joint lessons learned and clarifying the IRP's place in the JLLP enterprise.

In March 2014, version 3.4 of JLLIS software was released and the system was declared to be at full operational capability. By this time, key stakeholders included the Office of the Secretary of Defense, Joint Staff, CCMDs, Services, National Guard Bureau, CSAs, and other U.S. Government interagency partners. The Australian Ministry of Defence completed a foreign military sales purchase of version 3.4 for its national lessons learned program. There were more than 111,000 active users worldwide, and the database contained over 295,000 observations and approximately 135,000 documents. The system was available on Secret Internet Protocol Router, Nonsecure Internet Protocol Router, Joint Worldwide Intelligence Communications System, and Five Eyes environments.

As the number of organizations and active users grew, the benefit of using one common system became more apparent. Operations and training exercises involving multiple headquarters, Service components, and support activities would be able to draw on each other's observations and issues before and after event execution. With the addition of a Collection and Analysis Plan module in 2014, units and organizations could also gain visibility on planned collection efforts to synchronize activities and avoid duplication of effort. None of this was even remotely possible in the years prior to JLLIS, with multiple noninteroperable repositories and support systems.

In the fiscal year 2014 National Defense Authorization Act, Congress formally recognized the additional responsibilities transferred from USJFCOM to the Chairman and expanded his authorities to include the functional areas of joint force development. One of those new authorities was "formulating policies for gathering, developing, and disseminating joint lessons learned for the armed forces."[26] The Chairman's new authority was incorporated into the most recent JLLP instruction (CJCSI 3150.25F), signed June 26, 2015. Additionally, a new DOD Directive (DODD), 3020.ab, *DoD Lessons Learned Program*, is being staffed and, if approved, will reinforce the imperative of lessons learned information-sharing by calling on all DOD components to use the Chairman's JLLP to improve capabilities and requiring them to use JLLIS to manage their lessons learned information.

While great progress has been made in the joint lessons learned program over the past 29 years since Goldwater-Nichols, some challenges do remain. First, as the JLLIS is populated by more observations, the inclusion of efficient, user-friendly search tools becomes increasingly important. While some improvements are soon to be fielded using IBM Watson Content Analytics (formerly IBM Content Analytics with Enterprise Search), more could and should be done as database search technologies continue to improve. Second, as the program continues to grow as a result of the directive guidance in DODD 3020.ab, the number of joint operational and strategic challenges to be addressed by the Joint Staff IRP is likely to expand. Ensuring there is adequate bandwidth, within the JLLP in general and the Joint Staff in particular, to execute this process will be critical to continued success. Finally, developing a more clearly defined rule set for the JLLP to foster information-sharing across organizations remains an incomplete task. Timeliness of data entry relative to the completion of a major operation or exercise, scope of data entered into the system, and the pace at which issues are resolved vary across the joint force. To an extent, this is predictable because no two operations or exercises are exactly alike, and such uniqueness of events invariably implies differences in how lessons learned data are shared. However, developing a set of minimum standards, and then producing metrics to measure progress toward meeting those standards, would be of considerable use in assessing the overall health of the JLLP as it seeks to support the objectives of both supporting commanders as well as sharing information across the joint force. The Joint Staff has embarked upon an initial effort to do so, but much more work remains to be done.

Notwithstanding these remaining challenges, the JLLP in 2015 is miles ahead of the disconnected and disjointed lessons learned programs in existence nearly three decades prior. A common system, and processes to share best practices and resolve issues, today postures the joint force for learning at the organizational level. Embedded within the journey from 1986 until today are lessons about lessons that may be applicable to other large organizations seeking to maintain the same balance between leader's programs focused on suborganizational improvement and information-sharing related to common challenges across the greater organization as a whole. While still imperfect, the story of the JLLP shows that it can be done. JFQ

Notes

[1] General Accounting Office (GAO), Comptroller General's Report to Congress of the United States, *Improving the Effectiveness of Joint Military Exercises—An Important Tool for Military Readiness*, LCD-80-2 (Washington, DC: GAO, 1979), 29.

[2] GAO, Report to the Secretary of Defense, *Management of the Joint Chiefs of Staff Exercise Program Has Been Strengthened, But More Needs to Be Done*, GAO-NSIAD-95-46 (Washington, DC: GAO, 1985), iii.

[3] Office of the Chairman of the Joint Chiefs of Staff (CJCS), *Organizational Development of the Joint Chiefs of Staff, 1942–2013* (Washington, DC: Joint History Office, 2013), 63.

[4] Joint Staff Memorandum 251-87, *Director for Operational Plans and Interoperability Concept of Operations* (Washington, DC: The Joint Staff, 1987).

[5] Alan D. Landry, "The Joint Lessons Learned System and Interoperability" (master's thesis, U.S. Army Command and General Staff College, 1989).

[6] Army Regulation 11-33, *Army Lessons Learned Program* (Washington, DC: Headquarters Department of the Army, 2006), 1.

[7] Air Force Instruction 90-1601, *Air Force Lessons Learned Program* (Washington, DC: Headquarters Department of the Air Force, 2013), 8.

[8] Marine Corps Order 3504.1, *Marine Corps Lessons Learned Program (MCLLP) and the Marine Corps Center for Lessons Learned (MCCLL)* (Washington, DC: Headquarters Department of the Navy, 2006), 1.

[9] CJCS 234-90, *Remedial Action Project Program* (Washington, DC: The Joint Staff, 1990).

[10] Administrative Publication 1.1, *Organization and Functions of the Joint Staff* (Washington, DC: The Joint Staff, 1988), III-8-1.

[11] GAO, Report to the Chairman, Subcommittee on Military Personnel, Committee on National Security, House of Representatives, *Military Training: Potential to Use Lessons Learned to Avoid Past Mistakes Is Largely Untapped*, GAO/NSIAD-95-152 (Washington, DC: GAO, 1995), 2.

[12] Ibid.

[13] Hugh Barker, "The Transformation of the Joint Lessons Learned Program, 1996–11 September 2001," unpublished white paper, Joint Center for Operational Analysis, 2006.

[14] *Executive Summary: Joint Center for Lessons Learned (JCLL) Implementation Plan* (Washington, DC: The Joint Staff, 1996, rev. 1997).

[15] Barker.

[16] Ibid.

[17] Ibid.

[18] CJCS Instruction 3150.25C, *Joint Lessons Learned Program* (Washington, DC: The Joint Staff, 2007), enclosure C.

Joint Publications (JPs) Under Revision (to be signed within 6 months)

JP 1-04, *Amphibious Embarkation and Debarkation*
JP 2-01.2, *Counterintelligence/Human Intelligence*
JP 3-13.3, *Operations Security*
JP 3-14, *Space Operations*
JP 3-34, *Engineer Operations*
JP 3-68, *Noncombatant Evacuation Operations*
JP 4-01.2, *Sealift Support to Joint Operations*
JP 4-01.5, *Joint Terminal Operations*
JP 4-03, *Joint Bulk Petroleum and Water Doctrine*

JPs Revised (signed within last 6 months)

JP 1-0, *Joint Personnel Support*
JP 3-05.1, *Unconventional Warfare*
JP 3-50, *Personnel Recovery*
JP 3-61, *Public Affairs*
JP 6-0, *Joint Communications System*

[19] CJCS Memorandum CM-1318-03, *Expansion of Joint Lessons Learned—The Next Step* (Washington, DC: The Joint Staff, 2003).

[20] Commander, U.S. Joint Forces Command (USJFCOM) Memorandum, *Expanding the Lessons Learned Effort, J00 9 Dec 03* (Norfolk, VA: USJFCOM, 2003).

[21] Commander, USJFCOM Directive 5100.4, *Charter for the Joint Center for Operational Analysis* (Norfolk, VA: USJFCOM, 2007).

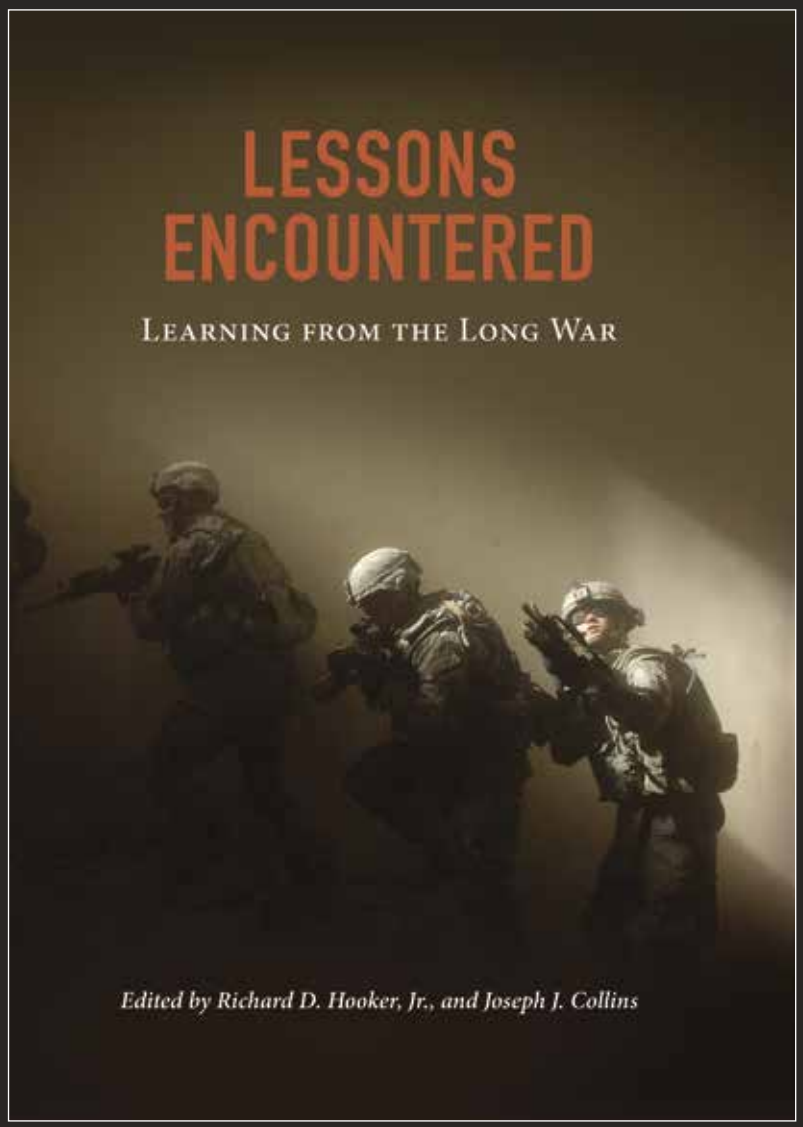
[22] *Enhanced Joint Lessons Learned Program Study Report* (Washington, DC: The Joint Staff, 2004).

[23] CJCS Notice 3150.25, *Joint Lessons Learned Program and Joint Lessons Learned Information System* (Washington, DC: The Joint Staff, 2008).

[24] CJCS Instruction 3150.25D, *Joint Lessons Learned Program* (Washington, DC: The Joint Staff, 2008).

[25] *Joint Lessons Learned Program and Joint Lessons Learned Information System*, B.7.g.

[26] 10 U.S. Code §153 (a)(5), *Chairman: Functions: Joint Force Development Activities* (Washington, DC: U.S. Government Printing Office, 2014).



NEW from NDU Press

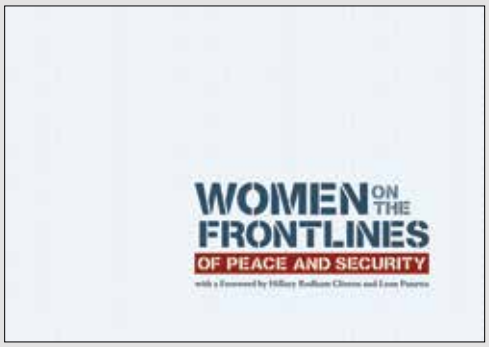
Lessons Encountered:
Learning from the Long War
NDU Press, 2015 • 488 pp.

This volume began as two questions from General Martin E. Dempsey, 18th 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



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

Have you checked out NDU Press online lately?

With 20,000 unique visitors each month, the NDU Press Web site is a great place to find information on new and upcoming articles, occasional papers, books, and other publications.

You can also find us on:

Facebook **Flickr**

Twitter **Pinterest**

Visit us online at: **http://ndupress.ndu.edu**

JFQ is available online at the Joint Electronic Library:
www.dtic.mil/doctrine/jfq/jfq.htm

JFQ
JOINT FORCE QUARTERLY
Published for the Chairman of the Joint Chiefs of Staff by National Defense University Press
National Defense University, Washington, DC
NDU Press