



Military Review

THE PROFESSIONAL JOURNAL OF THE U.S. ARMY

May-June 2014

Considerations for Offensive Cyberspace Operations p4

Lt. Cmdr. Kallie D. Fink, U.S. Navy; Maj. John D. Jordan, U.S. Marine Corps;
and Maj. James E. Wells, U.S. Air Force

Failed Cyberdefense p22

Jan Kallberg, Ph.D., and Rosemary A. Burk, Ph.D.

Beyond Cocaine Cowboys p34

Maj. Gen. Frederick S. Rudesheim, U.S. Army,
and Maj. Michael L. Burgoyne, U.S. Army

Medical Operations in Counterinsurgency p56

Maj. David S. Kauvar, M.D., U.S. Army;
Maj. Tucker A. Drury, M.D., U.S. Air Force



<http://militaryreview.army.mil>

PB-100-14-3/4
Headquarters, Department of the Army
PIN: 104200-000
Approved for public release; distribution is unlimited

COMBINED ARMS CENTER, FORT LEAVENWORTH, KANSAS



WELCOME to the first ever full-color issue of *Military Review*. We think color will add a positive dynamic and enhance the quality of our journal. A special thank you to the staff at our Leadership, Development, and Education headquarters for finding a way to fund this endeavor.

Our first themed edition (March-April) focused on leadership development. This edition is dedicated to cybersecurity and network-centric warfare. Inside this edition you will find articles on robotic

warfare, cyberattacks and the environment, cyberspace operations and the targeting cycle, and other fascinating concepts addressing cyber threats to the United States military.

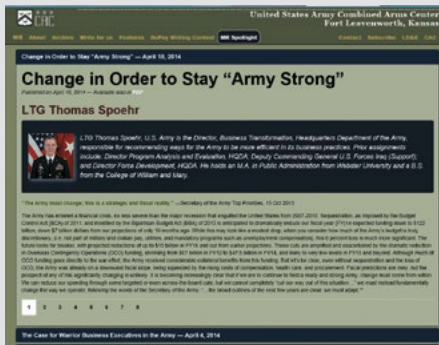
Inside the back cover, you will find a dedication to 24 Medal of Honor recipients from three wars who were honored for their uncommon bravery by President Obama in a ceremony on 18 March. The soldiers, originally awarded the Distinguished Service Cross, were of Hispanic, Jewish, and African-American descent. Their awards were upgraded due to a congressionally mandated review of awards to ensure heroism of veterans was not overlooked due to prejudice or discrimination.

We also have some great articles online at our new website addition—*Military Review Spotlight*. This site provides a platform *now* to discuss relevant issues and concepts. A new article is posted each week. You can find it at <http://usacac.army.mil/CAC2/MilitaryReview/repository/spotlight/spotlight.asp>.

There is still time to enter the William E. DePuy Combined Arms Center Writing Competition. The topic is “How can the Army maintain its adaptability and agility and find innovative solutions to face future threats during this time of workforce reductions?” The deadline for submission is 7 July 2014. You can find entry details on our website at <http://usacac.army.mil/CAC2/MilitaryReview/repository/DePuyWritingContestInformation2014.pdf>.

Visit *Military Review* online at <http://usacac.army.mil/CAC2/MilitaryReview/index.asp>. There you will find current and archived editions of the journal, as well as directions on how to submit your manuscripts for inclusion in our publication. You can also like us on Facebook at <https://www.facebook.com/OfficialMilitaryReview>.

I hope you enjoy the May-June edition of *Military Review*. Thanks to all our readers and very talented authors for their continued support.



MR Spotlight



Themes for Future Editions

2014

- July-Aug Strategic Landpower
- Sep-Oct Soldier and Noncommissioned Officer Development and Leadership
- Nov-Dec Budget Constraints and Maintaining Readiness

2015

- Jan-Feb Training Management: Lost Art or Wave of the Future?
- Mar-Apr The Army and the Congress: Who Really Should Have Responsibility and Authority for Preventing and Responding to Sexual Harassment and Sexual Assault?
- May-June Ready and Resilient Campaign: Challenges, Issues, Programs



Military Review

Lt. Gen. Robert B. Brown
Commander, USACAC
Commandant, CGSC

Brig. Gen. Chris Hughes
Deputy Commanding General, CGSC

Col. Anna R. Friederich-Maggard
Director and Editor in Chief

Military Review Staff

Lt. Col. James Lowe
Associate Editor

Maj. Efrem Gibson
Executive Officer

Marlys Cook, Lt. Col., USA (Ret.)
Managing Editor

Jeffrey Buczkowski, Lt. Col., USA (Ret.)
Senior Editor

Desirae Gieseeman
Associate Editor

Nancy Mazzia
Books and Features Editor

Julie Gunter
Visual Information Specialist

Linda Darnell
Administrative Assistant

Michael Serravo
Visual Information Specialist, Webmaster

Editorial Board Members

Command Sgt. Maj. Joe B. Parson Jr.
LD&E Command Sergeant Major

Clinton J. Ancker III, Director,
Combined Arms Doctrine Directorate

Robert Baumann, Director,
CGSC Graduate Program

Lester W. Grau
Foreign Military Studies Office

John Pennington, Chief,
Media Division,

Center for Army Lessons Learned

Col. Christopher Croft, Director,
Center for Army Leadership

Thomas Jordan
Deputy Director, MCCoE

Col. Thomas E. Hanson
Director, Combat Studies Institute

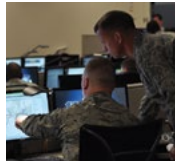
Mike Johnson
Combined Arms Center-Training

Col. Denton Knapp
Center for the Army Profession and Ethic

Consulting Editors

Col. Hertz Pires Do Nascimento
Brazilian Army, Brazilian Edition

Lt. Col. Claudio Antonio Mendoza Oyarce
Chilean Army, Hispano-American Edition



4

Considerations for Offensive Cyberspace Operations

Lt. Cmdr. Kallie D. Fink, U.S. Navy; Maj. John D. Jordan, U.S. Marine Corps; and Maj. James E. Wells, U.S. Air Force

Integrating offensive cyberspace operations into the joint targeting cycle presents distinct challenges for commanders and planners. Officers from three services provide considerations and recommendations for commanders to take full advantage of this combat multiplier.



12

Responsibility Practices in Robotic Warfare

Deborah G. Johnson, Ph.D., and Merel E. Noorman, Ph.D.

The authors discuss the issues of responsibility and accountability inherent to the use of autonomous robotic systems. They espouse the incorporation of responsibility practices during the development of new technologies.



22

Failed Cyberdefense: The Environmental Consequences of Hostile Acts

Jan Kallberg, Ph.D., and Rosemary A. Burk, Ph.D.

Defending against cyberattacks is more than just protecting computer networks. The authors discuss weaknesses in our cyberdefense and convey a warning that cyberattacks could cause long-term environmental damage.



26

The Utility of Cyberpower

Lt. Col. Kevin L. Parker, U.S. Air Force

The Department of Defense considers cyberspace an operational domain with distinctive characteristics that present advantages and corresponding limitations. An Air Force officer explains the importance of integrating cyberspace operations in a strategic context and discusses the way ahead.

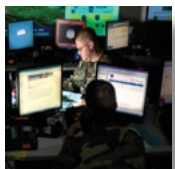


34

Beyond Cocaine Cowboys: Looking at Security in Latin America from a Different Perspective

Maj. Gen. Frederick S. Rudesheim, U.S. Army, and Maj. Michael L. Burgoyne, U.S. Army

The authors draw on their extensive regional expertise to show that U.S. security cooperation policy in Latin America needs to extend beyond the fight against drug trafficking.

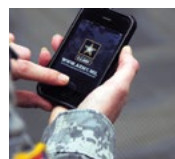


38

Cybersecurity: It Isn't Just for Signal Officers Anymore

Lt. Col. D. Bruce Roeder, U.S. Army, Retired

The author discusses a variety of cyberthreats and how the United States should combat them. He shows why cybersecurity is everyone's business.



43

Network-Centric Warfare and the Data-Information-Knowledge-Wisdom Hierarchy

Col. Harry D. Tunnell IV, U.S. Army, Retired

Integration of a data-information-knowledge-wisdom hierarchy into a network-centric-capable information system framework can enhance leader decision making in combat.



51 Is There Room for Peace Studies in a Future-Centered Warfighting Curriculum?

Maj. Thomas G. Matyók, Ph.D., U.S. Army, Retired; Cathryne L. Schmitz, Ph.D., MSW

The authors believe peace and conflict studies should be integrated into the Army's professional education curriculum. They show how this approach to educating soldiers could provide the skills to resolve conflicts through nonviolent conflict management.



56 Medical Operations in Counterinsurgency: Joining the Fight

Maj. David S. Kauvar, M.D., U.S. Army; Maj. Tucker A. Drury, M.D., U.S. Air Force

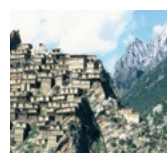
Two military physicians present lessons learned in Afghanistan for the successful employment of U.S. medical units during counterinsurgency operations.



62 Persistent Conflict and Special Operations Forces

Lt. Col. Phillip W. Reynolds, U.S. Army

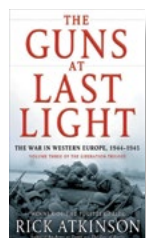
Special operations forces and an interagency mindset are the keys to success in low-intensity and irregular wars, especially in this time of reduced resources and war weariness, according to one civil affairs officer.



70 **INSIGHT:** COINvasion? Korengal and Weygal Valleys Post-Mortem

Maj. David H. Park, U.S. Army

A veteran of five combat tours gives an enlightening discourse on the strategic and human terrain in a remote region of Afghanistan. His analysis demonstrates the errors of the U.S. approach there and offers strategies for operating more effectively in the region.



78 **REVIEW ESSAY** THE GUNS AT LAST LIGHT: The War in Western Europe, 1944-1945

Col. A M Roe, Ph.D., British Army

83 **BOOK REVIEWS** CONTEMPORARY READINGS FOR THE MILITARY PROFESSIONAL

94 **WE RECOMMEND**

95 General William E. Depuy Combined Arms Center Writing Competition Announcement

The Secretary of the Army has determined that the publication of this periodical is necessary in the transaction of the public business as required by law of the department. Funds for printing this publication were approved by the Secretary of the Army in accordance with the provisions of Army Regulation 25-30.

Raymond T. Odierno
General, United States Army
Chief of Staff

Official:

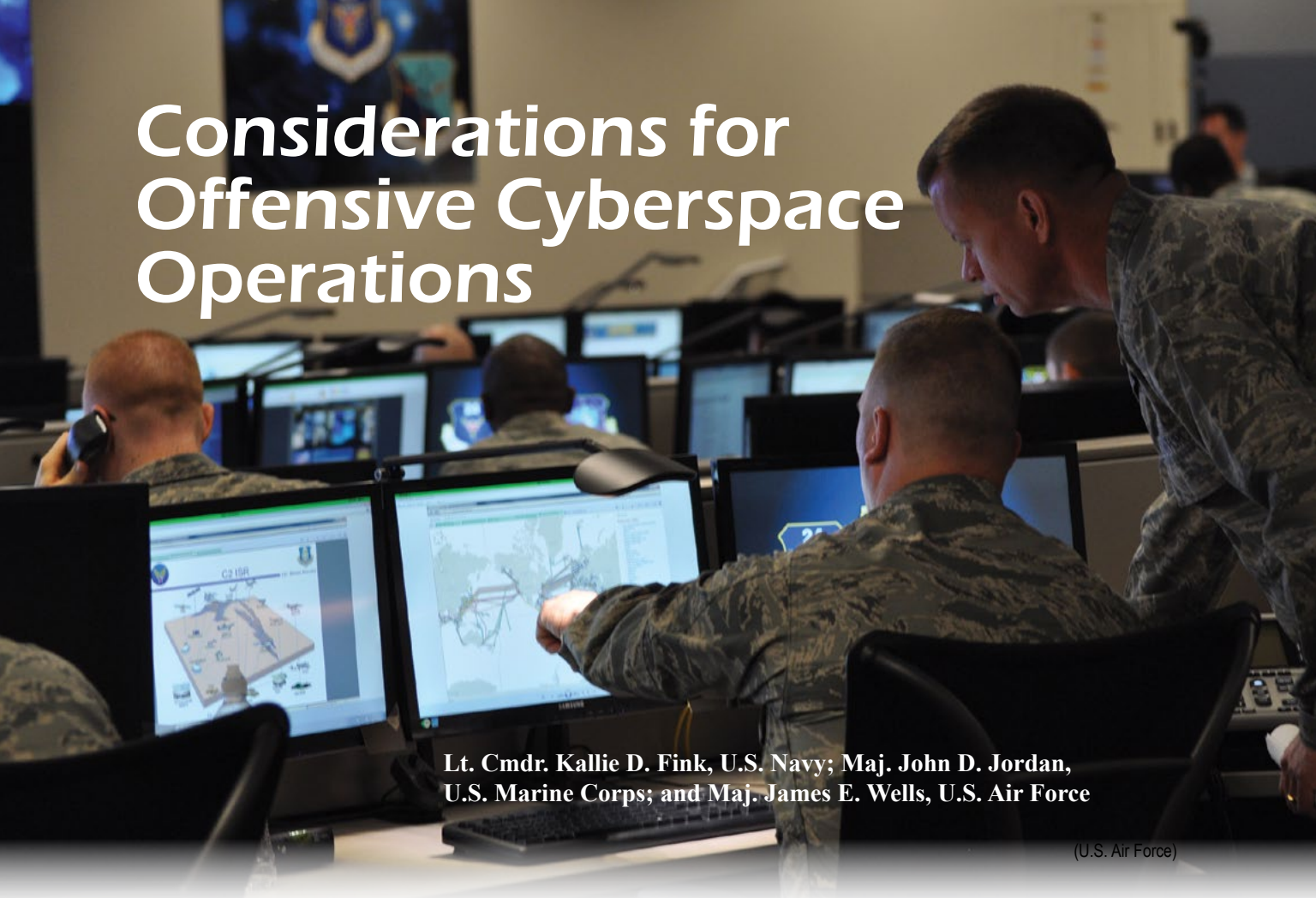
GERALD B. O'KEEFE
Administrative Assistant to the
Secretary of the Army

Authentication no. 1411302

Military Review presents professional information, but the views expressed herein are those of the authors, not the Department of Defense or its elements. The content does not necessarily reflect the official U.S. Army position and does not change or supersede any information in other official U.S. Army publications. Authors are responsible for the accuracy and source documentation of material they provide. *Military Review* reserves the right to edit material. Basis of official distribution is one per 10 officers for major commands, corps, divisions, major staff agencies, garrison commands, Army schools, Reserve commands, and Cadet Command organizations; one per 25 officers for medical commands, hospitals, and units; and one per five officers for Active and Reserve brigades and battalions, based on assigned field grade officer strength. *Military Review* is available online at <http://militaryreview.army.mil>.

Military Review (US ISSN 0026-4148) (USPS 123-830) is published bimonthly by the U.S. Army, CAC, Fort Leavenworth, KS 66027-1293. Paid subscriptions are available through the Superintendent of Documents for \$42 US/ APO/FPO and \$58.80 foreign addresses per year. Periodical postage paid at Leavenworth, KS, and additional mailing offices. POSTMASTER: Send address changes to Military Review, CAC, 290 Stimson Avenue, Unit 2, Fort Leavenworth, KS 66027-1254.

Considerations for Offensive Cyberspace Operations



Lt. Cmdr. Kallie D. Fink, U.S. Navy; Maj. John D. Jordan, U.S. Marine Corps; and Maj. James E. Wells, U.S. Air Force

(U.S. Air Force)

OFFENSIVE CYBERSPACE OPERATIONS (OCO) have become ubiquitous over the last decade, and their inclusion in deliberate planning is increasing. However, much of this inclusion is *pro forma*, as OCO are in many ways inscrutable to those who are not familiar with them. Moreover, the joint targeting cycle does not take into account the distinct characteristics of OCO. Improvements to the institutional perception of OCO and the integration of OCO into the joint targeting cycle would enable joint task force (JTF) commanders to make the most of this potent capability during deliberate planning.

Lt. Cmdr. Kallie D. Fink, U.S. Navy, is an information warfare officer assigned to Navy Information Operations Command Maryland. She holds a B.A. in German from the University of Minnesota and an M.S. in strategic intelligence from the National Intelligence University. Lt. Cmdr. Fink previously served as the deputy executive assistant to the Deputy Chief of Naval Operations for Information Dominance (N2/N6).

Maj. John D. Jordan, U.S. Marine Corps, is assigned to the Joint Staff J-7, Joint Force Development, as an operations research analyst working on cyberspace projects. He holds a B.S. in aerospace engineering from the University of Virginia and an M.S. in operations research from the Naval Post Graduate School. Major Jordan is a CH-46E pilot, and his previous assignments include flying casualty evacuation missions in Iraq, humanitarian assistance missions throughout United States Pacific Command, and service as a forward air controller in Afghanistan.

Maj. James E. Wells, U.S. Air Force, is assigned to the National Geospatial-Intelligence Agency as the chief of joint requirements programs. He holds a BFA in visual communications and an M.A. in human relations from the University of Oklahoma. Maj. Wells previously served as the chief of 3d Wing exercises and plans at Joint Base Elmendorf-Richardson, Alaska.

However, two main problems hinder effective inclusion of OCO in deliberate operational planning. The first problem is that planning staffs have misconceptions about OCO capabilities and limitations within an operational environment. Moreover, staffs are uncomfortable with the highly classified and technically complex aspects of the cyberspace domain because they do not understand them. The second problem is that OCO do not fit neatly into the joint targeting cycle and require much extra work and time to incorporate into deliberate planning.

Misconceptions About and Challenges to the Operational Employment of OCO

Among the many common misconceptions about OCO, two are particularly significant. The first misconception is that OCO are nonlethal enablers that play a marginal role in operations. The second is that since details of OCO are either inscrutable due to their technical complexity or inaccessible due to their classification, they are not worth the trouble of trying to employ at an operational level.

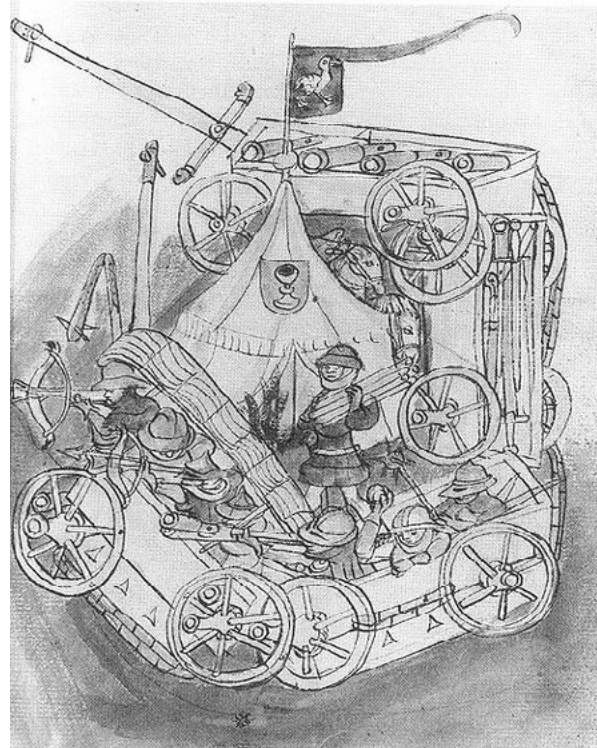
The “it’s just computers” misconception. A common perception among planners is that OCO are nonlethal means of attacking an opponent’s networks, with little physical effect. However, over the last decade OCO have become more than just a nonlethal enabler like electronic warfare. The nature and potential of OCO have not changed significantly, but our understanding of them has.

A revolutionary weapon system typically starts out as an asymmetric weapon that can, under favorable conditions, be used to counter traditional forms of military power. A historical example is the use of gunpowder weapons in the hands of the Hussites, a band of 15th-century religious dissenters who used primitive firearms to defeat armored knights.¹ In the 21st century, offensive cyberspace capabilities can give state and nonstate actors a new asymmetric weapon to use against traditional seats of power.

An event in Estonia in 2007 is considered by some to represent the first offensive cyberspace attack against a nation. It began after the Estonian government removed a World War II Soviet war memorial commemorating a Russian victory over the Nazis.² The Estonian government suspected

Russia of coordinating subsequent retaliatory cyber strikes at Estonia’s digital infrastructure, government command and control (C2), financial institutions, and media networks.³ The massive attacks shut down government agencies’ emails, published false documents, and severely limited Internet access. The digital bombardment lasted two weeks and forced a major bank, Hansabank, to shut down online services for more than an hour; its losses eventually were estimated around \$1 million.⁴ The denial and disruption of government, media, and financial networks caused confusion and chaos without physical damage or destruction. The attack did great economic damage to Estonia. Coordinating a defensive response was very difficult because the attack was so widely dispersed—no single Estonian authority was responsible for defense of so many different cyberspace assets.⁵

How new asymmetric weapons become integrated into a standard military arsenal. After military forces have used a new asymmetric weapon successfully, they sometimes adopt it as a complement to the traditional military arsenal. For



Hussite Wagon, Alois Niederstätter, 15th century (Archive of the Austrian National Library)

example, by the 16th century, armies had combined muskets with pikes and armored knights. During the 2008 Russian-Georgian War, some speculated that Russian forces integrated OCO with traditional operations to enhance their overall operational effectiveness. The Russians evidently conducted numerous cyberspace attacks that rendered Georgia's governmental and media networks inoperable.⁶ These attacks severely disrupted Georgian military C2. They were synchronized with the Russian troops' crossing of the Georgian border.⁷ Cyber expert Eli Jellenc stated this event represented "the birth of true, operational cyber warfare," as it appeared to be the first coordinated usage of cyber and conventional attacks on a nation state.⁸

A complementary weapon eventually can evolve into a primary weapon. For example, the musket equipped with a socket bayonet replaced the pike by the early 18th century as the universal infantry arm. In 2010, a computer worm known as Stuxnet evidently was used as a primary offensive weapon to create tangible operational effects. Stuxnet, while of unknown origin, was a "fire and forget" program, considered the world's first "cyber missile."⁹ The program apparently was deployed to sabotage Iran's nuclear fuel-refining centrifuges, which could be used to develop weapons-grade uranium, by altering the electrical current.¹⁰ According to German

researcher Ralph Langner, the attack may have been intended to destroy the centrifuge rotor by vibration—which could cause the centrifuge to explode—or simply to degrade the output over time (by slowing down and speeding up the motor).¹¹ Stuxnet—although delivered through what is perceived as a nonphysical and nonlethal domain—achieved decidedly physical effects by damaging Iranian nuclear facilities.

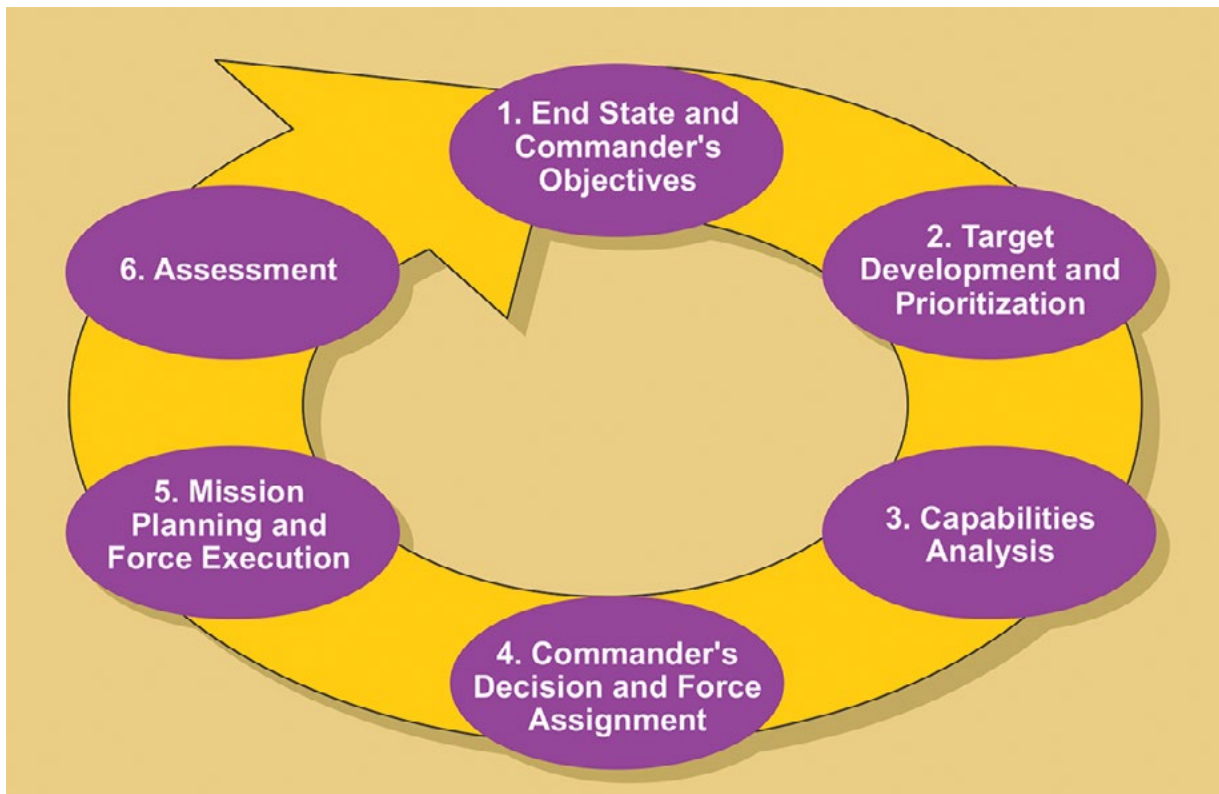
The examples from Iran and Georgia show how OCO have produced effects ranging from non-physical harassment and information operations through physical damage to key infrastructure. Without forces or weapons having direct physical contact, OCO can create nonphysical and physical operational effects. They can shut down air defense systems and C2 nodes, open or close a dam's floodgates, and destroy or damage industrial machines such as nuclear centrifuges.¹² Offensive cyberspace capabilities, like standard lethal and tangible weapons, can be arrows in a JTF commander's quiver. They can enable a commander to address a range of targets efficiently, on their own or in conjunction with other weapons.

The "I don't understand it" or "I can't get to it" misconception. Cyberspace capabilities, particularly OCO, tend to be shrouded in secrecy. OCO are highly classified because the nature of

these operations could divulge strategic and operational intentions if they are revealed. If a hostile power learned about even one OCO target under development, that power could learn much about U.S. cyberspace capabilities and a combatant command's operations. If certain enemies learned that an operation plan featuring them as a target involved a cyberspace attack on an infrastructure node, they could use U.S. military doctrine to develop some understanding of the plan. Further, if technical data were compromised, an



An Iranian technician works at the Uranium Conversion Facility just outside the city of Isfahan 255 miles south of Tehran, Iran, 3 February 2007. (AP Photo/Vahid Salemi)



Joint Targeting Cycle

opponent could use the data to design and build a cyber weapon to attack U.S. or allied interests.

In addition to the challenges of secrecy, the technical aspects of cyberspace operations are difficult to grasp for those without technical training. This is especially so in comparison to traditional weapon systems. Cyberspace is not like the traditional physical domains where we can touch and see all the parts. Rather, cyberspace is primarily a virtual realm that can be manipulated to achieve real-world effects in the air, land, maritime, and space domains. Putting a bomb on target is easier to visualize than launching a multihost cyber attack that will penetrate a network and eventually weaken or destroy a critical system.¹³

Marginalization by inaccessibility. Whether the issue is difficulty in understanding, getting access to, or employing technically complex cyberspace capabilities—inaccessibility can marginalize OCO more than any opponent’s defenses. Unfortunately, inaccessibility can make operational planners apathetic about employing OCO. They may regard “cyberspace operations” as a buzzword the boss

wants to pay lip service to rather than a set of weapons and tactics that deliver tangible benefits. At best, OCO can become marginalized—employed on the fringes of operations as they are not understood, not accessible, not easy to employ, and not trusted.

The joint targeting cycle. In addition to the common misconceptions and inaccessibility issues surrounding OCO, certain challenges are inherent to fitting OCO into the joint targeting cycle (see figure).¹⁴ Two phases of the joint targeting cycle—target development and prioritization, and capabilities analysis—have the most significant upstream effect on planning the operational employment of OCO.

United States Cyber Command (USCYBERCOM) coordinates the desired cyberspace effects against a target, based on the priorities of the combatant commander or JTF commander. During contingency planning, the capabilities analysis phase seeks to match apportioned assets and ordnance with the target and effect desired. Once a target is selected to be serviced by traditional means, it is periodically

reviewed during the plan review cycle. No further resources are expended on maintaining access to the target until the plan is executed. By contrast, designating a target to be engaged with OCO starts the immediate allocation and expenditure of additional resources. Maintaining and developing a target requires a significant amount of time. During Operation Odyssey Dawn in 2011, U.S. officials debated the use of OCO against Libya but decided against it for several reasons—mainly because of time. Analysts at the *New York Times* reported that “in reality it takes significant digital snooping to identify potential entry points and susceptible nodes in a linked network of communications systems, radars and missiles like that operated by the Libyan government, and then to write and insert the proper poisonous codes.”¹⁵

How the joint targeting cycle applies to OCO.

The first step to engage a target with OCO is to gain access to it. Without physical or electronic access to the target, it is impossible to proceed with OCO. A system linked to the Internet is, in general, more accessible, though getting into its targeted portions may be challenging due to its own network security environment. A closed system, such as the Iranian nuclear program, would require insider access to gain firsthand knowledge of the computing environment in the target facility.¹⁶ Once forces gain access to a target system, they need to maintain it as long as they might wish to strike the target. Network upgrades or system changes made in the regular maintenance of the target could make it difficult to maintain or regain access. The risk from gaining access to a system is that an adversary might detect the hacking well before the attack. The adversary would discover which systems were being targeted. Moreover, discovery would assuredly result in access being lost—and the possibility of the adversary studying the attack to understand U.S. cyberspace operations and develop better defenses or even counterattacks.

Once access is gained, the next step is to learn the unique internal attributes of the targeted system. Cyber attackers may need to acquire the software being targeted so they can determine its nature and vulnerabilities. For commercially available systems, this is relatively easy to do—a copy can be purchased. For rare systems or those whose development and use are limited to a given

country or region, forces might need to obtain insider knowledge of the network environment (as may have occurred with Stuxnet).¹⁷ Depending on the system to be attacked, the code might be commented in a language other than English. For whatever reason, if USCYBERCOM is unable to gain technical insight into the targeted software, then OCO cannot proceed; coordinating the proper effect is impossible. The JTF commander must consider these attributes of OCO when setting target priorities during deliberate planning.

Once USCYBERCOM has coordinated a means for continuous access and learned the targeted system, they must then coordinate acquisition or development of the weapon with which to attack it. Some weapons designed to attack common operating systems such as Windows are commercially available. However, systems produced and used only in certain countries typically require forces to develop weapons from scratch. This becomes a software acquisition project, in both the technical and legal sense. For purposes of defense acquisition, software development projects are more complex than physical engineering projects.¹⁸ Developing a cyber weapon is a complex challenge for this reason and many others. Once a weapon has been developed, the attackers must constantly maintain access to and monitor the target. They must ensure routine system maintenance does not nullify their labors until the weapon is employed, or until the target is removed from the joint integrated prioritized target list (JIPTL).

OCO force assignment challenges. All of these actions require a significant amount of time, perhaps months, before anything besides a rudimentary attack can be launched with a presumption of success. Furthermore, depending on the target and its accessibility, a weapon may need to navigate through several networks to its intended target. According to cyber forensics analysts, Stuxnet may have infected its target environment through a removable device inserted by a willing or unwitting third party or insider.¹⁹ Stuxnet would have needed numerous developers working up to six months to infect target computers in the Iranian nuclear program’s closed network.

Currently, USCYBERCOM coordinates all OCO, with the concurrence of the appropriate combatant command. This further complicates the challenge

of matching targets to weapons. Not only must a combatant command request USCYBERCOM to attack a target, but also each target in the command's JIPTL competes for resources against targets in the JIPTLs of other commands. USCYBERCOM sorts through all of these lists, assigning a global priority to individual targets and allocating scarce resources to them. Even if USCYBERCOM considers a target high priority, the command may not have the resources needed to service it. USCYBERCOM needs to inform combatant commands and JTFs of its ability to service targets on their JIPTLs.

Onerous legal reviews. Stewart A. Baker, former Department of Homeland Security assistant secretary for Policy and Technology, suggests that U.S. legal interpretation of the Hague Conventions reduces the operational utility of OCO.²⁰ He writes that “lawyers across the government have raised so many show-stopping legal questions about cyberwar that they’ve left our military unable to fight, or even plan for, a war in cyberspace.”²¹

Part of this legal complexity stems from the nature of OCO. As noted above, any but the most rudimentary cyberspace attack on an enemy requires the acquisition, development, or modification of software to engender the effects that a JTF commander desires. This brings Department of Defense Directive (DODD) 5000.01, *The Defense Acquisition System*, into the process. DODD 5000.01 requires that “the acquisition or procurement of DOD weapons and weapon systems shall be consistent with all applicable domestic law and treaties and international agreements.”²² In regard to Air Force operations, Air Force Instruction 51-402 states that the office of the Judge Advocate General of the Air Force will conduct legal reviews of any new cyberspace capabilities (including weapons) or any contemplated modification of a cyberspace capability to ensure legality under the Law of Armed Conflict (LOAC), domestic law, and international law.²³ A traditional attack on a target with missiles and bombs only has to pass through legal scrutiny during target development and prioritization since the weapons being employed have long since passed their assessment (per DODD 5000.01) during acquisition. By contrast, since cyberspace weapons are unique for almost every target, Air Force OCO require two legal reviews: one during target validation and the second during the acqui-

sition process. This puts conducting OCO at the mercy of the most restrictive reading of the LOAC by two separate legal teams.

This constraint, and the general ambiguity of how the LOAC applies to cyberspace operations, has created what Stewart Baker interprets as “a cyberwar strategy that simply omitted

Cyberspace, including OCO awareness, should be part of every officer's basic accession curriculum.

any plan for conducting offensive operations. Apparently, they're still waiting for all these lawyers to agree on what kind of offensive operations the military is allowed to mount.”²⁴

Solutions

Clarifying the perception of OCO. Education is the key to changing how we think, plan for, and employ OCO. Cyberspace, including OCO awareness, should be part of every officer's basic accession curriculum. Joint professional military education (JPME) level I should include foundational cyberspace operations and doctrine for all officers. Intermediate and senior officers should study and integrate operational and strategic cyberspace operations into joint planning through JPME II. In addition, capstone courses should include instruction in the capabilities and limitations of OCO. The goal of this education should not be to turn officers into cyber specialists, but to give them the same basic awareness of this domain that officers who are in supporting or combat arms fields have of how those in the other fields conduct their profession.

Not unlike the intricacies of sophisticated conventional weapon systems, the details of OCO should remain classified. This is an attribute of cyberspace operations that must be taken into account when targeting: knowledge of the specific processes by which cyber effects are achieved should be limited to those with a need to know. The inaccessibility

of offensive cyberspace capabilities—to anyone not working directly on developing and executing them—contributes a level of operational security that will support the capability over time. Additionally, maintaining a level of inaccessibility surrounding the offensive cyberspace capabilities affords the option to mask operational intent. Most joint planners do not possess the knowledge or security clearance to know how to build a Tomahawk cruise missile from scratch; nor should joint planners have the access to dissect an offensive cyberspace capability.

An example of this paradox is the espionage virus Flame, discovered in 2012 and thought to have circulated on the Internet approximately four years before detection.²⁵ According to Debra Van Opstal, Flame “exploited the Windows operating system to capture audio, screenshots, keyboard activity, and network traffic information from infected computers.”²⁶ Whoever decided to employ Flame likely did not understand the intricacies of its inner workings, but they did understand the desired effect. Flame is just one example of an offensive cyberspace tool that is difficult to detect, but its complex nature offers a unique perspective into the level of detail required to produce a pervasive cyber effect. The challenge for the combatant command and JTF staffs is accepting and operating in this borderless environment, which may involve hitting the “I believe” button when vetting desired, prioritized effects through USCYBERCOM.

Improvements to the joint targeting cycle. To better utilize OCO capabilities, joint targeting coordination boards (JTCBs) must change how they assemble their JIPTLs; they must coordinate cyber target nomination with USCYBERCOM. This will enable the JTCBs to enhance OCO utilization, while fully integrating cyberspace capabilities with the traditional land, air, and sea power.

Iterative capabilities analysis. Each JTCB should have a cyberspace representative assigned to it. The representative should be coequal with the joint force air, land, and maritime component command representatives. The cyberspace representative should provide a cyberspace target nomination list to the JTCB. When the JTCB begins to synthesize the target nomination lists into the draft JIPTL, the cyberspace representative can coordinate the draft JIPTL with USCYBERCOM. With this infor-

mation, USCYBERCOM can inform the JTCB as to which targets are considered susceptible to OCO, enabling the board to better shape the JIPTL. In addition, this practice will allow USCYBERCOM to look for possible synergies with work it is already undertaking for other plans. This information sharing will shape the design of the JIPTL and enable the JTCB to integrate OCO into its design.

To get the best results from OCO, the JTCB also needs to ensure that targets for OCO are enduring. The JTCB needs to focus on the effects needed rather than how the effects are generated. Enduring targets are necessary because they allow USCYBERCOM to most efficiently coordinate resources and avoid chasing fleeting targets. An enduring target should be one that will persist through multiple plan review cycles. This gives USCYBERCOM enough time to develop the weapons needed to engage it successfully. Moreover, a focus on effects will enable USCYBERCOM to propose alternate courses of action to the JTCB. This will allow the JTCB to maintain focus on the big picture rather than the details of OCO. The cyberspace representative to the JTCB should be more than capable of deconflicting and coordinating OCO with the rest of the JIPTL.

Coordination of global OCO assignment. Each JTCB must remain flexible regarding its JIPTL, as USCYBERCOM’s requirement to provide global support means that resources may shift. Whether for priority changes or other reasons, not every target on every JIPTL will be serviced. USCYBERCOM must inform each JTCB of the status of its targets, especially when priorities change, as this may have a significant effect on a command’s JIPTL. Each JTCB must prepare itself for this possibility by developing branch JIPTLs that reflect the lack of access to a cyberspace target. This again requires the JIPTL to be continuously reviewed and updated instead of sitting on the shelf until the next operation plan review. The direct link afforded by the cyberspace representative makes this less onerous, but it will require the JTCB to conduct extra research and planning to meet the commander’s desired end state. The temptation remains, of course, to ignore or marginalize cyberspace capabilities because using them would cause frustration and extra work. The JTCB must weigh the potential payoff of OCO with the extra workload this may inflict during deliberate

planning. However, successful integration of OCO can enable a JTF to expand its reach beyond what traditional fires assets would allow, and to husband those assets for more suitable targets.

Consolidated legal review. The legal challenges facing a JTCB seem daunting, but the board can address them in a way that satisfies the combatant commander's requirements. While the details of rules of engagement and target legitimacy reside in the realm of law, it is, especially with new technologies, a subjective field. The use of two distinct legal processes—in the target development and prioritization process described in Joint Publication 3-60 and the acquisitions process described in DODD 5000.01—to approve the development and employment of a cyber weapon is redundant and overuses scarce legal resources.

Instead, USCYBERCOM should conduct both legal reviews. The legal review during target development and prioritization should be skipped for cyberspace targets. USCYBERCOM should conduct an initial and final LOAC review while coordinating with the JTCB during the cyber weapon development. Moreover, since cyber weapons are custom crafted to engage a specific target, the legal team can conduct the legal reviews mandated by DODD 5000.01 as

well as target validation. USCYBERCOM, in coordination with the cyberspace representative, should have the technical expertise to review and assist in the weapon development. This will enhance the effectiveness of OCO development and employment. Furthermore, since the legal review team is not part of the combatant command, there is less opportunity for “group think” or command influence to warp the process.

Conclusion

OCO offer potent tools for a combatant command or JTF commander. However, our own internal friction—manifested as misunderstanding, inaccessibility, and slowly evolving processes—has not allowed us to take full advantage of these capabilities. None of the solutions described above are particularly costly, nor do they involve purchasing equipment or adding to the force structure. Rather, they focus on developing our people and processes so they are more prepared to engage an adversary in all domains. While implementing these solutions would be a long-term effort, delaying implementation only would enable the problem to fester, effectively denying use of OCO to joint force commanders. **MR**

NOTES

1. Saul David, *The Illustrated Encyclopedia of Warfare: From Ancient Egypt to Iraq* (London: DK Publishing, 2012), 95.

2. Sascha-Dominik Bachmann, “Hybrid Threats, Cyber Warfare and NATO's Comprehensive Approach for Countering 21st Century Threats—Mapping the New Frontier of Global Risk and Security Management,” *Amicus Curiae* 88 (January 2012).

3. Mark Landler and John Markoff, “After Computer Siege in Estonia, War Fears Turn to Cyberspace,” *New York Times* (29 May 2007).

4. *Ibid.*

5. Joshua Davis, “Hackers Take Down the Most Wired Country in Europe,” *Wired.com* (21 August 2007), <http://www.wired.com/politics/security/magazine/15-09/ff_estonia?currentPage=all>.

6. James P. Farwell and Rafal Rohozinski, “Stuxnet and the Future of Cyber War,” *Survival: Global Politics and Strategy* 53, no. 1 (January 2011): 23-40.

7. Stephen W. Korn and Joshua E. Kastenbury, “Georgia's Cyber Left Hook,” *Parameters* 38, no. 4 (Winter 2008-2009).

8. Eli Jellenc, quoted in Iain Thomson, “Georgia Gets Allies in Russian Cyberwar,” *Vnunet.com* (12 August 2008), <<http://www.v3.co.uk/v3-uk/news/1997915/georgia-allies-russian-cyberwar>>; see also John Markoff, “Before the Gunfire, Cyberattacks,” *New York Times* (12 August 2008), <http://www.nytimes.com/2008/08/13/technology/13cyber.html?_r=0>.

9. Mark Clayton, “How Stuxnet Cyber Weapon Targeted Iran Nuclear Plant,” *The Christian Science Monitor* (16 November 2010): 4.

10. Farwell and Rohozinski, 23-40.

11. Ralph Langner, as reported in Clayton, 4.

12. Stephenie Gosnell Handler, “The New Cyber Face of Battle: Developing a Legal Approach to Accommodate Emerging Trends in Warfare,” *Stanford Journal of International Law* 48, no. 1 (Winter 2012): 209.

13. Anoop Singal and Ximmgou Ou, *Security Risk Analysis of Enterprise Net-*

works Using Probabilistic Attack Graphs (Gaithersburg, MD: NIST Interagency Report 7788, National Institute for Standards and Technology, U.S. Department of Commerce, August 2011).

14. Joint Publication 3-60, *Joint Targeting* (Washington, DC: U.S. Government Printing Office [GPO], 31 January 2013), Figure II-2.

15. Eric Schmitt and Thom Shanker, “U.S. Debated Cyberwarfare in Attack Plan on Libya,” *New York Times* (17 October 2011), <http://www.nytimes.com/2011/10/18/world/africa/cyber-warfare-against-libya-was-debated-by-us.html?_r=0>.

16. Nicolas Falliere, Liam Murchu, and Eric Chien, W32.Stuxnet Dossier (Cupertino: Symantec Corporation, 2011), <http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf>.

17. *Ibid.*

18. Rene G. Rendon and Keith F. Snider, Management of Defense Acquisition Projects (Reston, VA: American Institute of Aeronautics and Astronautics, 2008), 66.

19. Falliere, Murchu, and Chien, 3.

20. Stewart A. Baker and Charles Dunlap Jr., “What Is the Role of Lawyers in Cyberwarfare?” *ABA Journal* (1 May 2012), <http://www.abajournal.com/magazine/article/what_is_the_role_of_lawyers_in_cyberwarfare>.

21. *Ibid.*

22. Department of Defense Directive 5000.01, The Defense Acquisition System (Washington, DC: GPO, 12 May 2003), 7.

23. U.S. Air Force, Air Force Instruction 51-402: Legal Reviews of Weapons and Cyber Capabilities (Washington, DC: GPO, 27 July 2011), 2.

24. Baker and Dunlap Jr.

25. Debra Van Opstal, “Aha! Findings from the Workshop on Securing the Smart Grid: Best Practices in Supply Chain Security, Integrity, and Resilience,” Center for Critical Infrastructure Protection and Homeland Security 11, no. 2 (August 2012).

26. *Ibid.*



Responsibility Practices in Robotic Warfare

Deborah G. Johnson, Ph.D., and Merel E. Noorman, Ph.D.

UNMANNED AERIAL VEHICLES (UAVs), also known as drones, are commonplace in U.S. military operations. Many predict increased military use of more sophisticated and more autonomous robots.¹ Increased use of robots has the potential to transform how those directly involved in warfare, as well as the public, perceive and experience war. Military robots allow operators and commanders to be miles away from the battle, engaging in conflicts virtually through computer screens and controls. Video cameras and sensors operated by robots provide technologically mediated renderings of what is happening on the ground, affecting the actions and attitudes of all involved.

Central to the ethical concerns raised by robotic warfare, especially the use of autonomous military robots, are issues of responsibility and accountability. Who will be responsible when robots decide for themselves and behave in unpredictable ways or in ways that their human partners do not understand? For example, who will be responsible if an autonomously operating unmanned aircraft crosses a border without authorization or erroneously identifies a friendly aircraft as a target and shoots it down?² Will a day come when robots themselves are considered responsible for their actions?³

Deborah G. Johnson is the Anne Shirley Carter Olsson Professor of Applied Ethics in the Science, Technology, and Society Program at the University of Virginia. She holds a Ph.D., M.A., and M.Phil. from the University of Kansas and a B.Ph. from Wayne State University. The author/editor of seven books, she writes and teaches about the ethical issues in science and engineering, especially those involving computers and information technology.

Merel E. Noorman is a postdoctoral researcher at the eHumanities group of the Royal Netherlands Academy for Arts and Sciences. Before joining the eHumanities group, she was a postdoctoral research associate in the Science, Technology, and Society Program at the University of Virginia, where she worked with Deborah Johnson on the research this paper is based on. She received her Ph.D. from Maastricht University and studied artificial intelligence and science and technology studies at the University of Amsterdam and Edinburgh University.

In principle, humans retain control of—and responsibility for—the behavior of autonomous machines. However, establishing precisely who is responsible for a machine's behavior is challenging. Autonomous machines, no matter how they are defined, developed, or used, operate as part of broad sociotechnical systems involving numerous individuals and organizations.

We advocate the concurrent development of new responsibility practices *with* the development of new technologies rather than before or after those technologies are developed and adopted for use. This is necessary because literature in the field of science and technology studies shows that the trajectory of a technology's development is unpredictable; how a technology takes shape depends on complex negotiations among relevant social groups.⁴ The technologies eventually adopted and used are not predetermined by nature or any other factor. No one can predict with certainty how a developing technology will turn out or what new technologies will emerge. In the course of development, a new technology may change in response to many factors, including changes in funding, historical events such as wars, changes in the regulatory environment, and market indicators. The technologies that succeed (i.e., that are adopted and used) are the outcome of complex negotiations among many actors, including engineers and scientists, users, manufacturers, the public, policymakers, politicians, and others.

Negotiations among the actors involved with a new technology are part of the overall discourse around that technology from its earliest stages of development. The discourse about responsibility and autonomous military robots is a case in point; current discourse provides an opportunity to observe issues of responsibility being worked out early in the technology's development. The negotiations between researchers, developers, engineers, philosophers, policymakers, military authorities, lawyers, journalists, and human rights activists are taking place in the media and academic journals, at conferences and trade shows, through drafting new policies and regulations, in negotiating international treaties, and also through designing and developing the technologies. This process contrasts starkly with the all-too-common idea that issues of responsibility are decided after

a technology is developed or separately from technological design.

Framing robots as autonomous challenges ordinary notions of responsibility. Autonomy in daily life and moral philosophy implies acting on one's own, controlling one's self, and being responsible for one's actions. On the other hand, being responsible generally means that individuals have some kind of influence or control over their actions and the outcomes of those actions. The idea of the autonomy of robots suggests that humans are not in control of the robots. Hence, at first glance, it may seem that humans should not be held responsible for autonomous robot behavior. However, this narrative of future autonomous robots operating on their own, without human control, is somewhat misleading, and it draws attention away from important choices about responsibility—choices made at the level of design and implementation.

Our analysis of the discourse on autonomous artificial agents and responsibility shows that delegating tasks to autonomous technologies *is* compatible with holding humans responsible for the behavior of those technologies. This is so for at least two reasons. First, the definition of machine autonomy has numerous interpretations, but all involve various kinds and degrees of human control. Second, humans decide who is responsible for the actions of a machine. Their decisions are affected by, but not entirely determined by, the nature of technology. Responsibility for the behavior of autonomous machines is and must continue to be determined by ongoing negotiations between relevant interest groups during the development of new technologies.

Negotiating Autonomy

Popular accounts of future military robots often portray these technologies as entities with capabilities that rival or surpass those of humans. We are told that robots of the future will have the ability to think, perceive, and even make moral decisions. In *Discover Magazine*, for instance, Mark Anderson writes, "As surely as every modern jetliner runs primarily on autopilot, tomorrow's military robots will increasingly operate on their own initiative. Before the decade is out, some fighting force may well succeed in fielding a military robot that can kill without a joystick operator behind a curtain

elsewhere in the world.”⁵ Such narratives raise concerns about the lack of human control, and as a result, they confound the determination of human responsibility.

However, in robotics and computer science, autonomy has many different meanings. It tends to be used metaphorically to emphasize certain features of a computational system that set it apart from other systems. Three conceptions of machine autonomy—as high-end automation, as something other than automation, or as collaborative autonomy—illustrate that humans do not necessarily lose control when tasks are delegated to autonomous systems. Rather, the delegation of tasks to these systems transforms the character of human control.

Autonomy as high-end automation. In its report, “The Role of Autonomy in Department of Defense Systems,” the Defense Science Board Task Force characterizes autonomy as “a capability (or a

set of capabilities) that enables a particular action of a system to be automatic or, within programmed boundaries, ‘self-governing.’”⁶ Capability, here, refers to a particular process (or processes) consisting of one or more tasks, such as navigation or flight control. This definition echoes a more traditional way of conceptualizing machine autonomy as at the high end of a continuous scale of increasing automation. In this way of thinking, automation involves the mechanization of tasks, where routine actions are translated into some formalized and discrete steps such that a machine can perform them.⁷ At the high end of the automation scale are systems in which the automated machine performs most or all of the steps in a process. At the low end of the scale are systems in which decision making and control of the process are left largely to human operators. Autonomy is attributed to those systems with higher levels of automation. Such systems close the control loop over a process, i.e., most of the tasks in the process are automated while human operators make few, if any, decisions.

Machine autonomy, in this way of thinking is bounded; it extends only as far as the automated process. Therefore, in this kind of machine autonomy, humans are in control of what the machine does, even if they do not directly intervene or are not ‘in the loop,’ because they fully specify the process and the routine tasks the machine performs.

Autonomy as something other than automation. However, some participants in the discourse sharply distinguish machine autonomy from automation. They argue, for example, that autonomous systems (of the future) will be different from automated systems because their behavior will not be preprogrammed. Autonomous systems will only have to be instructed what to do, not how to do it.⁸ Human operators and designers will not have to specify in advance all the behavior sequences that should follow a particular input.

In its *Unmanned Systems Integrated Roadmap FY2011–2036*, the Department of Defense (DOD) provides an illustration of this second take on machine autonomy. It argues that autonomous systems are “self-directed toward a goal in that they do not require outside control, but rather are governed by laws and strategies that direct their behavior.”⁹ Their behavior in response to certain events is not fully specified or preprogrammed. According to this



Lt. Gen. Jeffrey Talley (then Brig. Gen.), commander of 926th Engineer Brigade, Multi-National Division, watches a demonstration of robotic route-clearing equipment at 6th Iraqi Army Division headquarters motor pool, Iraq, 5 January 2009.



U.S. Army Sgt. Benjamin D. Parker, an explosive ordnance disposal team leader, and Spc. Chase Donnelly, a robotics operator, prepare their robot to inspect a suspected improvised explosive device in eastern Afghanistan's Nangarhar Province. (U.S. Army, Sgt. Tracy J. Smith)

2011 update of the *Roadmap*, “an autonomous system is able to make a decision based on a set of rules and/or limitations. It is able to determine what information is important in making a decision.”¹⁰ By contrast, the DOD argues, automatic systems are fully preprogrammed. They can “act repeatedly and independently of external influence or control,” but they “follow a predefined path,” and their behavior has to be fully specified in advance.¹¹

Machine autonomy, from this perspective, refers to robotic systems that would somehow be more flexible and unpredictable, compared to automated systems, in deciding how to operate—given predefined goals, rules, or norms. Those that make this distinction about autonomy tend to point to artificial intelligence technologies—such as machine learning or probabilistic reasoning methods—as technologies that would enable these kinds of robotic systems.¹² Robots equipped with these kinds of technologies would be able to learn from experience and adapt to changing

circumstances as well as deal with uncertain or missing data. Such descriptions of autonomy seem to suggest that human operators as well as developers would have less control over the behavior of the system. The machine would not only operate independently of the human operator, but also, to a certain extent, independently of its human creators.

Nevertheless, even here, autonomy does not mean that machines are free in the decisions they make; the conditions for making a decision are carefully set by humans. As the DOD’s 2011 conception of autonomy shows, laws and strategies provided by humans will still govern the behavior of autonomous systems. The envisioned systems could vary their behavior as long as they stayed within these predefined constraints. Note that this would be a remarkable feat, as it would mean these robots could interpret laws and strategies, applying them appropriately in ever-changing sociotechnical contexts.

Regardless of whether this is possible, devel-

opers and designers would delimit the problem any robotic system is intended to solve. If the envisioned robotic technologies were based on artificial intelligence methods now in development, then those artificial intelligence methods would limit any robotic system's abilities to act independently. Although programmers and developers would not have to specify all the possible situations with which the software has to contend, designers would have to generate a model that approximates the behavior of particular aspects

Humans exert their influence by defining the conditions for machine behavior.

of the world and their uncertainties. Learning and probabilistic algorithms would be able to operate more flexibly than a preprogrammed deterministic algorithm because they would allow for variations and could respond to certain unanticipated contingencies. Nevertheless, this flexibility is a function of the problem definitions and the world models that the developers or programmers of the algorithm have formulated. Therefore, even where machine autonomy is considered more than high-level automation, the autonomy of the machine does not mean there is no human control because humans design, choose, and plan for the strategies employed by the machine.

Collaborative autonomy. Both conceptions of machine autonomy described above (autonomy as high-level automation and autonomy as something other than automation) focus on what machines can do *without* direct human control. However, machine autonomy does not necessarily mean that humans will be taken out of the loop. Human operators may still be involved in the decision-making processes that autonomous robots execute. As explained in an earlier edition (published in 2009) of the *Roadmap (Unmanned Systems Integrated Roadmap FY 2009–2034)*: “First and foremost, the level of autonomy should continue to progress from today’s fairly high level of human control/intervention to a high level of autonomous tactical behavior that enables more

timely and informed human oversight.”¹³ The text implies an expectation that robots will operate in support of and in close communication with human actors, such that human oversight remains possible.

The ability of robots to engage in joint activities with humans has received more attention in human–computer interaction research, where researchers use terms such as collaborative control, situated autonomy, or adaptive autonomy.¹⁴ Robin R. Murphy and David D. Woods, for example, have argued for what they call “situated autonomy,” a notion that stresses the responsiveness of robots to humans.¹⁵ They contend that robots should have the capability to respond to humans, as appropriate to the humans’ roles. That is, a robot’s behavior should be attuned to the relationships and social roles of the humans with which it interacts. Thus, a robot may request a confirmation from a superior when it receives a command from a human operator that exceeds the operator’s level of authority, or it may decide to transfer control back to an operator when appropriate for the situation. The requirement of responsiveness, Murphy and Woods argue, captures a new form of autonomy, “not as isolated action but the more difficult behavior of engaging appropriately with others.”¹⁶ This type of autonomy places the emphasis on the interaction between humans and robots. It implies that robots should be designed so that control can be transferred smoothly from the human operator to the robot and back.

The Defense Science Board Task Force, cochaired by Murphy, uses a similar collaborative conception of autonomy. In their document *Task Force Report: The Role of Autonomy in DOD Systems*, the Task Force argues that many of the DOD studies of autonomy focus too much on machines and not enough on the human–machine system. They argue instead for the adoption of an “autonomous systems reference framework” that focuses on the explicit allocation of functions and responsibilities between human and computer, recognizing that these allocations may vary depending on the context. The framework should also make choices explicit about trade-offs inherent in technological design, such as optimization versus resilience or centralized information systems versus distributed systems. Human decisions about the allocation of control are thus an explicit part of the design process—a process that places overall control firmly in the hands of humans.

Human Influence over Military Robots

None of the three approaches to the autonomy of robots described above implies that humans are not in control of the technology they create and deploy. The Defense Science Board Task Force even argues that “it should be made clear that all autonomous systems are supervised by human operators at some level, and autonomous systems’ software embodies the designed limits on the actions and decisions delegated to the computer.”¹⁷ Instead of no human control, robot (or machine) autonomy appears to mean that humans have different kinds of control. Humans exert their influence by defining the conditions for machine behavior. They choose the mathematical and probabilistic models that will guide the behavior of the robotic system and determine the margins of error on what the robot can and cannot do. Designers, developers, managers, and operators set constraints on the behavior that robotic systems are allowed to exhibit.

As military robots become more autonomous, it would seem that they should only be allowed to operate autonomously if they exhibit predictable and reliable behavior. For example, an unmanned

helicopter would be allowed to fly into an unknown environment only if the software controlling the helicopter would adhere to certain expectations and norms. The helicopter should not fly into trees, it should execute given instructions, and it should fly between waypoints in a limited amount of time. If the helicopter would not perform as expected, it would be regarded as malfunctioning.

It should not be surprising, then, that the idea of more autonomous robotic systems comes with an increased emphasis on reliability of and trust in technology, along with the need to develop better methods for verification and validation. In the *Report on Technology Horizons: A Vision for Air Force Science & Technology 2010–2030*, the U.S. Air Force chief scientist argues that although it is possible to develop systems with relatively high levels of autonomy, the lack of suitable verification and validation methods stands in the way of certifying these technologies for use.¹⁸ The report claims that in the near- to mid-term future, developing methods for “certifiable trust in autonomous systems is the single greatest technical barrier that must be overcome to obtain the capability advantages that are achievable by increasing use of autonomous



U.S. Army soldiers operate a pack robot at Forward Operating Base Hawk, Iraq, 18 September 2008. (U.S. Air Force, Staff Sgt. Manuel J. Martinez)

systems.”¹⁹ These observations reflect the need for reliability and predictability that one would expect from an organization in which command responsibility is a guiding principle. At the same time, they show that control of autonomous systems is partly in the hands of those who develop verification and validation methods or other methods of ensuring trust and confidence in these systems.

The three different conceptions of autonomy illustrate that autonomy does not mean that robots are or will be out of the control of humans. The different approaches to machine autonomy may, nevertheless, have effects on how issues of responsibility are understood and managed since they shape the activities and attitudes of humans and relations between them.²⁰ Robots that can operate with more flexibility in unknown environments, for instance, may affect the way humans perceive and experience what it means to be in control of outcomes and thus what it means to be responsible. Further automation of decision making brings in developers, testers, and others, which may influence how responsibility is distributed.

Nevertheless, although technologies shape how participants in the system perceive, experience, and behave with autonomous systems, they do not determine these things. Nor do they determine responsibility. Responsibility for the behavior of an autonomous system is a matter that humans involved in the development and use of autonomous military robots negotiate and will likely continue to negotiate.

Responsibility Practices for Military Robots

As our discussion of different concepts of autonomy hints at, functioning military robots are not simply machines; they are not even simply intelligent and autonomous machines. They are sociotechnical systems. That is, the robot machine is a component in a system consisting of human actors and artifacts. The behaviors of both combine to produce a system that achieves (or attempts to achieve) human goals. When a robot is used in a military operation—say, an unmanned aircraft is sent to eliminate a target—the operation consists of human and nonhuman behavior. Humans decide if there is sufficient evidence of an appropriate target; a few of them decide whether and when to deploy a UAV; others sign off on the decision;

yet others monitor and communicate with the UAV; and so on. And, of course, many humans have been involved in the design and manufacturing of the UAV and its delivery to a particular location.

Although sociotechnical systems function by delegating specific tasks to each component of the system, delegation of tasks is not the same as delegation of responsibility. Artifacts—such as machines, software, and mechanical parts—might be considered responsible for the performance of particular tasks, but this use of “responsible” is limited to performance and possibly the effects of tasks. Because other senses of responsibility—such as moral, legal, and professional—require conscious deliberation and voluntary actions, they apply, conventionally at least, only to human beings or groups of human beings. In philosophical and moral traditions, ascribing responsibility for a particular outcome to a person requires that the person acted freely and was able to consider the consequences. Machines typically lack such capabilities.

Ascribing responsibility can nevertheless be a challenge. Conventional moral notions can be difficult to apply in practice because individuals rarely have full control over outcomes, and they seldom know exactly what the consequences of their actions will be.²¹ In sociotechnical systems, it can be difficult to figure out what happened and who was responsible for which actions or consequences following an untoward event.²² Numerous individuals and institutions act with and in sociotechnical systems, and human and technological components affect each other in contingent ways. However, although ascribing responsibility can be challenging, this is not to say that no one is responsible.

Human responsibility can best be understood as constituted through a set of *responsibility practices*. Responsibility practices are the established ways that people within a particular environment or community understand, assign, and ascribe responsibility based on shared values and ideas about fairness and utility. These practices involve accepted ways of evaluating actions, holding others to account, blaming or praising, and conveying expectations about obligations and duties. They are also about prevailing norms and moral principles that guide the behavior of the members of a community.

Responsibility practices are both forward- and backward-looking. Forward-looking responsibility involves specifying which tasks and duties are

assigned to which individuals and to which nonhuman components. Such practices might be promulgated through job descriptions, instruction manuals, ethical codes, observation of past practices, training before taking on a role, and so on. Backward-looking responsibility involves practices of tracing back what happened and identifying what went wrong. When a failure occurs, humans will seek out the cause of the failure, and humans operating in the system will be asked to account for their behavior. Backward-looking responsibility generally relies on, or at least presumes something about, forward-looking responsibility. That is, to understand what went wrong or what is to blame, we have to understand how tasks and responsibilities were assigned.

The extent to which individuals operating in the system are perceived to have responsibility or feel themselves in a position of responsibility is not simply a matter of tasks being delegated. It also depends on how responsibility practices convey expectations about the duties and obligations of the humans and hold actors accountable for performing or failing to perform as expected. Whether someone is considered responsible depends, as well, on evolving notions of what it means to be in control and able to think about the consequences of certain actions.

In a given system, adoption of a new technology may lead to negotiations about changes to existing responsibility practices, creation of entirely new practices, or both. Established practices may not accommodate the changes produced from introducing the new technology, e.g., changes in activities, attitudes, and relationships between people. The real-time stream of data that current UAVs produce is a good example here. The role of pilots has changed insofar as they now monitor video images and continuously communicate with others who have access to the same data and images (e.g., the sensor operator, the mission intelligence coordinator, and the data analysts miles away in an information fusion center). This has transformed the way targeting decisions are made, compared to manned operations. Decision making has become more shared and less compartmentalized. As a result, established ideas about what various human actors are supposed to do and what they have to account for have had to be adjusted.²³

New norms and rules have to be established to govern the activities a new technology makes possible. Duties and obligations have to be reevaluated

and redefined. Mechanisms for evaluating actions and holding others to account have to be adjusted or created. This will also be the case for future autonomous technologies. Regardless of how machine autonomy is interpreted, whether someone is responsible for the behavior of the system will not only depend on what

Human responsibility can best be understood as constituted through a set of responsibility practices.

the machine can and cannot do, it will also depend on the practices that prevail in the context.

Shared values and principles may shape the establishment of new practices. In the case of UAVs, organizational values and national and international laws provide a moral framework for and set limits on the new activities these technologies enable. Take the principle of distinction, a key principle in international law that states civilians should be distinguished from combatants. This principle is intertwined with established responsibility practices within military organizations, as they are part of their routines, protocols, and procedures.

Yet, these shared values and principles are subject to negotiation. Achieving an interpretation of them may be challenging because of the introduction of new technologies and also because of social, political, and economic developments. The current debates about the use of drones provide a pertinent example. One contentious issue is that, according to anonymous government officials, the U.S. government regards all military-age males killed in a drone strike as combatants unless proven otherwise.²⁴ Such a controversial and broad interpretation of a key principle of the law of war affects responsibility practices significantly, at least in the sense that soldiers involved in deploying drones are held to a certain standard of responsibility for harm to noncombatants.

Responsibility practices are continuously negotiated and renegotiated. This can often be seen when something goes wrong with a new technology, and investigators trace back the cause of the failure.



U.S. airmen with the 62nd Expeditionary Reconnaissance Squadron speak to Afghan men and children about an MQ-9 Reaper unmanned aerial vehicle during the 2012 Kandahar Air Wing open house in Kandahar, Afghanistan, 1 January 2012. (U.S. Air Force, Staff Sgt. David Carbajal)

They may discover that something should have been done—and in the future should be done—differently. For instance, the precise role of UAV operators was not immediately clear when UAVs were first introduced. Various investigative reports following UAV mishaps and accidents have made recommendations to adjust and enhance training programs, procedures, communication protocols, and task assignments. The recommendations are targeted to delineate clearly who is responsible for what and to enhance the conditions under which individuals make decisions.²⁵ Such reports reveal evolving notions of the kind of skills and knowledge that operators need as well as changing norms that govern their behavior.

Negotiations about responsibility practices also may involve adjustments to the technology. In its report on autonomy in DOD systems, the Defense Science Board, for example, stressed the need for a more careful consideration of human factors.²⁶ Neglect of human–robot interaction in the early UAV development programs resulted in a relatively high

number of mishaps. Operators made mistakes due to confusing interfaces and information overload. The Defense Science Board's report calls for changes to the existing interfaces.

Therefore, responsibility is best conceived of as a set of practices built on the foundation of a distribution of tasks. Responsibility practices are reinforced by activities that promulgate expectations about what individuals are supposed to do and what happens when failures occur. Among other things, organizations create expectations through policies and through their organizational culture. Responsibility practices develop expectations of how human and nonhuman components will behave (i.e., who is responsible for doing what) and specify what should or will happen when there is a failure to live up to expectations. These expectations and ideas about responsibility influence the design and eventual use of technologies. Increasingly autonomous technologies may necessitate changes to existing responsibility practices and creation of some entirely new practices in the future.

Conclusion

The use of autonomous artificial agents raises significant issues of responsibility and accountability, and this is especially so when the artificial agents are part of military operations. Whether and in what ways humans are responsible for the behavior of artificial agents is not just a matter of delegating tasks to machines. Negotiations about responsibility for the behavior of these agents are ongoing with the development of the technologies. These negotiations involve a variety of actors, including the scientists and engineers designing the technologies and users such as the military or the public. Although it is difficult to predict where current negotiations will end up (and that is not our goal), our analysis shows that different notions of autonomy are being used, and each has distinctive implications for how we think about responsibility. At the same time, issues of responsibility are not determined by the design of the artificial

agent. Decisions about responsibility, i.e., who is responsible for what behavior, are also made in the development and evolution of social practices that constitute the operation of artificial agents.

None of this is to say we should stop being concerned about the tasks assigned to the nonhuman components of military robotic systems. On the contrary, concerns about responsibility should be an important part of the negotiations. They should shape the delegation of tasks to the human and nonhuman components of these systems. The danger in concentrating on the technological side of autonomous robots is that the development of responsibility practices will be neglected. Instead of focusing on whether robots or humans can be held responsible for robots' behavior, we should focus on the best allocation of tasks and control among human and nonhuman components *and* how best to develop responsibility practices. **MR**

This paper is based on the research done for the National Science Foundation (Grant # 1058457) and draws on several papers that have been written as part of this project. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the National Science Foundation.

NOTES

1. Unmanned aerial vehicles (UAVs) are sometimes referred to as remotely piloted aircraft to emphasize the need for a pilot or unmanned systems to underline that the vehicle is inextricably linked to a larger system of human actors and technologies. For clarity, we use the terms drone and UAV. For different perspectives on the future of drones, see T. Adams, "Future Warfare and the Decline of Human Decision-Making," *Parameters* (Winter 2001-02): 55-71; Patrick Lin, George Bekey, and Keith Abney, *Autonomous Military Robots: Risk, Ethics, and Design* (California Polytechnic State University, 2008), <http://ethics.calpoly.edu/ONR_report.pdf>; Peter W. Singer, *Wired for War: The Robotics Revolution and Conflict in the 21st Century* (New York, New York: Penguin, 2009); U.S. Air Force Chief Scientist, *Report on Technology Horizons: A Vision for Air Force Science & Technology 2010-2030* (AF/ST-TR-10-01-PR, Maxwell Air Force Base, Alabama, September 2011), <http://www.defenseinnovationmarketplace.mil/resources/AF_TechnologyHorizons2010-2030.pdf>.

2. Peter M. Asaro, "How Just Could a Robot War Be," *Current Issues in Computing And Philosophy*, edited by Philip Brey, Adam Briggie and Katinka Waelbers, (Amsterdam, The Netherlands: IOS Press, 2008), 50-64.

3. Lin, Bekey, and Abney.

4. For an overview of science and technology studies, see Wiebe E. Bijker, Thomas P. Hughes, and Trevor Pinch, *The Social Construction of Technological Systems: New Directions in the Sociology and History of Technology* (London, UK: The MIT Press, 1987).

5. Mark Anderson, "How Does a Terminator Know When to Not Terminate?" *Discover Magazine*, 31(4)(May 2010): 36.

6. DOD, Defense Science Board, *Task Force Report: The Role of Autonomy in DOD Systems* (Washington, DC: U.S. Government Printing Office [GPO], July 2012), <<http://www.acq.osd.mil/dsb/reports/AutonomyReport.pdf>>, 1.

7. See Thomas B. Sheridan, *Telerobotics, Automation, and Human Supervisory Control* (Cambridge, MA: MIT Press, 1992).

8. See for example Bruce T. Clough, Metrics, Schmetrics: *How the Heck Do You Determine a UAV's Autonomy Anyway?* (Technical report, Air Force Research Lab., Wright-Patterson AFB, Ohio, 2002).

9. DOD, *Unmanned Systems Integrated Roadmap FY2011-2036*, (Washington, DC: GPO, 2011), <<http://www.acq.osd.mil/sts/docs/Unmanned%20Systems%20Integrated%20Roadmap%20FY2011-2036.pdf>>, 43.

10. *Ibid.*, 43.

11. *Ibid.*, 43.

12. U.S. Air Force Chief Scientist, *Report on Technology Horizons*.

13. DOD, *Unmanned Systems Integrated Roadmap FY2009-2034* (Washing-

ton, DC: GPO, 20 April 2009), <www.dtic.mil/dtic/tr/fulltext/u2/a522247.pdf>, 27.

14. See for a brief overview Matthew Johnson, et al., "The Fundamental Principle of Coactive Design Interdependence Must Shape Autonomy," in COIN@ AAMAS'10, *Proceedings of the 6th International Conference on Coordination, Organizations, Institutions, and Norms in Agent Systems*, (2010), 172-191.

15. Robin R. Murphy and David D. Woods, "Beyond Asimov: The Three Laws of Responsible Robotics," *IEEE Intelligent Systems*, 24(4) (July-August, 2009):14-20.

16. *Ibid.*, 18.

17. DOD, Defense Science Board, *Task Force Report*, 1.

18. U.S. Air Force Chief Scientist, *Report on Technology Horizons*, IX.

19. *Ibid.*, 42.

20. Peter-Paul Verbeek, "Materializing Morality," *Science, Technology and Human Values*, 31(3) (2006): 361-380.

21. Hans Jonas, *The Imperative of Responsibility: In Search of an Ethics for the Technological Age* (Chicago: The Chicago University Press, 1984); Mark Coeckelbergh, "Moral Responsibility, Technology, and Experiences of the Tragic: From Kierkegaard to Offshore Engineering," *Science and Engineering Ethics*, 18 (2012): 35-48.

22. Deborah G. Johnson and Thomas M. Powers, "Computer Systems and Responsibility: a Normative Look at Technological Complexity," *Ethics and Information Technology*, 7(2) (2005): 99-107.

23. Peter M. Asaro, "The Labor of Surveillance and Bureaucratized Killing: New Subjectivities of Military Drone Operators," *Journal of Social Semiotics*, 23(2) (2013): 196-224.

24. Jo Becker and Scott Shane, "Secret 'Kill List' Proves a Test of Obama's Principles and Will," *New York Times*, (May 29, 2012), <<http://www.nytimes.com/2012/05/29/world/obamas-leadership-in-war-on-al-qaeda.html?pagewanted=all>>.

25. See for example David S. Cloud, "Anatomy of an Afghan War Tragedy," *Los Angeles Times* (April 10, 2011) <<http://articles.latimes.com/2011/apr/10/world/la-fg-afghanistan-drone-20110410>>; Sharon D. Manning, Clarence E. Rash, Patricia A. LeDuc, Robert K. Noback and Joseph McKeon, *The Role of Human Causal Factors in U.S. Army Unmanned Aerial Vehicle Accidents* (U.S. Army Aeromedical Research Laboratory Report # 2004-11, 2004); Kevin W. Williams, *A Summary of Unmanned Aircraft Accident/Incident Data: Human Factors Implications* (Washington, DC: U.S. Department of Transportation, Federal Aviation Administration, Office of Aerospace Medicine. Technical Report Publication No. DOT/FAA/AM-04/24, 2004).

26. DOD, Defense Science Board, *Task Force Report*.



Failed Cyberdefense

The Environmental Consequences of Hostile Acts

Jan Kallberg, Ph.D., and Rosemary A. Burk, Ph.D.

(FEMA, David Valdez)

A FAILED CYBERDEFENSE CAN have wider effects than discussed in earlier debates of potential consequences of a cyberattack. The need for cyberdefense to protect the environment has not drawn the attention it deserves as a national security matter. Adversarial nations are covertly pursuing methods to damage and disrupt the United States in a cyberconflict in the future. The president of the United States noted this in *Sustaining U.S. Global Leadership: Priorities for 21st Century Defense*:

Both state and non-state actors possess the capability and intent to conduct cyberespionage and, potentially, cyberattacks on the United States, with possible severe effects on both our military operations and our homeland.¹

Jan Kallberg is an assistant professor at Arkansas Tech University and a research associate at the Cyber Security Research and Education Institute, the University of Texas at Dallas. He holds a Ph.D. from the University of Texas at Dallas. His works have been published in Joint Force Quarterly, Strategic Studies Quarterly, Air and Space Power Journal, IEEE Access, and IEEE Security and Privacy.

Rosemary Burk is an assistant professor in biology at Arkansas Tech University. She holds a Ph.D. from the Department of Biological Sciences at the University of North Texas. Her research has been published by International Journal of Water Resource Development and Journal of Freshwater Ecology.

The former U.S. Secretary of Defense Leon Panetta delivered a clear assessment of the risk for these attacks in a speech on 12 October 2012:

These attacks mark a significant escalation of the cyberthreat, and they have renewed concerns about still more destructive scenarios that could unfold. For example, we know that foreign cyberactors are probing America's critical infrastructure networks. They are targeting the computer control systems that operate chemical, electricity and water plants and those that guide transportation throughout this country.

We know of specific instances where intruders have successfully gained access to these control systems. We also know that they are seeking to create advanced tools to attack these systems and cause panic and destruction and even the loss of life.²

Even if the nation's leadership has identified the risk, expressed concern, and started to allocate resources to improve national cyberdefense, others consider the likelihood of a cyberwar as marginal. One of the leading arguments against the possibility of future cyberwar has been the premise that such an attack would cause no long-term damage.³ This argument is based on a marginalization of cyberattacks as intermittent disruptions of client computers by crude and unsophisticated malign software that creates temporary havoc.⁴ The perception is that damage is limited to the attacked computer networks—not the external environment that relies on these networks. However, the concerns aired by Panetta, originating from the assessment made by the president, convey a wider, more holistic perception of potential damage beyond computer networks.

In this article we present a tangible argument that cyberwar can inflict continuing damage on a targeted society beyond the actual destruction of a defending computer network. The long-term environmental consequences of a lost cyberwar and failed national cyberdefense are not well recognized. The last decade's intense study of cybersecurity, with its focus on networks and network security, has left the risk to physical environments that rely upon cybercontrolled networks unaddressed.⁵

The Concept of Cyberwar

In cyberwar conflicts, state actors are seeking to force a policy change in the other party. Therefore, cyberwar should be regarded first from a strategic viewpoint and second from lower levels of abstraction. A central part in all conflict is the fear of consequences—the actual repercussions of opposition to a will that seeks to subdue. Nuclear weapons are feared because of their validated and graphically devastating effects. Cyberweapons will need to show they are catastrophic; otherwise, the threat or deterrence of those weapons evaporates.

In earlier studies of cyberwar, the focus was on disruptions in technical or military capacity and the resilience to operate in a degraded environment. The potential to destroy opposing systems through digital lethality has recently been introduced.⁶ In these scenarios, the factual long-term damage is limited. For an adversary seeking to affect U.S. policy, current vulnerabilities in our industrial control systems are an inviting opportunity. Their targeting could have significant societal impacts—fear, uncertainty, and public pressure on political leadership if environmental damage occurs.

Attacking industrial control systems to damage the environment is a grave act of war. However, as long as attribution is unknown and there is no punitive mechanism in place, the prohibitions against such acts in international law are at the attacker's discretion to recognize. Today, there are limited options, if any, to enforce accountability for cyberattacks through international law.

Environmental Effects of Cyberwar

If an adversary could cause major irreversible environmental damage to the United States through cyberattacks on industrial control systems, or merely establish control over numerous systems, it could limit U.S. policy options. The threat and risk of a cyberattack would have to be considered, and it would give a minor power a force-multiplying effect in a direct conflict with the United States.

The barrage of cyberattacks on the nation's infrastructure in the last decade is a major concern for the federal government.⁷ These attacks have been extended to include supervisory control and data acquisition (SCADA) systems, which are a subset of industrial control systems. SCADA systems control

the processes in our energy, transportation, water management, and other industries. They are the backbone in the technical structure of our society. SCADA systems can remain viable for decades, depending on the processes and machinery these systems control. However, SCADA systems often lack capacity or are difficult to upgrade to meet contemporary cybersecurity challenges. Many of these systems were never intended nor designed to be connected to any other computer, let alone linked to a global information network such as the Internet. The range of vulnerabilities has increased dramatically as embedded software in electro-mechanical machinery has become a standard feature. These programmable controllers in industry and utility companies have limited cybersecurity features. The hardening and increased protection of American SCADA systems is likely to take decades; the majority of the SCADA systems are not upgraded once installed and need additional computer hard-

ware to be secured. The defense of these systems is defense in depth, where the corporations and municipalities are parties, as well as the Department of Defense in conjunction with other federal agencies. The most able components in these defensive layers reside within the federal sphere. The question is—if cyberdefense fails, what could happen? The environmental ramifications deserve as much attention as the potential threat to computer systems.

Hydroelectric Dams and Reservoirs

For example, a series of dam failures in a large watershed would have significant environmental impacts. Hydroelectric dams and reservoirs are controlled using different forms of computer networks, either cable or wireless, and the control networks connect to the Internet. A breach in the cyberdefenses of an electric utility company could lead all the way down to the logic controllers that instruct the electric machinery to open the floodgates. Many hydroelectric dams and reservoirs are designed as a chain of dams in a major watershed to create an even flow of water for generating energy. A cyberattack on several upstream dams could release water that would increase pressure on downstream dams. With rapidly diminishing storage capacity, downstream dams would risk being breached by the oncoming water. Eventually, the attack could have a cascading effect, literally and figuratively, through the river system and result in a catastrophic flood. The traditional cybersecurity way to frame the problem is to consider the loss of function and disruption in electricity generation—overlooking the potential environmental effect of an inland tsunami. This is especially troublesome where the population and the industries are dense along a river, such as in Pennsylvania, West Virginia, and other areas with cities built around historic mills. If the cyberattack occurred during a heavy rain when the dams were already stressed, any rapid increase in water level could trigger successive dam collapses.⁸ This could lead to a catastrophic loss of lives and property and a critical loss of hydroelectric capacity. The environmental effects would be dramatic and long-term: freshwater resources would be contaminated, complete ecosystems destroyed, toxic agents released, and soil heavily eroded or



The Big Tujunga Dam is under construction to reinforce the walls due to an increased debris flow from recent severe winter storms, La Cañada Flintridge, Calif., 2 August 2010. (Adam DuBrowa, FEMA)

completely washed away. Fish populations would be decimated along with fisheries that rely upon them. The short-term and long-term effects would be substantial, and restoration efforts could be too costly for the nation to pursue. The environmental damage would be permanent.

U.S. Chemical Industry

The sizeable U.S. chemical industry provides another example of the potential environmental impact of a cyberattack. Manufacturing plants and storage facilities store large quantities of industrial chemicals. The U.S. chemical industry produced \$759 billion of chemical products in 2011.⁹ Over 96 percent of all manufactured products in the United States rely on the input of chemical material. The country produces 15 percent of the world's chemicals and transports 847 million tons of chemicals on railways, highways, and freight ships each year.¹⁰ The transportation routes are adjacent to or passing creeks, rivers, ground water aquifers, urban areas, and agricultural land. These chemical fluids, once released, could create contamination that requires long-term mitigation, restoration, and remediation of affected areas with costs equal to that of an EPA superfund site.¹¹

Chemicals could infiltrate groundwater and make it a health hazard, pollute the air, contaminate the soil, and make land unsuitable for housing, agriculture, and development. Environmental damage could be irreversible if the national cyberdefense failed.

Environmental Defense

Defending American infrastructure from cyberattacks is not only protecting information, network availability, or the global information grid. It is also safeguarding the lives of citizens, protecting property, and preserving ecosystems and the ecosystem services that we rely on. An attack leading to environmental damages could impact our societal stability.¹²

The national cyberdefense organized by the Department of Defense and other government agencies is on a "green" mission to ensure cyberattacks do not create irreversible environmental damage within the United States. Successful cyberdefense mitigates the risk for significant damage to domestic freshwater drinking sources, aquatic and adjacent terrestrial ecosystems, and biological diversity. This mission must continue to protect the natural resources essential for life. **MR**

NOTES

1. Barack Obama and Leon E. Panetta, *Sustaining U.S. Global Leadership: Priorities for 21st Century Defense*, Vol. 1 (Washington DC: Government Printing Office, 2012).

2. Leon E. Panetta, "Defending the Nation from Cyber Attack" (speech given to Business Executives for National Security, New York, 11 October 2012).

3. Thomas Rid, "Cyber War Will Not Take Place," *Journal of Strategic Studies* 35, no. 1 (2012): 5-32.

4. Thomas Rid and Peter McBurney, "Cyber-Weapons," *The RUSI Journal* 157, no. 1 (2012): 6-13.

5. Idaho National Laboratory, 2005, "US-CERT Control Systems Security Center," Cyber Incidents Involving Control Systems, INL/EXT-05-00671, <<http://www.inl.gov/technicalpublications/documents/3480144.pdf>>.

6. Jan Kallberg and Adam Lowther, "The Return of Dr. Strangelove," *The Diplomat*, 20 August 2012.

7. William F. Lynn III, "Defending a New Domain: The Pentagon's Cyberstrategy," *Foreign Affairs* 89 (2010): 97.

8. "Isaac Leaves Hundreds of Homes Underwater; Dam Shows Stress," *Los Angeles Times*, 30 August 2012, <<http://articles.latimes.com/2012/aug/30/nation/la-na-isaac-storm-20120831>>.

9. American Chemistry Council, <<http://www.americanchemistry.com/Jobs/EconomicStatistics/Industry-Profile/Global-Business-of-Chemistry>>.

10. American Chemistry Council, <<http://www.americanchemistry.com/chemistry-industry-facts>>.

11. Environmental Protection Agency. Superfund Sites, <<http://www.epa.gov/superfund/sites/npl/where.htm>>.

12. Jan Kallberg and Bhavani Thuraisingham, "State Actors's Offensive Cyber Operations—The Disruptive Power of Resourceful Systematic Cyber Attacks," *IEEE IT Professional* 15, no. 3 (2013): 32-35.



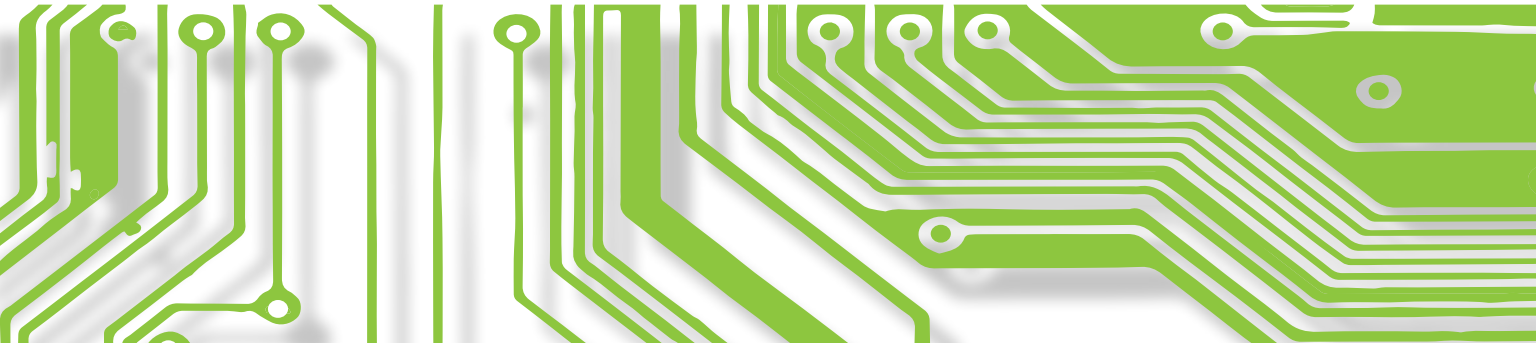
The Utility of Cyberpower

Lt. Col. Kevin L. Parker, U.S. Air Force

AFTER MORE THAN 50 YEARS, the Korean War has not officially ended, but artillery barrages seldom fly across the demilitarized zone.¹ U.S. forces continue to fight in Afghanistan after more than 10 years, with no formal declaration of war.² Another conflict rages today with neither bullets nor declarations. In this conflict, U.S. adversaries conduct probes, attacks, and assaults on a daily basis.³ The offensives are not visible or audible, but they are no less real than artillery shells or improvised explosive devices. This conflict occurs daily through cyberspace.

To fulfill the U.S. military's purpose of defending the nation and advancing national interests, today's complex security environment requires increased engagement in cyberspace.⁴ Accordingly, the Department of Defense (DOD) now considers cyberspace an operational domain.⁵ Similar to other domains, cyberspace has its own set of distinctive characteristics. These attributes present unique advantages and corresponding limitations. As the character of war changes, comprehending the utility of cyberpower requires assessing its advantages and limitations in potential strategic contexts.

Lt. Col. Kevin L. Parker, U.S. Air Force, is the commander of the 100th Civil Engineer Squadron at RAF Mildenhall, United Kingdom. He holds a B.S. in civil engineering from Texas A&M University, an M.A. in human resource development from Webster University, and an M.S. in military operational art and science and an M.Phil. in military strategy from Air University. He has deployed to Saudi Arabia, Kyrgyzstan, and twice to Iraq.



Defining Cyberspace and Cyberpower

A range of definitions for cyberspace and cyberpower exist, but even the importance of establishing definitions is debated. Daniel Kuehl compiled 14 distinct definitions of cyberspace from various sources, only to conclude he should offer his own.⁶ Do exact definitions matter? In bureaucratic organizations, definitions do matter because they facilitate clear division of roles and missions across departments and military services. Within DOD, some duplication of effort may be desirable but comes at a high cost; therefore, definitions are necessary to facilitate the rigorous analyses essential for establishing organizational boundaries and budgets.⁷ In executing assigned roles, definitions matter greatly for cross-organizational communication and coordination.

No matter how important, precise definitions to satisfy all viewpoints and contexts are elusive. Consider defining the sea as all the world's oceans. This definition lacks sufficient clarity to demarcate bays or riverine waterways. Seemingly inconsequential, the ambiguity is of great consequence for organizations jurisdictionally bound at a river's edge. Unlike the sea's constant presence for millennia, the Internet is a

relatively new phenomenon that continues to expand and evolve rapidly. Pursuing single definitions of cyberspace and cyberpower to put all questions to rest may be futile. David Lonsdale argued that from a strategic perspective, definitions matter little. In his view, "what really matters is to perceive the infosphere as a place that exists, understand the nature of it and regard it as something that can be manipulated and used for strategic advantage."⁸ The definitions below are consistent with Lonsdale's viewpoint and suffice for the purposes of this discussion, but they are unlikely to satisfy practitioners who wish to apply them beyond a strategic perspective.

Cyberspace: the domain that exists for inputting, storing, transmitting, and extracting information utilizing the electromagnetic spectrum. It includes all hardware, software, and transmission media used, from an initiator's input (e.g., fingers making keystrokes, speaking into microphones, or feeding documents into scanners) to presentation of the information for user cognition (e.g., images on displays, sound emitted from speakers, or document reproduction) or other action (e.g., guiding an unmanned vehicle or closing valves).

Cyberpower: The potential to use cyberspace to achieve desired outcomes.⁹



U.S. Cyber Command held a joint cyberspace training exercise during November 2011, primarily conducted at the Air Force Red Flag Facility at Nellis Air Force Base, Nev. The exercise brought together approximately 300 cyber and information technology professionals, 2 November 2011. (U.S. Army)

Advantages of Wielding Cyberpower

With these definitions being sufficient for this discussion, consider the advantages of operations through cyberspace.

Cyberspace provides worldwide reach. The number of people, places, and systems interconnecting through cyberspace is growing rapidly.¹⁰ Those connections enhance the military's ability to reach people, places, and systems around the world. Operating in cyberspace provides access to areas denied in other domains. Early airpower advocates claimed airplanes offered an alternative to boots on the ground that could fly past enemy defenses to attack power centers directly.¹¹ Sophisticated air defenses developed quickly, increasing the risk to aerial attacks and decreasing their advantage. Despite the current cyberdefenses that exist, cyberspace now offers the advantage of access to contested areas without putting operators in harm's way. One example of directly reaching enemy decision makers through cyberspace comes from an event in 2003, before the U.S. invasion of Iraq. U.S. Central Command reportedly emailed Iraqi military officers a message on their secret network advising them to abandon their posts.¹² No other domain had so much reach with so little risk.

Cyberspace enables quick action and concentration. Not only does cyberspace allow worldwide reach, but its speed is unmatched. With aerial refueling, air forces can reach virtually any point on the earth; however, getting there can take hours. Forward basing may reduce response times to minutes, but information through fiber optic cables moves literally at the speed of light. Initiators of cyberattacks can achieve concentration by enlisting the help of other computers. By discretely distributing a virus trained to respond on command, thousands of co-opted botnet computers can instantly initiate a distributed denial-of-service attack. Actors can entice additional users to join their cause voluntarily, as did Russian "patriotic hackers" who joined attacks on Estonia in 2007.¹³ With these techniques, large interconnected populations could mobilize on an unprecedented scale in mass, time, and concentration.¹⁴

Cyberspace allows anonymity. The Internet's designers placed a high priority on decentralization and built the structure based on the mutual trust of its few users.¹⁵ In the decades since, the number of

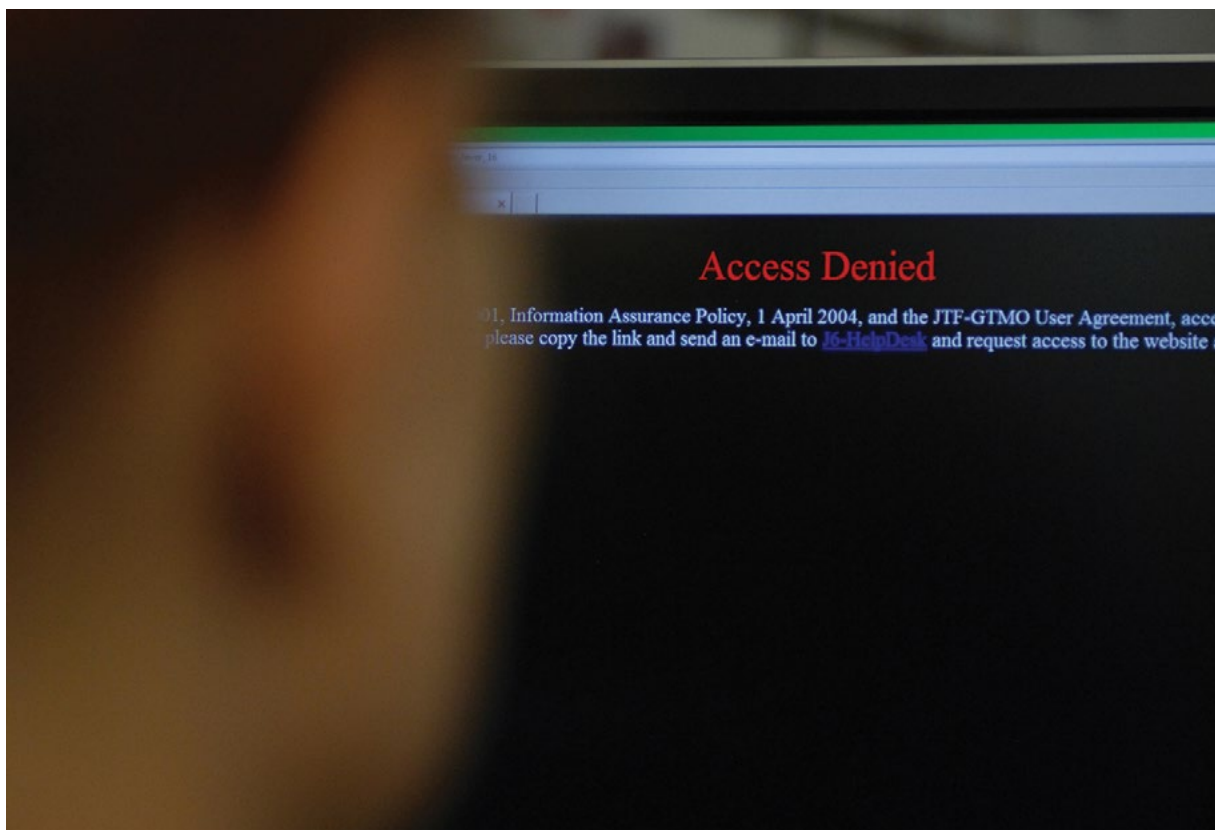
Internet users and uses has grown exponentially beyond its original conception.¹⁶ The resulting system makes it very difficult to follow an evidentiary trail back to any user.¹⁷ Anonymity allows freedom of action with limited attribution.

Cyberspace favors offense. In Clausewitz' day, defense was stronger, but cyberspace, due to the advantages listed above, currently favors the attack.¹⁸

Historically, advantages from technological leaps erode over time.¹⁹ However, the current circumstance pits defenders against quick, concentrated attacks, aided by structural security vulnerabilities inherent in the architecture of cyberspace.

Cyberspace expands the spectrum of nonlethal weapons. Joseph Nye described a trend, especially among democracies, of antimilitarism, which makes using force "a politically risky choice."²⁰ The desire to limit collateral damage often has taken center stage in NATO operations in Afghanistan, but this desire is not limited to counterinsurgencies.²¹ Precision-guided munitions and small-diameter bombs are products of efforts to enhance attack capabilities with less risk of collateral damage. Cyberattacks offer nonlethal means of direct action against an adversary.²² The advantages of cyberpower may be seductive to policymakers, but understanding its limitations should temper such enthusiasm. The most obvious limitation is that your adversary may use all the same advantages against you. Another obvious limitation is its minimal influence on nonnetworked adversaries. Conversely, the more any organization relies on cyberspace, the more vulnerable it is to cyberattack. Three additional limitations require further attention.

Cyberspace attacks rely heavily on second order effects. In Thomas Schelling's terms, there are no brute force options through cyberspace, so cyberoperations rely on coercion.²³ Continental armies can occupy land and take objectives by brute force, but success in operations through cyberspace often hinges on how adversaries react to provided, altered, or withheld information. Cyberattacks creating kinetic effects, such as destructive commands to industrial control systems, are possible. However, the unusual incidents of malicious code causing a Russian pipeline to explode and the Stuxnet worm shutting down Iranian nuclear facility processes were not ends.²⁴ In the latter case, only Iranian leaders' decisions could realize abandonment of



Access Denied! J-6 Information Assurance runs proxies to protect Joint Task Force Guantanamo servers from malicious websites. Information Assurance defends joint task force servers from internal and external threats while ensuring they comply with Defense Information Systems Agency, U.S. Army, and U.S. Southern Command procedures and policies, Guantanamo Bay, Cuba, 8 July 2008. (U.S. Navy)

nuclear technology pursuits. Similar to strategic bombing's inability to collapse morale in World War II, cyberattacks often rely on unpredictable second order effects.²⁵ If Rear Adm. Wylie is correct in that war is a matter of control, and "its ultimate tool ... is the man on the scene with a gun," then operations through cyberspace can only deliver a lesser form of control.²⁶ Evgeny Morozov quipped, "Tweets, of course, don't topple governments; people do."²⁷

Cyberattacks risk unintended consequences.

Just as striking a military installation's power system may have cascading ramifications on a wider population, limiting effects through interconnected cyberspace is difficult. Marksmanship instructors teach shooters to consider their maximum range and what lies beyond their targets. Without maps for all systems, identifying maximum ranges and what lies beyond a target through cyberspace is impossible.

Defending against cyberattacks is possible.

The current offensive advantage does not make

all defense pointless. Even if intrusions from sophisticated, persistent attacks are inevitable, certain defensive measures (e.g., physical security controls, limiting user access, filtering and anti-virus software, and firewalls) do offer some protection. Redundancy and replication are resilience strategies that can deter some would-be attackers by making attacks futile.²⁸ Retaliatory responses via cyberspace or other means can also enhance deterrence.²⁹ Defense is currently disadvantaged, but offense gets no free pass in cyberspace.

Expectations and Recommendations

The advantages and limitations of using cyberpower inform expectations for the future and several recommendations for the military.

Do not expect clear, comprehensive policy soon.³⁰ Articulating a comprehensive U.S. strategy for employing nuclear weapons lagged 15 years behind their first use, and the timeline for

clear, comprehensive cyberspace policy may take longer.³¹ Multiple interests collide in cyberspace, forcing policy makers to address concepts that traditionally have been difficult for Americans to resolve. Cyberspace, like foreign policy, exposes the tension between defaulting to realism in an ungoverned, anarchic system, and aspiring to the liberal ideal of security through mutual recognition of natural rights. Cyberspace policy requires adjudicating between numerous priorities based on

Defending against cyberattacks takes more than firewalls.

esteemed values such as intellectual property rights, the role of government in business, bringing criminals to justice, freedom of speech, national security interests, and personal privacy. None of these issues is new. Cyberspace just weaves them together and presents them from unfamiliar angles. For example, free speech rights may not extend to falsely shouting fire in crowded theaters, but through cyberspace all words are broadcast to a global crowded theater.³²

Beyond the domestic front, Internet access creates at least one significant foreign policy dilemma. While it can help mobilize and empower dissidents under oppressive governments, it also can provide additional population control tools to authoritarian leaders.³³ The untangling of these sets of overlapping issues in new contexts is not likely to happen quickly. It may take several iterations, and it may only occur in crises. Meanwhile, the military must continue developing capabilities for operating through cyberspace within current policies.

Defend in depth—inner layers. Achieving resilience requires evaluating dependencies and vulnerabilities at all levels. Starting inside the firewall and working outward, defense begins at the lowest unit level. Organizations and functions should be resilient enough to sustain attacks and continue operating. In a period of declining budgets, decision makers will pursue efficiencies through leveraging technology.³⁴ Therefore, prudence requires

reinvesting some of the savings to evaluate and offset vulnerabilities created by new technological dependencies.³⁵ Future war games should not just evaluate what new technologies can provide, but also they should consider how all capabilities would be affected if denied access to cyberspace.

Beyond basic user responsibilities, forces providing defense against cyberattacks require organizations and command structures particular to their function. Martin van Creveld outlined historical evolutions of command and technological developments. Consistent with his analysis, military cyberdefense leaders should resist the technology-enabled urge to centralize and master all available information at the highest level. Instead, their organizations should act semi-independently, set low decision thresholds, establish meaningful regular information reporting, and use formal and informal communications.³⁶ These methods can enhance “continuous trial-and-error learning essential to collectively make sense of disabling surprises” and shorten response times.³⁷ Network structures may be more appropriate for this type of task than traditional hierarchical military structures.³⁸ Whatever the structure, military leaders must be willing to subordinate tradition and task-organize their defenses for effectiveness against cyberattacks.³⁹ After all, weapons “do not triumph in battle; rather, success is the product of man-machine weapon systems, their supporting services of all kinds, and the organization, doctrine, and training that launch them into battle.”⁴⁰

Defend in depth—outer layers. Defending against cyberattacks takes more than firewalls. Expanding defense in depth requires creatively leveraging influence. DOD has no ownership or jurisdiction over the civilian sectors operating the Internet infrastructure and developing computer hardware and software. However, DOD systems are vulnerable to cyberattack through each of these avenues beyond their control.⁴¹ Richard Clarke recommended federal regulation starting with the Internet backbone as the best way to overcome systemic vulnerabilities.⁴² Backlash over potential legislation regulating Internet activity illustrates the problematic nature of regulation.⁴³ So, how can DOD effect change seemingly beyond its control? Label it “soft power” or “friendly conquest of cyberspace,” but the answer lies in leveraging assets.⁴⁴

One of DOD's biggest assets to leverage is its buying power. In 2011, DOD spent over \$375 billion on contracts.⁴⁵ The military should, of course, use its buying power to insist on strict security standards when purchasing hardware and software. However, it also can use its acquisition process to reduce vulnerabilities through its use of defense contractors. Similar to detailed classification requirements, contracts should specify network security protocols for all contract firms as well as their suppliers, regardless of the services provided. Maintaining stricter security protocols than industry standards would become a condition of lucrative contracts. Through its contracts, allies, and position as the nation's largest employer, DOD can affect preferences to improve outer layer defenses.⁴⁶

Develop an offensive defense. Even in defensive war, Clausewitz recognized the necessity of offense to return enemy blows and achieve victory.⁴⁷ Robust offensive capabilities can enhance deterrence by affecting an adversary's decision calculus.⁴⁸ DOD must prepare for contingencies calling for offensive support to other domains or independent action through cyberspace.

The military should develop offensive capabilities for potential scenarios but should purposefully define its preparations as defense. Communicating a defensive posture is important to avoid hastening a security-dilemma-inspired cyber-arms race that may have already started.⁴⁹ Over 20 nations reportedly have some cyberwar capability.⁵⁰ Even if it is too late to slow others' offensive development, controlling the narrative remains important.⁵¹ Just as the name Department of Defense sends a different message than its former name—War Department—developing defensive capabilities to shut down rogue cyberattackers sounds significantly better than developing offensive capabilities that “knock [the enemy] out in the first round.”⁵²

Do not expect rapid changes in international order or the nature of war. Without question, the world is changing, but world order does not change overnight. Nye detailed changes due to globalization and the spread of information technologies, including diffusion of U.S. power to rising nations and nonstate actors. However, he claimed it was not a “narrative of decline” and wrote, “The United States is unlikely to decay like ancient Rome or even to be surpassed by another state.”⁵³ Adapting to current trends is



Secretary of the Army John McHugh receives an update briefing from staff members of U.S. Army Cyber Command, Fort Belvoir, Va., 2 April 2012. (U.S.Army)

necessary, but changes in the strategic climate are not as dramatic as some proclaim.

Similarly, some aspects of war change with the times while its nature remains constant. Clausewitz advised planning should account for the contemporary character of war.⁵⁴ Advances in cyberspace are changing war's character but not totally eclipsing traditional means. Sir John Slessor noted, "If there is one attitude more dangerous than to assume that a future war will be just like the last one, it is to imagine that it will be so utterly different that we can afford to ignore all the lessons of the last one."⁵⁵ Further, Lonsdale advised exploiting advances in cyberspace but not to "expect these changes to alter the nature of war."⁵⁶ Wars will continue to be governed by politics, affected by chance, and waged by people even if through cyberspace.⁵⁷

Do not overpromise. Advocates of wielding cyberpower must bridle their enthusiasm enough to see that its utility only exists within a strategic context. Colin Gray claimed airpower enthusiasts "all but invited government and the public to ask the wrong questions and hold air force performance to irrelevant standards of superheroic effectiveness."⁵⁸ By touting decisive, independent, strategic capabilities, airpower advocates often failed to meet such hyped expectations in actual conflicts. Strategic contexts may have occurred where airpower alone could achieve strategic

effects, but more often, airpower was one of many tools employed.

Cyberpower is no different. Gray claimed, "When a new form of war is analyzed and debated, it can be difficult to persuade prophets that prospective efficacy need not be conclusive."⁵⁹ Cyberpower advocates must recognize not only its advantages, but also its limitations applied in a strategic context.

Conclusion

If cyberpower is the potential to use cyberspace to achieve desired outcomes, then the strategic context is key to understanding its utility. As the character of war changes and cyberpower joins the fight alongside other domains, military leaders must make sober judgments about what it can contribute to achieving desired outcomes. Decision makers must weigh the opportunities and advantages cyberspace presents against the vulnerabilities and limitations of operations in that domain. Sir Arthur Tedder discounted debate over one military arm or another winning wars single-handedly. He insisted, "All three arms of defense are inevitably involved, though the correct balance between them may and will vary."⁶⁰ Today's wars may involve more arms, but Tedder's concept of applying a mix of tools based on their advantages and limitations in the strategic context still stands as good advice. **MR**

NOTES

1. See Chico Harlan, "Korean DMZ troops exchange gunfire," *Washington Post*, 30 October 2010, <<http://www.washingtonpost.com/wp-dyn/content/article/2010/10/29/AR2010102906427.html>>. Bullets occasionally fly across the demilitarized zone, but occurrences are rare.

2. See *Authorization for Use of Military Force*, Public Law 107-40, 107th Cong., 18 September 2001, <<http://www.gpo.gov/fdsys/pkg/PLAW-107publ40/html/PLAW-107publ40.htm>>. The use of military force in Afghanistan was authorized by the U.S. Congress in 2001 through Public Law 107-40, which does not include a declaration of war.

3. "DOD systems are probed by unauthorized users approximately 250,000 times an hour, over 6 million times a day," Gen. Keith Alexander, director, National Security Agency and Commander, U.S. Cyber Command (remarks, Center for Strategic and International Studies Cybersecurity Policy Debate Series: US Cybersecurity Policy and the Role of US Cybercom, Washington, DC, 3 June 2010, 5), <http://www.nsa.gov/public_info/files/speeches_testimonies/100603_alexander_transcript.pdf>.

4. "The purpose of this document is to provide the ways and means by which our military will advance our enduring national interests ... and to accomplish the defense objectives in the 2010 Quadrennial Defense Review." Joint Chiefs of Staff, *The National Military Strategy of the United States of America, 2011: Redefining America's Military Leadership* (Washington, DC: United States Government Printing Office [GPO], 8 February 2011), i.

5. DOD, *DOD Strategy for Operating in Cyberspace* (Washington, DC: GPO, July 2011), 5.

6. Daniel T. Kuehl, "From Cyberspace to Cyberpower: Defining the Problem," in *Cyberpower and National Security*, eds. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Dulles, VA: Potomac Books, 2009): 26-28.

7. Staff Report to the Senate Committee on Armed Services, *Defense Organization: The Need for Change*, 99th Cong., 1st sess., 1985, Committee Print, 442-44.

8. David J. Lonsdale, *The Nature of War in the Information Age: Clausewitzian Future* (London: Frank Cass, 2004), 182.

9. See Joseph S. Nye, Jr., *The Future of Power* (New York: PublicAffairs, 2011), 123. This definition is influenced by the work of Nye.

10. "From 2000 to 2010, global Internet usage increased from 360 million to over 2 billion people," *DOD Strategy for Operating in Cyberspace*, 1.

11. Giulio Douhet, *The Command of the Air* (Tuscaloosa, AL: University of Alabama Press, 2009), 9.

12. Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What To Do About It* (New York: HarperCollins Publisher, 2010), 9-10.

13. Nye, 126.

14. Audrey Kurth Cronin, "Cyber-Mobilization: The New *Levée en Masse*," *Parameters* (Summer 2006): 77-87.

15. Clarke and Knake, 81-84.

16. See Clarke and Knake, 84-85. Trends in the number of Internet-connected devices threaten to use up all 4.29 billion available addresses based on the original 32-bit numbering system.

17. Clay Wilson, "Cyber Crime," in *Cyberpower and National Security*, eds. Franklin D. Kramer, Stuart H. Starr, Larry Wentz (Washington, DC: NDU Press, 2009), 428.

18. Carl von Clausewitz, *On War*, ed. and trans. Michael Howard and Peter Paret (Princeton, NJ: Princeton University Press, 1976), 357; John B. Sheldon, "Deciphering Cyberpower: Strategic Purpose in Peace and War," *Strategic Studies Quarterly* (Summer 2011): 98.

19. Martin van Creveld, *Command in War* (Cambridge, MA: Harvard University Press, 1985), 231.

20. Nye, 30.

21. Dexter Filkins, "US Tightens Airstrike Policy in Afghanistan," *New York Times*,

21 June 2009, <<http://www.nytimes.com/2009/06/22/world/asia/22airstrikes.html>>.

22. "We will improve our cyberspace capabilities so they can often achieve significant and proportionate effects with less cost and lower collateral impact." Chairman of the Joint Chiefs of Staff, *The National Military Strategy of the United States of America 2011: Redefining America's Military Leadership*, (Washington, DC: GPO, 2011), 19.

23. Thomas C. Schelling, *Arms and Influence* (New Haven, CT: Yale University, 2008), 2-4.

24. For Russian pipeline, see Clarke and Knake, 93; for Stuxnet, see Nye, 127. 25. Lonsdale, 143-45.

26. Rear Adm. J.C. Wylie, *Military Strategy: A General Theory of Power Control* (Annapolis, MD: Naval Institute Press, 1989), 74.

27. Evgeny Morozov, *The Net Delusion: The Dark Side of Internet Freedom* (New York: PublicAffairs, 2011), 19.

28. Nye, 147.

29. Richard L. Kugler, "Deterrence of Cyber Attacks," *Cyberpower and National Security*, eds. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Washington, DC: NDU Press, 2009), 320.

30. See United States Office of the President, *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World*, May 2011.

31. See Clarke and Knake, 155. International strategy for cyberspace addresses diplomacy, defense, and development in cyberspace but fails to outline relative priorities for conflicting policy interests. 31.

32. First Amendment free speech rights and their limits have been a contentious issue for decades. "Shouting fire in a crowded theater" comes from a 1919 U.S. Supreme Court case, *Schenck v. United States*. Justice Oliver Wendell Holmes' established context as relevant for limiting free speech. An "imminent lawless action" test superseded his "clear and present danger" test in 1969, <http://www.pbs.org/wnet/supremecourt/capitalism/landmark_schenck.html>.

33. Morozov, 28.

34. "Today's information technology capabilities have made this vision [of precision logistics] possible, and tomorrow's demand for efficiency has made the need urgent." Gen. Norton Schwartz, chief of staff, U.S. Air Force, "Toward More Efficient Military Logistics," address on 29 March 2011, to the 27th Annual Logistics Conference and Exhibition, Miami, FL, <<http://www.af.mil/shared/media/document/AFD-110330-053.pdf>>.

35. Chris C. Demchak, *Wars of Disruption and Resilience: Cybered Conflict, Power, and National Security* (Athens, GA: University of Georgia Press, 2011), 44.

36. Van Creveld, 269-70.

37. Demchak, 73.

38. Antoine Bousquet, *The Scientific Way of Warfare: Order and Chaos on the Battlefields of Modernity* (New York: Columbia University Press, 2009), 228-29.

39. See R.A. Ratcliff, *Delusions of Intelligence: Enigma, Ultra, and the End of*

Secure Ciphers (Cambridge, UK: Cambridge University Press, 2006), 229-30. Allied World War II Enigma code-breaking offers a successful example of creatively task-organizing without rigid hierarchy.

40. Colin S. Gray, *Explorations in Strategy* (Westport, CT: Praeger, 1996), 133.

41. *DOD Strategy for Operating in Cyberspace*, 8.

42. Clarke and Knake, 160.

43. Geoffrey A. Fowler, "Wikipedia, Google Go Black to Protest SOPA," *Wall Street Journal*, 18 January 2012, <http://online.wsj.com/article/SB10001424052970204555904577167873208040252.html?mod=WSJ_Tech_LEADTop>; Associated Press, "White House objects to legislation that would undermine 'dynamic' Internet," *Washington Post*, 14 January 2012, <http://www.washingtonpost.com/politics/courts-law/white-house-objects-to-legislation-that-would-undermine-dynamic-internet/2012/01/14/gIQAJsFcyP_story.html>.

44. "Soft power," see Nye, 81-82; "friendly conquest," see Martin C. Libicki, *Conquest in Cyberspace: National Security and Information Warfare* (Cambridge, UK: Cambridge University Press, 2007), 166.

45. U.S. Government, USASpending.gov official Web site, "Prime Award Spending Data," <<http://www.usaspending.gov/explore?carryfilters=on>> (18 January 2012). "2011" refers to the fiscal year.

46. DOD Web site, "About the Department of Defense," <<http://www.defense.gov/about>> (18 January 2012). DOD employs 1.4 million active, 1.1 million National Guard/Reserve, 718,000 civilian personnel.

47. Clausewitz, 357.

48. Kugler, "Deterrence of Cyber Attacks," 335.

49. "Many observers postulate that multiple actors are developing expert [cyber] attack capabilities." Ibid., 337.

50. Clarke and Knake, 144.

51. "Narratives are particularly important in framing issues in persuasive ways." Nye, 93-94.

52. Quote from Gen. Robert Elder as commander of Air Force Cyber Command. See Clarke and Knake, 158; Defense Tech, "Chinese Cyberwar Alert!" 15 June 2007, <<http://defensetech.org/2007/06/15/chinese-cyberwar-alert>>.

53. Nye, 234.

54. Clausewitz, 220.

55. John Cotesworth Slessor, *Air Power and Armies* (Tuscaloosa, AL: University of Alabama Press, 2009), iv.

56. Lonsdale, 232.

57. Clausewitz, 89.

58. Gray, 58.

59. Colin S. Gray, *Modern Strategy* (Oxford, UK: Oxford University Press, 1999), 270.

60. Arthur W. Tedder, *Air Power in War*, (Tuscaloosa: University of Alabama Press, 2010), 88.

Military Review



Tired of waiting between issues for great articles?

You no longer have to—MR Spotlight is online now! This new feature publishes articles bi-weekly, so you now have access to more information more often! Check out our most current and previous articles now on our website! Go to <http://usacac.army.mil/CAC2/MilitaryReview/index.asp> and click on the "MR Spotlight" link to get started.

Want to comment? *Military Review* is on Facebook and Twitter.

The official *Military Review* Facebook and Twitter sites are now available for readers to comment on the overall layout, design, or content of the magazine. We also strongly encourage professional discussion and debate on all articles published in *Military Review*. To comment, go to our webpage at <http://militaryreview.army.mil/> and click on the Facebook icon, or reach out to us on Twitter at <http://twitter.com/@MilReview>.

"Military Review is an important forum that helps shape the dialogue of our profession."

—GEN Raymond T. Odierno



Beyond Cocaine Cowboys

Looking at Security in Latin America from a Different Perspective

Maj. Gen. Frederick S. Rudesheim, U.S. Army and Maj. Michael L. Burgoyne, U.S. Army

LET'S PLAY A REGIONAL WORD ASSOCIATION GAME: I say "Latin America," you say "drugs." Perhaps you have visions of gun-toting 1980s Colombian drug cartel enforcers tearing up the streets of Miami as depicted in Billy Corben's documentary *Cocaine Cowboys*.¹ Since 1986, when President Ronald Reagan first designated drug trafficking as a threat to "the national security of the United States," U.S. counterdrug policy has come to dominate every aspect of U.S. security efforts in the Western Hemisphere.² In 2012, nearly 90 percent of law enforcement and military aid to Latin America was focused on counternarcotics.³ Yet, there is so much more to Latin America than drugs; it is a dynamic economic region. The United States needs a broad security policy for Latin America that looks beyond a counterdrug focus to create stability and foster increased prosperity.

Maj. Gen. Frederick S. Rudesheim, U.S. Army, currently serves as the vice director of the Joint Staff. He most recently commanded U.S. Army South and previously served as deputy director, Western Hemisphere, J5, Joint Staff. He holds a B.S. from the University of Texas at Austin, an M.S. from Troy State University, an M.S. from the School of Advanced Military Studies, and an M.S. from the U.S. Army War College.

*Maj. Michael L. Burgoyne, U.S. Army, has served as the Andean Ridge desk officer at U.S. Army South. Previous assignments include two tours in Iraq. He holds an M.A. from Georgetown University. Maj. Burgoyne is the coauthor of *The Defense of Jisr al-Doreaa*, a tactical primer on counterinsurgency.*

Former chairman of the Joint Chiefs of Staff Adm. Michael Mullen stated, “The most significant threat to our national security is our debt.”⁴ Consistent with this true statement, U.S. security policy has a vital role in improving the economic prosperity of our nation. As “the third pillar of the West, alongside Europe and North America,” Latin America can have a significant economic effect on the United States.⁵ Cultural ties with the region are rapidly strengthening; U.S. Latinos are expected to make up a third of the population by 2050.⁶ The United States may find itself with more Spanish speakers than any other country. Economic opportunities are remarkable; last year, U.S. trade with the region exceeded \$700 billion.⁷ The population of Latin America is nearly 600 million, roughly half the population of China.⁸ Geo-strategist Parag Khanna makes a powerful argument for a U.S. focus not on Asia, but rather on Latin America. He argues persuasively that by increasing commerce with Latin America, the United States can significantly boost economic prosperity in the hemisphere.⁹ The diplomatic and economic elements of national power are already deeply involved in development, but these initiatives will be stymied in the absence of a matching military and law enforcement effort.

If the United States is to pursue a more robust policy toward increasing our economic partnerships with Latin American countries, the security of their citizens will be a prerequisite. One need only look to Colombia to see the importance of security in economic development. A decade of successful security policies under presidents Alvaro Uribe and Juan Manuel Santos have reduced the number of Revolutionary Armed Forces of Colombia members by half. Colombia’s focus on “democratic security” has delivered positive results in virtually every measure of citizen security: kidnappings declined 89 percent, homicides 49 percent, and terrorist attacks 66 percent.¹⁰ As a result, Colombia’s gross domestic product averaged a 4.54 percent growth rate from 2002 to 2012, increasing by \$244 billion.¹¹ The U.S. role in Colombia’s success was driven mainly by Plan Colombia counterdrug funding. However, not all destabilizing forces in the region fit into the drug trafficking mold.

Powerful criminal gangs are a serious problem throughout the region and especially in Central America. The most dangerous criminal gangs, often referred to as “third-generation gangs,” are militarized criminal groups that use guerrilla or rudimentary light-infantry tactics against the state.¹² These groups often engage in retail drug sales but do not reach the transnational level that would invite significant U.S. counterdrug interventions; yet, their impact on citizen security is tremendous. It is estimated that crime costs almost

The Darien region of Panama remains so remote and outside of government control that the Pan-American Highway has yet to bridge the complex terrain.

eight percent of Central America’s gross domestic product, some \$20 billion.¹³ Perhaps worse is the loss of untold amounts of foreign direct investment that goes to safer locales.

Stability and security are crucial for developing extensive hemispheric economic infrastructure. Criminal groups limit the free flow of commerce, engaging in illegal taxation and extortion in cities, seaports, airports, and highways. The Darien region of Panama remains so remote and outside government control that the Pan-American Highway has yet to bridge the complex terrain. Given the economic benefit this highway would have for the region, it should be a priority for U.S. security efforts. Moreover, pipelines, mining, electrical grids, and other valuable economic infrastructure are often the target of attack by criminal groups and insurgents. Unfortunately, infrastructure security is largely a secondary priority behind counterdrug engagement. Security cooperation will need to expand outside the limitations of its current construction if stability is the overarching goal.

The need to contend with state threats and border tensions often becomes secondary to the



Former U.S. Secretary of State Colin Powell visiting Colombia as a part of United States support of Plan Colombia. (DOD)

counterdrug fight, but such issues can have a significant and long-term effect on economic engagement. A dispute between Chile and Peru—two of the fastest growing economies in the region—over maritime boundaries continued for decades. Security cooperation that embraces setting the conditions for increased trade would examine this type of security problem and devote resources to alleviating tension through engagement.

The erosion of democracy is another major concern. Subversive elements following socialist or communist tenets—such as those of Lenin, Gramsci, and Verstrynge—are seeking to undermine democratic institutions. In some cases, they have caused significant economic disruption.¹⁴ The ongoing political unrest in Venezuela has the potential to destabilize an important economic

player in the hemisphere and the 13th largest oil producer in the world.¹⁵ Unfortunately, the United States and its regional partners have yet to develop a viable response to this type of challenge to the Democratic Charter.¹⁶ Many countries that have fallen under this scheme are intensely focused on thwarting regional economic integration.

Of course, from any perspective, the fact is that drug trafficking will remain a serious threat in the region. Cocaine begins its journey in the Andean Ridge, passes through Central America and Mexico, and brings crime, violence, and corruption all along its way to the United States. Illegal drugs, according the 2012 *National Drug Control Strategy*, were estimated to cost the U.S. economy \$193 billion.¹⁷ They create a tremendous burden on U.S. law enforcement,

the judicial system, and the health care system. Unfortunately, drugs and illicit trafficking are enduring problems that must remain a part of security policy in Latin America for the foreseeable future. Wherever possible, counterdrug programs should focus on targeting the drug trafficking organizations that are the most destabilizing. In other words, we should prioritize resources to fight drug trafficking groups that threaten stability over groups that simply traffic. The drug fight should be put into the context of stability whenever possible.

The counterdrug fight will continue, but it should no longer drive all engagement in the region. U.S. security cooperation must expand its aperture from a threat-based focus on the enduring problem of drugs to include setting the conditions for increased economic prosperity and regional integration.

The economic possibilities in Latin America are boundless. U.S. security professionals should embrace their supporting role in seizing these opportunities and change their perspective from one of defense against drugs to one of positive action to create opportunities. **MR**

The views expressed in this article are those of the authors and do not reflect the official policy or position of the Department of the Army, Department of Defense, or the U.S. Government.

NOTES

1. *Cocaine Cowboys*, documentary film directed by Billy Corben, Rakontur [film studio], 2006, <<http://www.rakontur.com/cocaine-cowboys>>.

2. United States, National Security Decision Directive No. 221, "Narcotics and National Security," 8 April 1986, <<http://www.reagan.utexas.edu/archives/reference/NSDDs.html>>. Drugs are a larger problem for producing countries and transit countries. Others, such as Chile, have been largely spared from these issues and thus have not received extensive U.S. counterdrug support.

3. Martha Mendoza, "US Military Steps Up Drug War in Latin America," *The Associated Press*, Bloomberg Business Week, 3 February 2013, <<http://www.businessweek.com/ap/2013-02-03/us-military-expands-its-drug-war-in-latin-america>>.

4. CNN Wire Staff, "Mullen: Debt is Top National Security Threat," CNN, 27 August 2010, <<http://www.cnn.com/2010/US/08/27/debt.security.mullen/index.html>>.

5. Parag Khanna, "Look South, Not East," *Foreign Policy.com*, 11 November 2011, <http://www.foreignpolicy.com/articles/2011/11/11/look_south_not_east>. See also Parag Khanna video "Mapping the future of countries," at TED.com, <http://www.ted.com/talks/parag_khanna_maps_the_future_of_countries.html>.

6. Jeffrey Passel and D'Vera Cohn, "U.S. Population Projections: 2005-2050," *Pew Research, Social and Demographic Trends*, 11 February 2008, <<http://www.pewsocialtrends.org/2008/02/11/us-population-projections-2005-2050/>>.

7. U.S. Census Bureau website, Trade in Goods With South and Central America, <<http://www.census.gov/foreign-trade/balance/c0009.html>>.

8. United Nations Department of Economic and Social Affairs, Population

Division website, *World Population Prospects: The 2012 Revision*, <<http://esa.un.org/unpd/wpp/index.htm>>.

9. Khanna.

10. Diana Quintero, Colombian vice-minister of defense, Presentation at NAS-PAA (Network of Schools of Public Policy, Affairs, and Administration) Conference, Austin, Texas, 18 October 2012.

11. The World Bank website, <<http://databank.worldbank.org/ddp/home.do>>.

12. John P. Sullivan "Third Generation Street Gangs: Turf, Cartels and Net-warriors," *Crime & Justice International*, October/November 1997, <<http://www.cjimagazine.com/archives/cjica76.html?id=543>>.

13. The World Bank website, news feature, "Central America: Private Sector Makes Fighting Crime its Business," 13 December 2012, <<http://www.worldbank.org/en/news/2012/12/13/crime-prevention-central-america-private-sector-business>>.

14. Max G. Manwaring, *Gangs, Pseudo-Militaries, and Other Modern Mercenaries: New Dynamics in Uncomfortable Wars* (Norman: University of Oklahoma Press, 2010).

15. U.S. Energy Information Administration website, Countries, <<http://www.eia.gov/countries/>>.

16. See the *Inter-American Democratic Charter* at the Organization of American States website, <http://www.oas.org/charter/docs/resolution1_en_p4.htm>.

17. Executive Office of the President of the United States, National Drug Control Strategy (Washington, DC: U.S. Government Printing Office, 2012), <http://www.whitehouse.gov/sites/default/files/ondcp/2012_ndcs.pdf>.



CyberSecurity

It Isn't Just for Signal Officers Anymore

(PHOTO: U.S. Air Force)

Lt. Col. D. Bruce Roeder, U.S. Army, Retired

SIGO!" WAS THE CRY that went up at the dining-in when the cantankerous public address microphone on the dais at the officers' club ballroom failed to work. The meat eaters in the unit would laugh or smile in relief as the poor SIGO (signal officer) valiantly struggled to get the malfunctioning feature of the podium to work as it should have. That is how some of us have approached the subject of cybersecurity: it is that wire-head guy's bailiwick, and thank goodness!

Well, if it ever was so, then it is no more. When Director of National Intelligence James R. Clapper issued the 2013 *Worldwide Threat Assessment of the US Intelligence Community* to the Senate Select Committee on Intelligence, cyberthreats appeared ahead of terrorism and weapons of mass destruction in its list of global threats to U.S. national security.¹ Indeed, cyberattacks are constantly in the news. Cybersecurity expert and Finnish reserve officer Mikko H. Hyppönen posits that in developed countries, people are more likely to be victims of crime online than crime "in real life."² With the ubiquitous nature of online interactions in modern life, the cyberthreat is a top security threat to individuals and the nation. So, how is that frantic SIGO doing anyway, with his efforts to make the funky thing work properly?

Lt. Col. D. Bruce Roeder, U.S. Army, Retired, is an instructor at the Department of Distance Education at the U.S. Army Command and General Staff College at Fort Leavenworth, Kan. He is a graduate of the United States Military Academy and has an M.A. from Webster University. Lt. Col. Roeder previously served in a variety of provost marshal, security, and operations assignments.

Well, let's take a look at the difficult situation our SIGO faces. First, in simple terms, three typical kinds of cyberattackers pose a threat: criminals, ideologues, and nation states. Usually, professional criminals are motivated by greed. They fall under the jurisdiction of law enforcement although the technology they use tends to be beyond the capabilities of ordinary police agencies. Next are the ideologues and so-called "hacktivists," such as WikiLeaks or Anonymous, who generally are motivated by their political or philosophical worldview, or perhaps by cynicism. They often announce their targets and, sometimes, conduct attacks merely to gain attention or to get a laugh. The law treats them as criminals, too. The third type is nation states, which usually are motivated by security, economic, or other interests. They can plan and execute coordinated cyberattacks against their enemies. Normally, they have access to more resources than criminals and ideologues. It is not always easy to assign cyberattackers to neat categories, however. Further muddying the water is the open question of whether a cyberattack is a use of force.

Moreover, determining which specific cyberthreats are most dangerous to U.S. national security and which are most likely to do damage is difficult. Specific cyberthreats arise in unexpected ways. For example, Stuxnet, the fiendishly destructive malware that targeted centrifuges at the uranium enrichment facility in Natanz, Iran, now poses a threat well beyond its original purpose. This is because code used to build Stuxnet (discovered in 2010 and widely considered a state-sponsored cyberattack) was leaked inadvertently onto the Internet. Some analysts believe its descendants (such as Duqu and Flame) or their progeny could already be residing in the databases of critical infrastructure worldwide.³ The bad things going on are beyond any SIGO's skill set or resources. How should we respond at this point?

More Bureaucracy?

The typical, and even mandatory, response of government is to give an office or agency the responsibility and resources to fix a problem. This predictable, slow, and top-down approach to problem solving at the national level is ineffective against an uncertain, fast-changing, and bottom-up problem. For example, the Department of Defense established

United States Cyber Command (USCYBERCOM), a subunified command subordinate to United States Strategic Command. The service components are duly organized to provide support. The Army has the U.S. Army Cyber Command, the Navy has the U.S. Fleet Cyber Command, the Air Force has the Twenty-Fourth Air Force (Air Forces Cyber), and the Marine Corps has the Marine Forces Cyber Command. However, as capable as these units are, they focus mainly on the cybersecurity threats to U.S. defense information networks. On the other hand, "the government is often unaware of malicious activity targeting our critical infrastructure," said Gen. Keith Alexander, former head of the National Security Agency and USCYBERCOM.⁴

When it comes to the civil sector, U.S. Congressman Mike Rogers of Michigan says that "today, we are in a stealthy cyberwar ... and we're losing."⁵ However, there is no doubt U.S. business leaders realize the cyberthreat is real and that it would behoove them to work closely with the government to prevent a big attack or be ready to respond to one effectively. To them, if something affects their profits, it is important. Even so, companies currently have little incentive to alert federal officials after being hacked because the feds will then turn around and share that information with their competitors. Moreover, if businesses share certain information with some of their competitors, they risk prosecution from the government under antitrust laws. Therefore,



unless corporations have some protection from liability or losing their competitive edge, they are unlikely to work together voluntarily. Legal protections need to be codified by Congress, but Congress has not passed any cybersecurity legislation since 2002. On 12 February 2013, President Obama issued an executive order named “Improving Critical Infrastructure Cybersecurity” as a stopgap measure to shield businesses from antitrust litigation if they voluntarily share data with their competitors.⁶ Even when Congress does act, participation will almost certainly remain voluntary on the part of the civilian-owned economic infrastructure.

The care and feeding of the government cybersecurity apparatus (including affiliated contractors) will almost certainly enable us to gain and maintain contact with the cyberthreat, but that apparatus will unlikely be able to seize the initiative from the enemy. It appears that we are coming at the problem like a bull in a china shop. Solving the problem will require something more.

The defining characteristic of the World Wide Web is that it is worldwide; the very strength of

the Internet is its international character. That is precisely the feature that allows hacktivists, cybercriminals, and their money to flit quickly and easily from country to country as their websites are painstakingly identified and shut down. It is crucial for an effective cybersecurity effort to have the same ability to cross international jurisdictions. Agencies must be able to coordinate with similar agencies across the globe just as nimbly as the criminals can. The United Nations Interregional Crime and Justice Research Institute (UNICRI) website offers insights about how such an operational approach might be able to work.⁷ Although UNICRI is a small and underfunded agency within the United Nations, this organization is, at least, looking in the right direction.

Hire the Hackers?

Journalist Misha Glenny has interviewed several cybercriminals. He has not only found that the institutions tasked with keeping us safe from cybercrime do a poor job of deterring, finding, and investigating cases, but also that they might



Cadet 4th Class Anthony Canino, left, and Cadet 2nd Class Matthew Toussain discuss network defenses during a National Collegiate Cyber Defense “At Large” regional competition at the Air Force Academy, 6 March 2011. (courtesy photo/Jeff Scaparra)

be driving back the key to a solution.⁸ Glenny's assessment is that we have a surplus of technology being thrown at the problem but a shortage of human intelligence. While we continue to pour billions of dollars into ubertechnological solutions to cybersecurity, he proposes instead that we look at the characteristics and abilities of the hackers at the center of the problem. While the hacker is only one piece of the overall cybersecurity threat, this piece may be the most vulnerable. Many figures in the business of hacking are not Mafiosi craving the high life, but shy, socially awkward math geniuses who, in his view, are prone to being swayed by sponsors more sophisticated than they are. Glenny presents some facts regarding several recent well-known cybercriminals, including Scotsman Gary McKinnon, Ukrainian Dimitry Golubov, Sri Lankan Renukanth Subramaniam, American Max Vision, Nigerian Adewale Taiwo, and Turk Cagatay Evyapan. He describes some common qualities they and many other hackers share. These include advanced math and science abilities along with advanced computer hacking skills developed during their childhood and early teen years, before their moral compasses were formed. He also, interestingly, points out characteristics consistent with Asperger's Syndrome, a mild form of autism, as well as its attendant depression. These disabilities in the real world often seem to accompany amazing skills in the virtual world of computer hacking. By choosing to prosecute and punish rather than attract and hire these savants, the United States is punishing and alienating its best chance of finding and fixing the problems that vex it, or so the argument goes. Glenny makes a compelling case that, sometimes, we should consider hiring them instead—as our adversaries do. China, Russia, and other countries, he asserts, recruit and employ these gifted people before and after their involvement in cybercrimes. These countries mobilize them to work for the state, while we continue to rely on our criminal justice system to investigate and punish them.⁹

Have a Back-up Plan?

Long-time computer engineer Danny Hillis warned early in 2013 that while we spend a great deal of energy and attention focused on protecting the computers on the Internet, we give little



Staff Sgt. Kenneth Tecala, an aviation operations sergeant, and Chief Warrant Officer 2 Ben Carmichael, command and control system integrator, both with Air Defense Artillery Management, Brigade Aviation Element, Headquarters and Headquarters Company, 2nd Brigade Combat Team, 1st Armored Division, troubleshoot the Rocket, Artillery and Mortar Warning system during Network Integration Evaluation 13.1 at McGregor Range, N.M., 13 November 2012. (U.S. Army, Sgt. Candice Harrison)

thought to the security of the Internet itself as a medium.¹⁰ Hillis considers the Internet an emergent system. He says we do not fully understand it, like the weather and the economy: “it’s changing so quickly that even the experts don’t know exactly what’s going on.”¹¹ He says that because of how the Internet has expanded, we do not even know how an effective denial-of-service attack would affect us, so we need “a plan B.”¹²

The good news is that a backup system consisting of a basic plan for alternate ways essential services can continue communicating and functioning should be relatively easy to design, according to Hillis.¹³ Although he does not offer details on how

it might work, cybersecurity planners who were around during the Y2K scare (referring to the anticipated damaging effects of the millennium bug) could dust off their old plan. That would provide a decent start. The backup plans would vary according to the sector of infrastructure involved. Having continuity plans independent of computer-based operations, and exercised and updated regularly, can provide a safeguard should the worst happen. The plans can also be vehicles for creative problem solving in an organization. The resiliency mindset at the core of the Army's recent efforts to improve comprehensive soldier fitness can be applied to our national critical infrastructure as well as to our personal mental health. Developing well-balanced, robust, and confident key infrastructure sectors whose resilience and total well-being enable them to thrive in an era of high information exchange and persistent threat is not too hard to do. In fact, it is a worthy goal within our reach.

Late to the Party Indeed

Whether we can avoid a catastrophic cyberattack, or for how long, remains uncertain. Given the nature of the threat, the omnipresence and

vulnerability of the Internet and our computers, and the limited resources of the "good guys," our chance of success may seem slim. Yet, those of us in the government and the military have been aware of cybersecurity issues for a long time. We conduct mandatory online annual training to demonstrate our knowledge of computer and information security. In fact, to military people, those sessions sometimes feel like the old SIGO is getting revenge for all those dinings-in from days gone by. Therefore, we can approach cybersecurity expecting that military personnel will be receptive to anticipating and overcoming the challenges of readiness, if not well prepared to respond to a cybersecurity crisis. The 2013 report from the director of national intelligence was an important milestone and clarion call (the 2014 update still lists cyberthreats first). Just as physical security is an inherent responsibility and not solely the job of the provost marshal, so too cybersecurity is not the wire-head's lane; it is all of ours. For anyone who has mistakenly filed cybersecurity into the SIGO's inbox, you should call your office. The podium is ours, and the SIGO is each of us. **MR**

NOTES

1. Director of National Intelligence James R. Clapper, statement for the record to the Senate Select Committee on Intelligence, *Worldwide Threat Assessment of the US Intelligence Community* (12 March 2013), <<https://www.hsdl.org/?view&did=732599>>.

2. Mikko H. Hypponen, *Three Types of Online Attack* (November 2011), video online at Technology, Entertainment, and Design (TED) website, <http://www.ted.com/talks/mikko_hypponen_three_types_of_online_attack.html>.

3. Ralph Langner, *Cracking Stuxnet, a 21st-century Cyber Weapon* (February 2011), video online at Technology, Entertainment, and Design (TED) website, <http://www.ted.com/talks/ralph_langner_cracking_stuxnet_a_21st_century_cyberweapon>; Kaspersky Lab website, Resource 207: *Kaspersky Lab Research Proves that Stuxnet and Flame Developers are Connected* (11 June 2012), <http://www.kaspersky.com/about/news/virus/2012/Resource_207_Kaspersky_Lab_Research_Proves_that_Stuxnet_and_Flame_Developers_are_Connected>.

4. Ann Flaherty, "Feds Roll Out Cyber Plan as Hill Vows Legislation," Associated Press, *The Big Story* (13 February 2013), <<http://bigstory.ap.org/article/white-house-revealing-obamas-cybersecurity-plan>>.

5. Mike Rogers, "America is Losing the Cyber War vs. China," originally in

Detroit News, 8 February 2013, reproduced online by Congressman Mike Rogers, <<http://mikerogers.house.gov/news/documentsingle.aspx?DocumentID=319502>>.

6. President, Executive Order no. 13636, "Improving Critical Infrastructure Cybersecurity," *Federal Register* (12 February 2013), <<https://www.federalregister.gov/articles/2013/02/19/2013-03915/improving-critical-infrastructure-cybersecurity>>.

7. United Nations Interregional Crime and Justice Research Institute website, About UNICRI, <<http://web2012.unicri.it/institute/>>.

8. Misha Glenny, *Darkmarket: How Hackers Became the New Mafia* (New York: Vintage Books, 2012), 271.

9. *Ibid.*, 269.

10. Danny Hillis, *The Internet Could Crash. We need a Plan B* (February 2013), video online at Technology, Entertainment, and Design (TED) website, <http://www.ted.com/talks/danny_hillis_the_internet_could_crash_we_need_a_plan_b.html>.

11. *Ibid.*

12. *Ibid.*

13. *Ibid.*

Network-Centric Warfare and the Data-Information-Knowledge-Wisdom Hierarchy

Col. Harry D. Tunnell IV, U.S. Army, Retired

EACH TIME PEOPLE use smartphone apps, they are creating a form of digital information unknown to most soldiers less than a decade ago. Today, people produce so much digital information at such a rapid rate that it is physically impossible to store all of it.¹ In 2010 alone, consumers stored more than six exabytes of new data on personal computers (PCs) and other devices—this is 24,000 times the amount of information stored in the Library of Congress.² “Big data” are produced somewhere every day, and volumes of data are characteristic of modern combat operations. Soldiers must become experts with systems that manage, manipulate, transform, and analyze data. In the 21st century, tactically relevant information is produced, monitored, and shared in the digital space; commanders must learn to take advantage of data if they are to exercise mission command effectively.

Col. Harry D. Tunnell IV, U.S. Army, Retired, is principal at InRef, LLC, a new media consultancy, and a Ph.D. student in informatics at the Indiana University School of Informatics & Computing. He is a West Point graduate and holds an M.S. in information systems from the University of Maryland Baltimore County. Col. Tunnell's research interests are network-centric warfare theory, military informatics, and secondary user experiences. He has served in combat in Panama, Iraq, and Afghanistan. Col. Tunnell is the sole inventor on two U.S. patents, has written two books for the Army, and has seven vendor and vendor-neutral information technology certifications.



The Department of Defense (DOD) concept for network-centric warfare theory predates the 9/11 terrorist attacks that immersed our nation in its longest war.³ Before the war, network-centric warfare theory was an important transformational concept, and Congress was briefed about its implementation within DOD. However, the theory was not adopted as the basis for operational doctrine. Rather than emphasizing U.S. advances in technology, doctrine has used European colonial experiences as the underpinnings for the war's counterinsurgency (COIN) doctrine.⁴ This represents a missed opportunity.

Network-centric warfare theory is different from other doctrinal frameworks because of how it takes advantage of technological capabilities available only to U.S. forces. The U.S. government has an advantage because other countries simply cannot afford the high level of information technology (IT) investments needed to support network-centric operations. The U.S. government is the largest single purchaser of IT in the world, and out of an approximately \$75 billion expenditure in 2011, DOD consumed about half.⁵ Network-centric warfare theory promotes myriad technologies that allow U.S. military forces to gain information superiority over an adversary and apply combat power decisively through improved decision making; the networked capability enables these benefits.⁶ The IT for such operations is increasingly available in Army formations.⁷ The level of IT investment the U.S. government already makes for DOD enables information superiority; therefore, it is unlikely an adversary could counter the advantage gained through network-centric operations. Because neither adversaries nor allies and coalition partners make comparable IT investments, network-centric warfare theory would allow DOD to take advantage of an exclusively U.S. capability.

The U.S. military must overcome resistance to network-centric warfare theory so it can take advantage of its huge IT investments to win wars. Three factors can explain this resistance. First, while adequate individual IT components have been available for more than a decade, only recently have they been integrated sufficiently to create a useful information system (IS) for Army small-unit planning and tactical command and control. (The IS capabilities of other services are beyond the scope of this paper.)

Second, analysis of training with digital systems shows that there has not been an accompanying shift in doctrine and work practice (e.g., standard operating procedures) meaningful enough to take full advantage of advances in IT.⁸ Based on such reports, one can conclude that 21st-century Army doctrine and work practice remain rooted in the work practice developed for the manual processes, analog equipment, and older digital technologies that contemporary systems have replaced.⁹ Consequently, commanders in the field are often using archaic techniques with a cutting-edge IS. Third,

The level of IT investment the U.S. government already makes for DOD enables information superiority...

many analysts believe the cultural change needed for acceptance of network-centric warfare theory is overdue.¹⁰

This paper describes how to integrate a “data-information-knowledge-wisdom” (DIKW) hierarchy into a network-centric-capable IS framework. The hierarchy can help commanders understand how to interact with data in order to convert it into something useful for decision making in combat.

Background of the Network-Centric Warfare Concept

Network-centric operations were considered so essential to DOD transformation before 9/11 that the U.S. Congress, in Public Law 106-398, required the Department of Defense to report on the implementation of the concept.¹¹ The object of network-centric operations is to take advantage of advances in IT so leaders can improve their speed of command to act decisively against an enemy.¹² A RAND Corporation case study compared the performance of an Army Stryker brigade combat team (BCT), which is a digitally equipped, networked infantry unit, and a non-digital, non-networked U.S. Army light infantry BCT in a training scenario.¹³ The case study showed that speed of command for the networked

commander was about 3 hours, versus 24 hours for the non-networked commander. The accurate identification of friendly, neutral, and enemy forces was approximately 60 percent better with networking. The networked formation had a 1:1 (friendly:enemy) casualty ratio, while the non-networked force suffered a 10:1 casualty ratio.¹⁴

Information system theory and Army mission command doctrine describe how an IS does not operate independently of people.¹⁵ An IS consists of equipment that collects, processes, stores, displays, and disseminates information.¹⁶ People use policies, procedures, and communications as they manage and process data to enhance decision making with automation. Network-centric warfare theory frames decision making in terms of four domains of conflict: physical, information, cognitive, and social.¹⁷

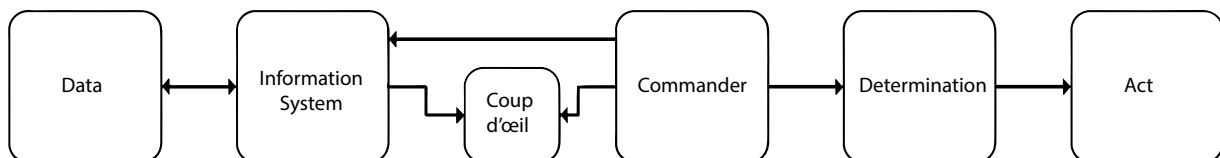
The DIKW hierarchy is a knowledge management structure that helps people make data become meaningful for decision making. The elements of the DIKW hierarchy are—

- *Data*: raw, frequently unstructured items apart from context or interpretation.¹⁸ Data are the first link between an IS and the DIKW hierarchy. People use an IS to interact with the data.
- *Information*: data that have been transformed to have meaning for human beings by being organized with specific relationships between the data.¹⁹ Information adds value to a person's understanding about something.²⁰ People use an IS to perform this transformation.
- *Knowledge*: information that is transformed so it has patterns and repeatable processes.²¹

It is independently useful for decision making. People use an IS to perform this transformation.

- *Wisdom*: the application of intuition to accumulated knowledge applied in a visionary or anticipatory manner.²² People do not use an IS to create wisdom. Rather, they review knowledge discerned through data-information-knowledge transformations and apply personal intuition to create wisdom.

A 19th-century seminal work on military theory, *On War*, provides the elements that military commanders can use to bind an IS, people, and the DIKW hierarchy together for network-centric operations. The elements are *coup d'œil* and determination. Coup d'œil is the ability of a military commander to quickly make sense of battlefield activity and come to a tactically sound conclusion.²³ Being determined, or resolute, is the courage to accept responsibility and act once a decision is made.²⁴ Clausewitz's concept for coup d'œil fits well with the framework for creating wisdom; it provides the context for a military-specific type of intuition. In addition, Clausewitz's notion that determination balances coup d'œil by providing the courage to act captures the culminating act of decision making supported by an IS. Coup d'œil and determination together link the DIKW hierarchy to competent, informed tactical decisions in battle and the leader's will to act. The figure illustrates the relationship between a commander, coup d'œil, and an IS in the DIKW hierarchy. The transformations from data to information and from information to knowledge occur with use of the IS. The transformation from knowledge to wisdom only occurs when a commander



Relationship Between a Commander, Coup d'œil, and an Information System

has a well-formed, mature coup d'œil to apply to knowledge during operations.

There is an important note of caution. Coup d'œil and determination work together. It is relatively easy using a modern IS to develop situational awareness, but it is much harder to act, particularly when potential consequences of poor decisions include censure from others or injury and death within the command or to the commander. Clausewitz recognized that competence and the ability to be resolute decrease in some leaders based on the duration and frequency of the leader's exposure to danger.²⁵ This perspective illustrates the need for caution when advocating for "flattening" decision making.²⁶ Flattening (reducing middle layers of a hierarchy and giving more autonomy to skilled individuals) is not always wise or possible in a networked environment because the authority to decide or act at certain echelons might be restricted (by law, policy, or other constraints). Furthermore, subordinates may wish to defer decisions to a higher headquarters for a variety of reasons. Finally, ease of analysis is not equivalent to experience when it comes to decision making. Just because technology enhances analysis does not mean it improves coup d'œil—a second lieutenant is still an inexperienced leader regardless of the technology used.

The consequence of poorly developed coup d'œil, as applied to the DIKW hierarchy, can be catastrophic if a commander's poor decision (or indecision) affords the enemy an advantage. Even leaders using the DIKW hierarchy could make errors and poor decisions: as Jay H. Bernstein writes, "folly proceeds from error and exacerbates it."²⁷ Folly and error can come from overreliance on technology. Networks permit flattening an organization; in business, many consider flattening an organization desirable. However, overreliance on technology can increase opportunities for folly to manifest by increasing the number of people making decisions, especially in military organizations. Commanders should avoid *technology-centric* organizational designs based on the capability and performance of hardware and software. They should avoid decentralizing decision making simply because the technology makes it possible. *Network-centric* operations are human-centered. Network-centered warfare theory provides a framework for military leaders to take full advantage of technology. In this human-centered

theory, the success or failure of operations is based on the quality of a commander's action rather than the capabilities of technology.

Intuition, a type of domain knowledge that serves as a personal repository of historical information for decision making, is developed through experience and practice.²⁸ Coup d'œil is a military-specific form of intuition initially formed through training, but it requires close combat experience to reach full maturity. Moreover, intuition has an important place in the design of technological systems. In intelligent systems research, the notion of "sensemaking" includes a goal of designing systems that allows people to access the intuition of other people.²⁹ Sensemaking is an element of the social domain within network-centric warfare theory.³⁰

Computing and Command and Control

A small number of soldiers in ground combat maneuver units have used PCs on a day-to-day basis since the 1980s. Early PCs typically were found in the operations section and were used for office productivity tasks such as writing orders, preparing presentations, or planning troop movements. They were not networked or employed collaboratively. Tactical command and control were exercised according to an established hierarchy with little lateral situational awareness; they were exercised largely through analog voice communication or personal presence.³¹ If information was exchanged with another unit, it was often done via analog voice communication or the physical exchange of map overlays and other materials. In addition, specialized items of digital technology, such as artillery computers, were in use before 1990.

As PCs became increasingly common in the military workplace, concepts for digitizing U.S. Army formations were also evolving. By the 1990 Gulf War, Army tactical units communicated using packet-switched mobile networks that provided secure voice, facsimile, and computer communication services.³² Today, the Army uses the Army Battle Command System (ABCS) to support command and control. ABCS is a digital system intended to integrate other battle management systems into a comprehensive tactical digital architecture.³³ The system normally is associated with battalion and brigade level; however, components are used at other levels. An example is



The 29th Combat Aviation Brigade deployed its Army Battlefield Command System to Bethany Beach, Del., for annual training, 13-27 May 2010. ABCS is a digital system of networked components that gives commanders a better perspective of their operating environment, assets, resources, and strengths. (U.S. National Guard, Sgt. Thaddeus Harrington)

Force XXI Battle Command Brigade and Below (FBCB2), a ruggedized, PC-size computer that displays the common operational picture, provides position location information, is capable of text communication, and operates on the lower tactical Internet (small unit, terrestrial line-of-sight) and upper tactical Internet (battalion and higher, satellite).³⁴

Not all components of ABCS technology are recent developments. For example, FBCB2 predates 9/11. Furthermore, not all elements of ABCS were designed to work together. The battle management systems used by different staff sections, for instance, were developed independently.³⁵ They were integrated into one IS to support command and control over a period of years. Because of this integration, commanders have had many opportunities to employ formations according to network-centric warfare theory. Unfortunately, one of the shortfalls of ABCS implementation is that institutional and unit training are inadequate. Units frequently rely on contractors for training, limiting the manner in which these digital systems are incorporated into training.³⁶ These practices are indicative of Army-wide technology resistance.³⁷

The difference in capability between legacy command and control tools and a modern tactical IS such as ABCS is enormous. When network-centric warfare theory first was envisioned, the needed command and control systems for Army formations had not been created. Today, the evolution and integration of network-centric capabilities makes it possible to implement network-centric operations. Unfortunately, the intellectual effort necessary to use information-age military tools effectively did not keep up. After 9/11, less offensively oriented military approaches gained ascendancy, and a lack of decisive operations was claimed to characterize modern war. The indecisive nature of operations resulted from a *falsely assumed lack* of information superiority that became a common theme of COIN.³⁸ Because the Army never adopted network-centric warfare theory for conducting operations, it does not have an adequate doctrinal framework to use the superb IT capabilities that reside within every tactical formation.

Network-centric warfare theory is sometimes derided because it is seen as placing too much emphasis on technology, or it is considered unsuitable for COIN and counterterrorism operations.³⁹ This thinking misses the mark. Network-centric

warfare theory is designed to change the perspective about the military use of IT from a platform-centric focus, in which an item of equipment is the center-piece, to a network-centric focus based on the four domains of conflict.⁴⁰ The theory can be applied to any type of military operation—offense, defense, or stability. Furthermore, the idea of network-centric warfare should not be confused with improved speed of command due to better technology, which is a platform-centric notion.

The Army continues to focus on individual equipment as it attempts to digitize operations by introducing more digital technology components rather than unifying how leaders think and fight in the digital space.⁴¹ This leads to capabilities being overlooked. Military technology has advanced to the point that information superiority has been possible for some time.

Some military organizations already have devised means to achieve seamless interservice integration between their combat capabilities. For example, some Army and Air Force units in Afghanistan have integrated their systems (the Army's ABCS, Air Force aircraft systems, and unmanned aerial systems [UASs]) so that pilots and infantrymen can have almost perfect awareness of each other's positions before a fighter aircraft arrives on station.⁴² The technology enables leaders to make faster and more informed assessments of the environment before applying coup d'œil and determination. Unfortunately, few leaders recognize the potential that such capability affords soldiers so it remains underutilized.⁴³

Applied Network-Centric Warfare Theory

Two vignettes from my experience in Afghanistan during 2009 demonstrate the application of network-centric warfare theory.

Vignette 1. Task Force (TF) Stryker, a Stryker BCT, had recently arrived in Afghanistan and started conducting operations in early August 2009. During the first major offensive mission, TF Stryker elements observed a group of Taliban mining a road at approximately 1900 hours on 1 September 2009 and attacked them with aerial munitions from a UAS.⁴⁴ The TF Stryker command group, consisting of the commander and assault command post personnel from the brigade

battle staff, were forward at a small combat outpost. The command group observed the attack and commanded follow-on operations from the outpost. The enemy, after the attack, evacuated casualties to an intermediate point, massed additional personnel, and continued to evacuate the most seriously injured to an outpost—a Canadian-advised Afghan police element across the river and outside TF Stryker's area of operations, which provided the highest-quality medical care available. The wounded Taliban were identified by 2100 hours, and the Afghan National Security Forces assumed responsibility for their medical care.⁴⁵

Analysis of vignette 1. The command group relied on a variety of computing devices and multimedia data streams to observe enemy tactics, techniques, and procedures (TTPs) in real time. The command group's equipment included video, Internet chat, radio (digital) voice communication, VoIP (voice over Internet protocol), laptop PCs, position location data, FBCB2, and Land Warrior (a ruggedized wearable computer for infantrymen).⁴⁶ Because the command group was located with a Canadian-advised Afghan company, the Canadian advisors provided accurate, timely information from Afghan army and police units. All of these factors contributed to the successful identification and detention of the enemy.

Several enemy TTPs were revealed as a result of the data collected (and transformed into information and knowledge) throughout August 2009 and into September. In fact, by the beginning of September 2009, the IS in TF Stryker had contributed more relevant information about enemy TTPs to BCT-level domain knowledge than combat certification training conducted before the deployment. The data, information, and knowledge discerned during these initial operations would manifest as coup d'œil during subsequent engagements with the enemy. One of the key enemy TTPs the command group now understood was enemy casualty evacuation.

Vignette 2. At approximately 1930 hours on 23 September 2009, intelligence reporting to the TF Stryker command group (located in the tactical operations center) indicated that a Taliban formation was in the TF Stryker area; a retasked UAS found the enemy group, and their location

was disseminated to the battalion operating in the area.⁴⁷ The enemy was attacked using Army aviation. Because the command group already understood enemy casualty evacuation TTPs, the battle staff was ordered to perform an immediate analysis of how and where the enemy would evacuate their casualties.

The understanding that developed during earlier operations was used to turn the ongoing data-information-knowledge transformations of this engagement into wisdom. Through coup d'œil, the command group understood the enemy would seek out high-quality medical facilities and evacuate casualties quickly over good routes. Enemy casualties were subsequently identified because IS use was guided by this refined coup d'œil.

Analysis of vignette 2. Several months before deploying to Afghanistan, the geospatial engineer section of the battle staff collected data about the terrain and infrastructure of the anticipated area of operations. The data were refined and updated during the first 50 days of combat. After the aerial attack on the enemy, a geographic IS was used to evaluate the data and perform an assessment of where the enemy might evacuate their casualties. Four options were selected; however, they were all outside the TF Stryker area of operations. After approval by the TF Stryker commander, the staff communicated the options via email to TF Stryker liaisons with other coalition units. By midnight, Afghan police, dispatched based on the predictive analysis, identified six wounded enemy fighters at the first predicted location and agreed to take responsibility for them.⁴⁸

Summary of vignettes. Forces seldom find enemy personnel after evacuation from the battlefield because they seldom get feedback about the enemy evacuation channel in time to act. Typically,

reports about enemy casualties come through intelligence reporting days, weeks, or months after the event—if ever. A network-centric warfare framework integrated with the DIKW hierarchy and coup d'œil improved decision making during combat based on the BCT's IS output. The integration enabled TF Stryker data and information transformations across the operational area, leading to knowledge that resulted in enemy detention (vignette 1). The framework also enabled accurate prediction because of transformations from knowledge to wisdom, guided by a honed coup d'œil, that the force acted upon in minutes (vignette 2). These experiences demonstrate that the predictive planning and preemption, integrated force management, and execution of time-critical missions envisioned by network-centric warfare theorists are possible.⁴⁹

Conclusion

The framework provided for network-centric warfare theory integrates people, the IS, and traditional military theory. Army forces already have applied such a framework innovatively during real-world infantry combat operations in Afghanistan. Technically competent, courageous, and well-trained soldiers remain important for the successful implementation of network-centric warfare theory. Technology cannot replace the essential and historically significant aspects of traditional military leadership. The integration of network-centric warfare theory with the DIKW hierarchy, coup d'œil, and determination provides soldiers with unparalleled opportunities for knowledge discovery and action in an information-rich environment. This enhances human decision making in the intense, uncertain environment of close combat. **MR**

NOTES

1. James Manyika, Michael Chui, Brad Brown, Jacques Bughin, Richard Dobbs, Charles Roxburgh, and Angela Hung Byers, "Big Data: The Next Frontier for Innovation, Competition, and Productivity" (McKinsey Global Institute, May 2011), 3-4, <http://www.mckinsey.com/insights/business_technology/big_data_the_next_frontier_for_innovation>.

2. Ibid., 3.

3. Arthur K. Cebrowski and John J. Garstka, "Network-Centric Warfare: Its Origin and Future," *Proceedings* 124, no. 1139 (1998), <<http://www.usni.org/magazines/proceedings/1998-01/network-centric-warfare-its-origin-and-future>>; Department of Defense (DOD), *Report on Network Centric Warfare Sense of the Report*, Arthur L. Money (March 2001), 8, <http://www.dodccrp.org/files/ncw_report/report/ncw_sense.pdf>.

4. Raymond J. Curts and Joseph P. Frizzell, "Implementing Network-Centric

Command and Control," report for the *10th International Command and Control Research and Technology Symposium: The Future of C2* (17 March 2005): 4, 16-18, 20-21; John Nagl, "Learning and Adapting to Win," *Joint Force Quarterly* 3rd Quarter, no. 58 (2010): 123-24.

5. CIO [U.S. Chief Information Officer] Council, "A year in Review: Outcomes and Lessons Learned from Implementing Agency-Led TechStat Reviews Across the Federal Government" (Washington, DC: U.S. Government Printing Office [GPO], 8 December 2011), 10; Report of U.S. Chief Information Officer on federal information technology budgets, Steven VanRoekel, "Federal Information Technology FY 2013 Budget Priorities: 'Doing More With Less'" (Washington, DC: GPO, 2012), 4-6.

6. DOD, Office of Force Transformation, *The Implementation of Network-Centric Warfare* (Washington, DC: GPO, 2005): 8; Ang Yang, "Understanding Network Centric Warfare," *Bulletin of the American Schools of Oriental Research [BASOR]* 23(4)(2004): 2-3.

7. Clay Wilson, *Network Centric Operations: Background and Oversight Issues for Congress* (Washington, DC: Congressional Research Service, 2007): 5, 23-26, and 37.
8. Darrell Collins, "Enabling Army Digital Organizations" (Kandahar, Afghanistan: 5/2/ID (SBCT), forthcoming research paper), 5-7; Gregory A. Goodwin and David R. James, *Decision Making With Digital Systems* (Arlington, VA: U.S. Army Research Institute for the Behavioral and Social Sciences, 2009).
9. Ibid.
10. Curtis and Frizzell; Thomas P.M. Barnett, "The Seven Deadly Sins of Network-Centric Warfare," *Proceedings* 125, no. 1151 (1999), <<http://www.usni.org/magazines/proceedings/1999-01/seven-deadly-sins-network-centric-warfare>>; David S. Alberts and Richard E. Hayes, *Power to the Edge: Command ... Control ... in the Information Age* (Washington, DC: Command and Control Research Program, 2003), 58; Collins, 6-7.
11. Money, 1; DOD, *Network Centric Warfare: Department of Defense Report to Congress* (27 July 2001), 1-1. <http://www.dodccrp.org/files/ncw_report/report/ncw_main.pdf>.
12. Cebrowski and Garstka.
13. Daniel Gonzales, Michael Johnson, Jimmie McEver, Dennis Leedom, Gina Kingston, Michael S. Tseng, report prepared for the Office of Force Transformation in the Office of the Secretary of Defense, *Network-Centric Operations Case Study: The Stryker Brigade Combat Team* (Santa Monica, CA: RAND Corporation, 2005), 61-99.
14. Ibid., 105.
15. N. Au, Eric W.T. Ngai, T.C.E. Cheng, "Extending the Understanding of End User Information Systems Satisfaction Formation: An Equitable Needs Fulfillment Model Approach," *MIS [Management Information Systems] Quarterly* 32, no. 1 (2008): 44; Army Doctrine Reference Publication (ADRP) 6-0 (Washington, DC: GPO, 17 May 2012), 2-7 to 2-9.
16. ADRP 6-0, 3-10.
17. Office of Force Transformation, 19-20.
18. Jennifer Rowley, "The Wisdom Hierarchy: Representations of the DIKW Hierarchy," *Journal of Information Science* 33, no. 2 (2007): 170-71; Jay F. Nunamaker Jr., Nicholas C. Romano, and Robert Owen Briggs, "A Framework for Collaboration and Knowledge Management," paper presented at the 34th Hawaii International Conference on Systems Sciences (2001), 3; V. Chiew, "A Software Engineering Cognitive Knowledge Discovery Framework," paper published in *Proceedings: First IEEE [Institute of Electrical and Electronics Engineers] International Conference on Cognitive Informatics, ICCI 2002* (2002): 1.
19. Nunamaker, Romano, and Briggs: 3; Chiew, 1; JP 1-02, 160.
20. Rowley, 171-72.
21. Nunamaker, Romano, and Briggs, 3.
22. Rowley, 174; Nunamaker, Romano, and Briggs, 3.
23. Carl von Clausewitz, *On War*, trans. Michael Howard and Peter Paret (Princeton, NJ: Princeton University Press, 1989), 102-103.
24. Ibid., 141-42.
25. Ibid., 103.
26. Alberts and Hayes, 153, 76; Nathan Minami and Donna Rhodes, "Network Centric Operations and the Brigade Unit of Action," paper presented at the 2007 International Conference of the System Dynamic Society and 50th Anniversary Celebration, Boston, MA (2007), 11, 13.
27. Jay H. Bernstein, "The Data-Information-Knowledge-Wisdom Hierarchy and its Antithesis," paper presented at the 2nd North American Symposium on Knowledge Organization, Syracuse University, NY (18-19 June, 2009), 73.
28. Gu Jiajun and Xie Fenghua, "The Empirical Research on the Domain Knowledge Factors Influencing the Effectiveness of Intuition in Decision Making," paper presented at the Second International Symposium on Knowledge Acquisition and Modeling (30 November-1 December 2009), 299; Robert L. Glass, "Intuition's Role in Decision Making," *Software*, IEEE 25, no. 1 (2008): 95.
29. Gary Klein, Brian Moon, and Robert R. Hoffman, "Making Sense of Sensemaking 1: Alternative Perspectives," *IEEE Intelligent Systems* (2006): 70.
30. Office of Force Transformation, *The Implementation of Network-Centric Warfare*, 20.
31. P.F. Sass and L. Gorr, "Communications for the Digitized Battlefield of the 21st Century," *Communications Magazine*, IEEE 33, no. 10 (1995): 87.
32. Ibid., 91; Paul Sass, "Communications Networks for the Force XXI Digitized Battlefield," *Mobile Networks and Applications* 4 (1999): 140, 42.
33. Minami and Rhodes, 3-4; Gonzales et al., 30-36.
34. This is a generalization of the different tactical Internets for command and control. Small units on an increasingly frequent basis have satellite access, and a higher headquarters can use terrestrial line-of-sight systems; Wilson, 33; Gonzales et al., 65.
35. Gregory A. Goodwin and David R. James, *Decision Making With Digital Systems* (Arlington, VA: U.S. Army Research Institute for the Behavioral and Social Sciences, 2009), 1.
36. Ibid., 18, 23; Brooke B. Schaab, J. Douglas Dressel, and Peter B. Hayes, *Training Requirements of Digital System Operators in a Stryker Brigade Combat Team* (Arlington, VA: U.S. Army Research Institute for the Behavioral and Social Sciences, 2005), vii, 8, 13; Collins, 2, 5-9; *Army Digital Education Survey* (Kandahar, Afghanistan: 5/2 ID [SBCT], forthcoming), 7, 10, 21-22.
37. DongBack Seo, Albert Boonstra, and Marjolein Offenbeek, "Managing IS Adoption in Ambivalent Groups," *Communications of the ACM* 54, no. 11 (2011): 72-73; Rhoda C. Joseph, "Individual Resistance to IT Innovations," *Communications of the ACM* 53, no. 4 (2010): 145.
38. Joint Chiefs of Staff, Joint Staff, *Net-Centric Operational Environment Joint Integrating Concept, Version 1.0* (Washington, DC: GPO, 31 October 2005), D-3; Field Manual 3-24, *Counterinsurgency* (Washington, DC: GPO, 2006), 1-3, 1-4, 5-1 through 5-28; Sean Lawson, "Is Network-Centric Warfare (Finally) Dead? Only Partly" in Sean Lawson ICTs and International Affairs Blog, blog entry posted 14 August 2010, <<http://www.seanlawson.net/?p=772>>.
39. Barnett.
40. Cebrowski and Garstka.
41. A. Borgman, P. Smith, and D. Johnson, "Tools for Enhancing Distributed, Asynchronous Collaboration in Army Operations," paper presented at the IEEE International Conference on Systems, Man, and Cybernetics (October 11-14, 2009), 3530-31.
42. Jared Cox, "Digital Air-Ground Integration, the Future is Here," *Fires* (2010): 16-17; Joseph Turnham et al., "Digital Air/Ground Integration in Afghanistan: The Future of Combat is Here!" *Fires* (2012): 58.
43. Christopher J. Toomey, "Army Digitization: Making it Ready for Prime Time," *Parameters* 33, no. 4 (2004): 43-45.
44. Harry D. Tunnell IV, "Task Force Stryker Network-Centric Operations in Afghanistan," *Defense and Technology Papers* (Washington, DC: Center for Technology and National Security Policy, National Defense University, 2011), 6.
45. Ibid., 7.
46. Ibid., 2-5; Sam Linn, "An assault CP in a Stryker BCT," *Infantry Magazine* (May-August 2010): 24-25.
47. Ibid., 8.
48. Ibid., 9.
49. F. Stein, J. Garska, and P.L. McIndoo, "Network-Centric Warfare: Impact on Army Operations," paper presented at EUROCOMM 2000, Information Systems for Enhanced Public Safety and Security Conference (2000), 291-92.

Is There Room for Peace Studies in a Future-Centered Warfighting Curriculum?

Maj. Thomas G. Matyók, Ph.D., U.S. Army, Retired, and Cathryne L. Schmitz, Ph.D., MSW



A nation that draws too broad a difference between its scholars and its warriors will have its thinking done by cowards, and its fighting done by fools.

—Thucydides

CHANGING POLITICAL, SOCIAL, AND ECONOMIC REALITIES in the United States, as well as the rest of the world, suggest that the Army will need to review how it accomplishes future military-centric missions. In a 2012 article in *Foreign Affairs*, Chief of Staff of the Army Gen. Raymond Odierno argues that today's Army needs to transition in critical areas that affect the size of the force, material, and training.¹ Gen. Odierno also posits that the Army must assume a broader definition of battlefield. Future missions may involve, for instance, assisting victims of natural disasters, restoring order in collapsing or failed states, or confronting nonstate forces. For successful on-the-ground peace development, an expanded skill set is needed. This paper contributes to an emerging narrative about the proper role of conflict transformation and conflict management education within a military context.

Maj. Thomas G. Matyók, Retired, is an associate professor and graduate studies director of the Program in Conflict and Peace Studies at the University of North Carolina at Greensboro. He is currently a visiting research professor at the U.S. Army Peacekeeping and Stability Operations Institute. He holds a B.A. from Montclair State College and master's degrees from Chapman University and the University of Saint Mary. His Ph.D. in conflict analysis and resolution is from Nova Southeastern University.

Dr. Cathryne L. Schmitz is a professor and the director of the Program in Conflict and Peace Studies and a professor in the Department of Social Work at the University of North Carolina at Greensboro. She has an MSW from the University of Washington and a Ph.D. in social work from Ohio State University.

The Field of Peace and Conflict Studies

As an academic field of study, peace and conflict studies is over 50 years old. The field has an active base of scholars, a growing body of disciplinary literature, an established curriculum, and a pedagogical tradition that includes classroom teaching, experiential learning, internships, and international study. Peace and conflict scholars and educators seek to understand the causes of conflict. They examine ways to prevent and transform conflict situations. They seek to build peaceful and just social systems and societies. They achieve these goals by educating specialists and engaging with policymakers and the broader community of governmental and nongovernmental organizations in creating the context for nonviolent conflict management. Peace and conflict studies primarily engages a practice-centered form of scholarship, with academics and students actively involved in numerous forms of fieldwork.

Peace science and peace research are rapidly growing fields of study oriented toward conflict management, peace building, and developing appropriate interventions. Peace and conflict scholars are united not by ideology or political perspective, but by a commitment to understanding the causes of violent conflict and finding effective and sustainable nonviolent solutions to world problems. Peace and conflict studies curricula cover a wide range of issues related to peace, conflict, violence, justice, inequality, social change, and human rights. The field of study and practice is now applied at all levels of conflict from interpersonal to global.² As an emerging field of study and practice, the shape and terminology of the discipline have expanded and transitioned from an amateurish to a professional framework. In fact, many practitioners now believe that conflict is not *resolved*; rather, it is *transformed* as part of a creative process. As a result, *conflict transformation* has moved forward as the core construct shaping the field.³

Formal conflict management as part of a deliberate peace development strategy can be traced to the Kingdom of Mari in 1800 BCE, when kings regularly employed mediation and arbitration to resolve conflicts.⁴ From that time forward, conflict management and conflict resolution have been employed as formal and informal

practices for addressing smaller disputes and broader conflicts.

In fact, peace and conflict studies prepares individuals for a wide variety of careers. Graduates become negotiators, mediators, government officials, educators, business managers, activists, and professionals in organizations focused on human rights, dispute resolution, environmental protection, international law, and human and economic development. Currently, programs are reporting, anecdotally, an increase in the number of military veterans enrolling in peace and conflict studies programs—graduate and undergraduate. Quantifying this trend, however, will require further research.

Contributions of Peace and Conflict Studies to Military Education and Development

Peace and conflict studies should be deliberately integrated into the Army's professional education curriculum at all levels. Peace and conflict studies, as part of professional military education and training, can reduce the size of forces needed by providing conflict transformation and management skills to military and civilian personnel. This can be a force multiplier. In an environment of shrinking resources, peace studies and conflict management training require little in the way of assets.

Gen. Odierno states that today's Army is positioning itself to respond to conflict as a flexible force based on the escalating complexity of contingencies worldwide.⁵ The force must be prepared to meet a range of challenges, including the increasing need for the prevention and management of regional conflicts. Peace and conflict studies is uniquely positioned to contribute to the development of a breadth of responses.⁶

As a continuum of approaches develops, a balanced narrative regarding military intervention is needed. It should include a discussion of policing and community development, with less focus on national security and more on human security and the protection of individuals.⁷ According to the *Human Security Report 2005*, 95 percent of violent conflicts are intrastate. The nature of intrastate conflict implies that military forces need to maintain proficiency in skills other than those used for large-scale, interstate warfighting.⁸

Creating room for peace and conflict studies in military professional development has numerous possibilities, such as the inclusion of military personnel in existing peace and conflict studies programs, and the inclusion of peace and conflict studies curricula within the Army's professional military and civilian education systems. We propose that processes that contribute to building the capacity for meeting human needs complement conflict prevention and management activities. The learning is multidirectional, with military professionals providing another dimension of understanding and critique to peace and conflict studies and its application as part of a broad peace-building and development strategy. In other words, military personnel have much to contribute to the field of peace and conflict studies.

Peace Building and the Military

Some will certainly disagree with our suggestion that there is a proper role for peace and conflict studies in professional military education. Civilians may judge it as a form of "sleeping with the enemy." We think this is a shortsighted view. If war is too serious a business to be left solely to the generals, we argue peace is too important to be left to those without military experience because members of the military can support informed decision making. Creation of a just, sustainable, and lasting peace is everyone's business; certainly, it is the business of those *on the ground*. All those involved in peace *making*, peace *keeping*, and peace *building* should be welcomed to the peace *development* table.

Louis Kreisberg notes that as "the conflict resolution (CR) field has developed, it offers many strategies and methods that are relevant for partisans in a fight as well as for intermediaries seeking to mitigate destructive conflicts."⁹ Conflict resolution, one component of conflict transformation and management, is more than negotiation and mediation. The focus is on responses to conflict that are contextually driven and grounded in theory and practical experience. When we discuss peace, we are talking about the study of conditions that are advancing inclusive, sustainable development within political, economic, and cultural contexts. Conflict management and conflict transformation address activities occurring on the ground that prevent peace from breaking out.

Peace development needs more than good intentions. Far too often, individuals believe their good

intentions alone are all that is required for success in resolving conflict and building peace. Experience proves otherwise. Effective peace development requires the participation of subject matter experts regarding conflict. A just, sustainable, and lasting peace is brought into existence through hard work. Skill mastery and individuals educated in transdisciplinary responses to conflict and violence are essential.

The approach outlined here for integrating peace and conflict studies into Army professional education is premised on a three-tier approach that

Far too often, individuals believe their good intentions alone are all that is required for success in resolving conflict and building peace.

correlates with the strategic, operational, and tactical levels of war. Our definitions here do not mirror exactly those found in Army doctrine; rather, they are used to construct an approach that would complement existing doctrine.

Strategic peace building is grounded in the analysis of conflict. It is heavily weighted toward the understanding and development of the foundation of peace theory. Students follow an interdisciplinary approach to conducting analysis primarily at mega levels of conflict, toward societal and regional peace and peace operations.

Operational peace building encompasses the macro and meso levels and bridges the theoretical aspects of peace building found at the strategic level with tactical approaches to conflict transformation and management. Students at the operational level of practice integrate theory into practical responses to conflict. Theory translates into practice, and feedback from practice refines theory in a constant feedback loop. The focus at the operational level is construction of the institutions and structures of peace such as community justice centers, training programs in conflict transformation and management, and transitional justice activities.

Tactical peace building occurs mainly at the micro level. Tactical peace building includes the interpersonal, grassroots, and community contexts. This is where the rubber meets the road. Students gain hands-on experience in conflict transformation work and peace building. Skills such as mediation, negotiation, group problem solving, restorative practices, community building, and facilitation are major components of a conflict studies curriculum at the tactical level.

The Curriculum

Pursuing just peace connects to the military ethos captured in the United States Military Academy motto, “duty, honor, country.” We suggest a curriculum informed by this ethos. Peace and conflict studies can contribute to a new type of force based on Gen. Odierno’s suggestion that military units, in the near future, may need to be configured based on expertise.¹⁰ We ask, “Why not a unit schooled in conflict management? What might be included in a peace and conflict studies curriculum? What competencies might be addressed?” These questions can inform an expanded dialogue regarding peace building within an evolving military context.

Just policing introduces an approach to conflict transformation and management configured similarly to a methodology employed by the Metropoli-

tan Police Service in London. Unit members rely primarily on conflict resolution skills to confront issues within communities. The word *service* replaces *force* as a way of communicating a new role within a military context. Armed military forces can be held in reserve as a way of contributing to a graduated response to conflict. Gerald W. Schlabach suggests that Reserve Officer Training Corps programs could build closer relationships with justice and peace studies programs and that this collaboration can create “think tanks for transarmament from potentially lethal and military forms of defense to nonviolent civilian-based defense.”¹¹

Language and, perhaps most important, sustained dialogue are key. Developing a common language of peace and conflict studies can contribute to a seamless integration of humanitarian organizations in peace operations. Shared competency in a common language can help break down barriers of mistrust, which sometimes exists between military professionals and humanitarian organizations. Integrating peace and conflict studies into Army professional development can also contribute to an increased competency in working with the nongovernmental humanitarian organizations increasingly present in intrastate conflicts.



U.S. Army 2nd Lt. Paul Knudtson speaks to a Shah Joy village elder during a shura at the Shah Joy District Center in Afghanistan's Zabul Province on 26 January 2011. (Staff Sgt. Brian Ferguson, U.S. Air Force)

Skill Development

Connie Peck notes that knowledge and practice must inform each other, and that conflict resolution and management programs need to be constructed to assist conflict practitioners—not simply to add to theory development.¹² If peace is the desired outcome of any conflict, it must be achieved through conflict transformation and management. Therefore, it is critical to begin a discussion on how peace and conflict studies can be integrated into Army professional development and training by—

- Including peace studies and peace scholarship in the U.S. Army War College curriculum, with the focus of scholarship at the strategic level.
- Focusing on conflict management at the U.S. Army Command and General Staff College.
- Emphasizing conflict transformation skills training at branch qualifying schools and noncommissioned officer academies, with individuals concentrating on grassroots problem solving.

Too often, it is simply assumed that individuals possess the skills necessary to address conflict. In fact, multiple skill sets undergird the process of conflict transformation. Mediation and negotiation, nonviolence, restorative justice, and joint problem solving skills can be integrated into existing military education and training.

Mediation and negotiation. Skills that can be taught under mediation and negotiation include—

- Introduction to mediation and negotiation skills.
- Mediator as process expert.
- Negotiation skills: hard-bargaining and principled negotiation.

Nonviolence. Skills that can be taught under nonviolence include—

- Nonviolence as a peace-building tool.
- Just policing.
- Nonviolent communication.

Restorative justice. Skills that can be taught under restorative justice include—

- Community circles.
- Dialogue groups.

Joint problem solving. Skills that can be taught under joint (referring to all partners) problem solving include—

- Facilitation.
- Large-group problem solving.
- Integration of the curriculum.

Summary

Peace is a charged, contested, and often marginalized term. It can challenge the warrior ethos. However, we find ourselves in a period of significant change, and formal and informal institutions and systems of the past that support negative peace alone need modification to meet new demands. Tomorrow's battlefields still need warriors able to close with and destroy the enemy but also those proficient in conflict prevention, management, and transformation skills. Asymmetrical approaches to conflict management are the new norm.

An increasing focus is needed on preventing conflict.¹³ The desired end state of all military operations should be a durable, lasting, and just peace. Experience suggests that a tension can exist between the military and those in the field of peace and conflict studies. This seems an unnecessary tension. With fewer people having military experience, uninformed opinions regarding military culture are guiding the peace discourse.

Military professionals are often the strongest advocates for peace development and nonviolence. Professional soldiers must not be marginalized and left absent from the peace development table because of peace activist prejudices. Rather, the warrior ethos that embodies mission, selfless service, and physical and mental courage should be embraced. Professional soldiers who view themselves as peace builders can be counted upon to use force only when necessary, and judiciously. **MR**

NOTES

1. Raymond T. Odierno, "The U.S. Army in a Time of Transition: Building a Flexible Force," *Foreign Affairs* 91, no. 3 (2012).

2. Oliver Ramsbotham, Tom Woodhouse, and Hugh Miall, *Contemporary Conflict Resolution*, 2 ed. (San Francisco: Wiley, John & Sons, Inc., 2005).

3. Johannes Botes, "Conflict Transformation: A Debate Over Semantics or a Crucial Shift in the Theory and Practice of Peace and Conflict Studies," *The International Journal of Peace Studies* 8, no. 2 (2003).

4. Jerome T. Barrett, *A History of Alternative Dispute Resolution: The Story of a Political, Cultural, and Social Movement* (San Francisco: Jossey-Bass, 2004).

5. Odierno.

6. Reina C. Neufeldt, "Just Policing and International Order: Is It Possible?" in *Just Policing, Not War: An Alternative Response to World Violence*, ed. G. W. Schlabach (Collegeville, MN: Liturgical Press, 2007).

7. John P. Lederach, "The Doables: Just Policing on the Ground," in *Just*

Policing, Not War.

8. Human Security Center, *Human Security Report 2005: War and Peace in the 21st Century* (British Columbia, Canada: Oxford University Press, 2005), <<http://www.hsrgr.org/human-security-reports/2005/overview.aspx>>.

9. Louis Kreisberg, "Contemporary Conflict Resolution Applications," in *Leashing the Dogs of War*, ed. Chester Crocker (Washington, DC: Institute of Peace, 2001).

10. Odierno.

11. Gerald W. Schlabach, "Practicing for Just Policing," in *Just Policing, Not War*, 104.

12. Connie Peck, "Training as a Means to Build Capacity in Conflict Prevention: The UNITAR Approach," in *Conflict Prevention: From Rhetoric to Reality*, ed. D. Carment and A. Schnabel (Lanham, MD: Lexington Books, 2004).

13. Odierno.

Medical Operations in Counterinsurgency

Joining the Fight

Maj. David S. Kauvar, M.D., U.S. Army; Maj. Tucker A. Drury, M.D., U.S. Air Force

COUNTERINSURGENCY (COIN) CAMPAIGNS generally emphasize nonlethal means more than conventional engagements, but medical units at the battalion and brigade level are deployed in COIN theaters according to conventional doctrine dictating a focus on caring for combat casualties. U.S. military forces have no medical doctrine specific to COIN, and expeditionary health support operations are not mentioned in conventional COIN doctrine. When combat units have primarily engaged primarily in COIN operations in Iraq and Afghanistan, the disconnect between conventional medical support doctrine and operational conditions has resulted in significant underuse of medical assets, particularly at forward surgical teams assigned at the brigade level.¹

Maj. David S. Kauvar, M.D., is a vascular surgeon and the chief of surgical research at Dwight D. Eisenhower Army Medical Center and an associate professor of surgery at the Uniformed Services University of the Health Sciences. He commanded the Tarin Kowt Forward Surgical Element as a member of the Combined Joint Special Operations Task Force-Afghanistan in 2012 and served as a combat support hospital surgeon in Baghdad in 2008-2009.

Maj. Tucker A. Drury, M.D., is the orthopedic clinic chief at Joint Base Elmendorf Richardson in Alaska. He received his orthopedic surgery training at the University of Vermont. He commanded the Tarin Kowt Forward Surgical Element as a member of the Combined Joint Special Operations Task Force-Afghanistan in 2011-2012.



(Maj. David S. Kauvar)

Insurgents are drawn to rural communities that are underserved by the host-nation health sector.² Because COIN is primarily a civil-military endeavor, properly leveraged expeditionary medical assets can be force multipliers in the effort to improve governance and marginalize the activities of insurgents.

This article examines the theory and practice of COIN operations conducted by a forward-deployed special operations surgical element in Uruzgan Province, Afghanistan, in 2012. The Tarin Kowt Forward Surgical Element (TK FSE) was uniquely integrated into the regional special operations task force (SOTF) COIN mission and contributed to the expansion of medical care in Uruzgan and beyond. The experience of TK FSE in Uruzgan should serve as a model for future special operations and conventional military medical unit participation in COIN missions.

General Principles

The goal in COIN is to promote the legitimate host-nation government as a source of stability and order in the lives of the indigenous population.³ To this end, medical operations should focus on increasing the capacity of the host-nation health sector and promoting the host-nation government's role in the people's health. Military medical programs that provide direct care to local nationals can be useful in the initial stages of a COIN engagement to gain the trust of the populace and accustom them to foreign military involvement in their health care. However, direct medical care should be avoided in the long term because it eventually leads to undesirable reliance on foreign medical care and marginalization of the country's health sector.⁴

In contrast to direct care, capacity building can be achieved in two ways: first, through the focused delivery of sustainable direct health and reconstruction aid, and second, by leveraging medical skills and knowledge through training programs and partnerships with the country's health system. Both of these require intensive engagement and relationship building with key health sector leaders. These relationships should form the basis of all COIN health engagements. Specifically, military and host-nation leaders should jointly conduct real-world needs assessments to develop reasonable goals for COIN health programs. Local leaders should maximize the use of host-nation personnel, facilities, and materials in any planned health sector interventions.

Assessments of needs and health sector progress should be performed continually during any health operations in COIN. Engagements and programs should be flexibly designed and executed to allow for responses to fluctuations in local sociopolitical circumstances and changes in the security situation. Measurement of outcomes should be planned for from the beginning of any health program in a COIN mission. The *output* of foreign military activities in the indigenous health sector is easy to measure, in terms of the volume of patients seen and treated. The *outcome* of a COIN health program is reflected in the ability of the host nation's health sector to care for the population; the key data to capture and use to plan further engagements will measure this outcome.

TK FSE and Uruzgan Provincial Healthcare

Uruzgan Province, located in southeastern Afghanistan, has just over 300,000 inhabitants and is one of the poorest, most rural areas in the country. The province has one hospital, located in the capital of Tarin Kowt (TK Hospital). This facility provides referral-level care for the residents of Uruzgan and parts of the adjacent provinces of Day Kundi and Zabul. TK FSE was a small U.S. special operations medical facility, established in 2010 and located on a base just outside the city of Tarin Kowt. The FSE's primary mission was to provide combat casualty and acute primary care for coalition special operators and Afghan partner forces from southeastern Afghanistan. The FSE was adopted an additional mission to leverage its assets in support of the broader SOTF COIN mission. The goal of the engagements arising from this leverage was to increase Afghan regional healthcare capacity and decrease reliance on coalition medical assets, especially for trauma and acute surgical care. The expected strategic outcome of this mission was further legitimacy for the Afghan government, reinforcing it as a provider of health resources for its people.

Afghan Medical Training Partnership and Validation

TK FSE initiated the Afghan Medical Training Partnership and Validation (AMTPV) program in 2010, which was TK FSE's primary COIN medical engagement. The program was a response to an assessment by SOTF medical personnel—through

engagements with district and provincial Afghan health officials—that found unmet health needs in Uruzgan.

The assessment's principal finding was a significant knowledge and skills deficit in the individuals providing trauma services at TK Hospital. Therefore, most injured patients were cared for in U.S. and coalition facilities in the area. To address the deficit and expand local capabilities for the future, a three-year training program for TK Hospital staff was designed, approved, and implemented. An essential criterion for entry into the program was a commitment on the part of the participants to remain in practice at TK Hospital and serve the population of Uruzgan following their graduation. The complement of participants included four groups of three local Afghan providers, each including a physician, a nurse, and an anesthetist. The participants lived and worked at TK FSE alongside U.S. personnel for three months of the year and worked and trained others at TK Hospital the remaining nine months. The trainees participated in all aspects of care performed at the FSE, including the resuscitation of trauma and acute surgical patients, assisting in operations, and caring for patients in the small hospital ward. U.S. military trauma and orthopedic surgeons

supervised all aspects of the Afghan trainees' work and validated their progress.

The Afghan participants were paid for their participation in the AMTPV program by Commander's Emergency Relief Program funds from the SOTF, with a total annual cost of \$76,000. The FSE could help provide care for local national and noncoalition military patients who would not otherwise receive coalition medical care because of their ongoing training of Afghan providers and also the SOTF command's support of medical COIN engagements. The additional workload at the FSE increased resource utilization and provided training experience for AMTPV participants, expanding the capacity of the Afghan health sector to care for its own people. The success of the program was striking: at the program's midpoint, TK Hospital experienced a 100 percent increase in admissions, and we saw a corresponding decrease in the local population's use of coalition health resources.

TK Hospital—TK FSE Partnership

With the successful implementation of the AMTPV program, a strong and durable partnership between TK Hospital and TK FSE evolved. This



Afghan physicians and nurses making patient rounds at Tarin Kowt Provincial Hospital. This practice emerged as a result of education programs instituted by the Tarin Kowt Forward Surgical Element. (Maj. David S. Kauvar)

partnership was reinforced by ongoing needs and capabilities assessments performed by FSE staff at TK Hospital and through frequent key leader engagements with district and provincial health sector officials. The knowledge gleaned from these engagements allowed the FSE to tailor AMTPV program training to the specific capabilities and challenges the participants faced when they worked at the hospital. Specific knowledge of the situation “on the ground” at TK Hospital also permitted the FSE to guide medical reconstruction and humanitarian assistance efforts toward providing the aid and services that would be most sustainable and beneficial.

A patient transfer agreement between the medical director of TK Hospital and the medical staff of the FSE was developed to enhance the education of AMTPV participants and to facilitate complex trauma and initial surgical care for Afghan patients at the FSE. TK Hospital’s director communicated via telephone with one of TK FSE’s two embedded interpreters, facilitating the transfer of patients with needs exceeding TK Hospital’s capabilities to the FSE for care by the AMTPV residents under the supervision of FSE staff. Such transfers were typically sought because of the lack of surgical resources at TK Hospital, compared to those at the FSE. The patient would be transferred back to TK Hospital for ongoing care after being stabilized, usually after initial operative care. Local Afghan surgeons from outside the residency program occasionally accompanied their patients to TK FSE to participate in operations with FSE surgeons, increasing their skills to perform more complex procedures at their home facility.

Patients from Uruzgan and the adjacent provinces of Day Kundi and Zabul gained access to TK Hospital and FSE resources by first seeking care at smaller, local Afghan facilities or SOTF Village Stability Program sites. Then they could be referred to TK Hospital, and then to the FSE if needed. Patients were also evacuated by coalition medical assets from the Village Stability Program sites for more urgent care at the FSE followed by transfer to TK Hospital.

The FSE also hosted a clinic dedicated to caring for local nationals, seeing primarily follow-up patients from TK Hospital and the surrounding area. AMTPV program participants were used in this clinic, learning aspects of long-term care in



Afghan physician examining x-rays of a transferred Afghan patient with his U.S. counterpart at the Tarin Kowt Forward Surgical Element. (Maj. David S. Kauvar)

an austere environment. To preserve base security and control access, the FSE used a *parcha* (paper) system, requiring outpatients seeking care at the FSE to have a referral or follow-up note signed by one of the U.S. physicians stating their need for FSE care on a certain day. This also ensured that in almost all circumstances, patients would be seen at TK Hospital before being seen at the FSE.

Partner Force Care and Training

Supporting the ability of indigenous forces to conduct the campaign is a central principle of COIN military operations. To this end, TK FSE and medical elements of their local partner forces, the 8th *Kandak* (camp) Afghan National Army (ANA) commandos and the 4th *Kandak* ANA conventional forces, developed a partnership for the training and supervised care of ANA soldiers. The ANA medics had basic field medical training, including the use of direct pressure and tourniquets to control bleeding and the use of intravenous fluids for initial resuscitation. In consultation with senior ANA medics and



Personnel from the Tarin Kowt Forward Surgical Element delivering donated medical supplies to Tarin Kowt Provincial Hospital. (Maj. Tucker A. Drury)

physicians through embedded interpreters, FSE staff members taught specific advanced field and hospital medical skills to the ANA elements in response to their specific needs. Such training reduced the ANA's reliance on coalition medical resources in the field and decreased the need for coalition combat casualty care. The ANA medics were highly motivated and quick learners, and their skill set and comfort level with treating complex battle trauma expanded greatly because of the combined training program.

In addition to medical training, TK FSE provided supervised medical care to the 8th Kandak Commandos. A weekly primary care clinic for commandos was held at the FSE. The senior commando medic attended these clinics, learning from FSE primary care providers and AMTPV program participants how to manage commonly encountered problems. The FSE also provided acute and dental care for commandos in a similar fashion. Over time, the number of commandos treated at the FSE declined as the commandos' medical assets assumed much of their routine care.

Critical Enablers and Difficulties

Several critical factors influenced TK FSE's ability to contribute to the SOTF's broader mission by performing medical COIN engagements. The

most important of these were consistent command support. TK FSE was fortunate to have SOTF commanders who supported its participation in COIN activities and who understood the low-cost benefit that embedded medical participation in COIN operations provides. These commanders provided the Commander's Emergency Relief Program funds necessary for projects such as the AMTPV program and authorized leeway in the medical rules of engagement to allow the FSE to assist in the care of local national patients. The SOTF commanders were crucial to ensuring security for FSE personnel during "outside the wire" missions to TK Hospital.

Security was a critical enabler of TK FSE's COIN activities. Civil-military operations in COIN can only be effective in an environment where security has been established, both to provide a stable environment for civil operations and to secure and thus gain the trust of the populace so they will accept such operations.⁵ TK FSE's COIN mission was facilitated by the willingness of the SOTF command to provide security for medical engagements on and off the base. The FSE's acceptance of Afghan medical providers and care of local national patients on our installation required force protection measures beyond those usually in effect. Local national patients had to be searched upon arrival, and the

residents who worked and lived with FSE personnel had to be thoroughly vetted before gaining entry.

The final critical enabler for TK FSE's COIN operations was highly motivated, strongly dedicated personnel who were committed to the mission. Without such personnel, the FSE could not have participated in complex, often demanding medical COIN operations. Basic understanding and acceptance of the cultural differences between FSE personnel and their local national patients were vital as well. Included in the personnel essential to accomplish this mission were the embedded interpreters who lived and worked with the FSE every day. These team members, in addition to interpreting, also provided links with local health authorities and valuable cultural insights. The value of embedded interpreters was multiplied as they worked in the medical environment—learning and practicing basic medical skills, narrowing the cultural gap between host nation patients and coalition medical providers, and becoming true medical interpreters.

The expansion of TK FSE's mission into COIN operations revealed some notable difficulties as well. When operating in the midst of an active insurgency, security was always an issue. FSE operations had to remain flexible within a variable security environment. Planning missions with inherent adaptability helped to mitigate some security difficulties. Another complication in the FSE's COIN operations was the broad cultural gap between FSE providers and Afghan residents, community stakeholders, and patients. Continually fostering a clinical environment in which such differences were acknowledged and accepted, as well as encouraging cultural education by the embedded interpreters, was vital in enhancing cultural understanding among FSE personnel.

The easy part of the FSE's mission was providing medical care to the sick and injured—this is what all medical personnel have trained for. The hardest and most important TK FSE COIN mission was to

decrease local reliance on coalition medical assets so Afghans eventually could provide medical care independently. The intricacies encountered in focusing on training our local partners to better prepare them for caring for their own populace proved vexing. We strived to incrementally increase our partners' capacity to care for their own people. Continual reinforcement of and adherence to the fundamental COIN principle of enhancing indigenous capacity and maintaining a mission profile consistent with this principle helped mitigate some of these difficulties.

Conclusion

Integrating a forward-deployed U.S. surgical unit into the indigenous host-nation health sector in the midst of a COIN operation was a new approach to medical operations in COIN. TK FSE joined the SOTF COIN offensive to an unprecedented degree, its missions garnering measurable positive outcomes in the health care capacity of Uruzgan Province and beyond. The education of local Afghan and partner force medical providers by U.S. military medical providers fulfilled the COIN principle of increasing indigenous health care capacity without unsustainable traditional direct health aid. The depth of TK FSE's involvement in the indigenous health sector allowed for long-term relationships with local Afghan entities that could continually adapt to a changing environment. These relationships resulted in partnerships that were the foundation for the success of the FSE's medical COIN operations in southern Afghanistan. The TK FSE experience was beyond the unsustainable humanitarian assistance efforts of most medical COIN operations. Operations were low cost and high value, and they resulted in dramatic and sustainable gains. TK FSE's resounding successes in increasing Afghan health sector capacity represent a framework for future COIN medical operations. **MR**

NOTES

1. Richard W. Thomas, *Ensuring Good Medicine in Bad Places: Utilization of Forward Surgical Teams in the Battlefield* (academic research paper, U.S. Army War College, Carlisle Barracks, PA, 2006), 18.

2. Report prepared for the Office of the Secretary of Defense, *Counterinsurgency in Afghanistan*, Seth G. Jones, (Santa Monica, CA: RAND Corporation, 2008), 100.

3. Sebastian L.V. Gorka and David Kilcullen, "An Actor-centric Theory of War:

Understanding the Difference Between COIN and Counterinsurgency," *Joint Force Quarterly* (1st Quarter 2011): 17.

4. Matthew S. Rice and Omar J. Jones, "Medical Operations in Counterinsurgency Warfare: Desired Effects and Unintended Consequences," *Military Review* (May-June 2010): 49.

5. Jones, 130-31.

Persistent Conflict and Special Operations Forces

Lt. Col. Phillip W. Reynolds, U.S. Army

The art of war was always to start with...adapting [forces] to the requirements of the particular case.

Carl von Clausewitz, *On War*

AS THE WAR IN AFGHANISTAN CLOSES, there is an almost tangible sense of relief within the Army. Military services are shifting their focus toward Asia. The frustration and grief of the last decade have convinced many that guerrilla wars are best left to the guerrillas. Decisive victory in conventional terms has been elusive.

However, special operations forces in Colombia, the Philippines, eastern Africa, and other locations around the globe have achieved successes. Even during the initial phase of the campaign in Afghanistan, special operations forces achieved many objectives. Organized as small task forces, special operations forces worked efficiently and effectively, while the larger staffs of brigade combat teams and divisions tended toward regimentation and institutionalism.

Conventional headquarters and formations in the Army are too slow and bulky to manage small, persistent, irregular conflicts. The massive multinational headquarters during the late phases of the wars in Iraq and Afghanistan seemed to produce little more than colossal plans for an ever-fleeting victory. Moreover, such military organizations tend to cause massive disruptions in civilians' lives and induce counterstate violence.

Lt. Col. Phillip W. Reynolds is the Southeast Asia branch chief for the 25th Infantry Division where he plans and executes security cooperation engagements in support of U.S. Pacific Command objectives. He holds an M.S. in defense analysis from the Naval Postgraduate School and is a Ph.D. student at the University of Hawaii-Manoa. He has worked in Africa, Iraq, and extensively in Central Asia.



In Afghanistan, conventional military organizations were asked to implement the difficult *social policies* needed to end persistent, irregular conflict—rooted in social problems—while lacking the expertise and experience for the job. It is no wonder conventional forces were marginally successful in Afghanistan; they are designed and resourced to destroy an opposing state's ability to resist. They will always be needed for conventional types of conflict, but irregular warfare needs other types of organizations and tools. United States Special Operations Command (USSOCOM) assets are better suited to the persistent, low-intensity conflicts likely to characterize operations in the near future. This is because USSOCOM is focused on its role as a partner in long-term, strategic, interagency engagement aimed at resolving conflicts that cannot be settled by purely military means.

Future Conflicts

Irregular conflicts will continue to characterize the global security environment. From 2002 to 2011, the Uppsala Conflict Data Program's online *UCDP Conflict Encyclopedia* counted over 370 small or nonstate conflicts—nearly ten times the number of interstate wars.¹ Irregular conflicts take the form of insurgencies, guerrilla wars, terrorism, smuggling, and even simple banditry. Nations are likely to avoid state-versus-state conflict because it is so expensive. Nonstate groups will increasingly seek to achieve their goals using asymmetric and irregular methods because they cannot compete directly against the overwhelming power of U.S. conventional military forces.

A range of conflicts. The United States must remain prepared for very different types of conflicts. On one hand, the U.S. military faces near-peer competitors with the ability to cause significant harm to U.S. interests. The Department of Defense (DOD) will attempt to remain unmatched in its ability to destroy the offensive or defensive capabilities of enemy nations in conventional wars. However, the U.S. military will inevitably find itself confronting more unconventional threats.

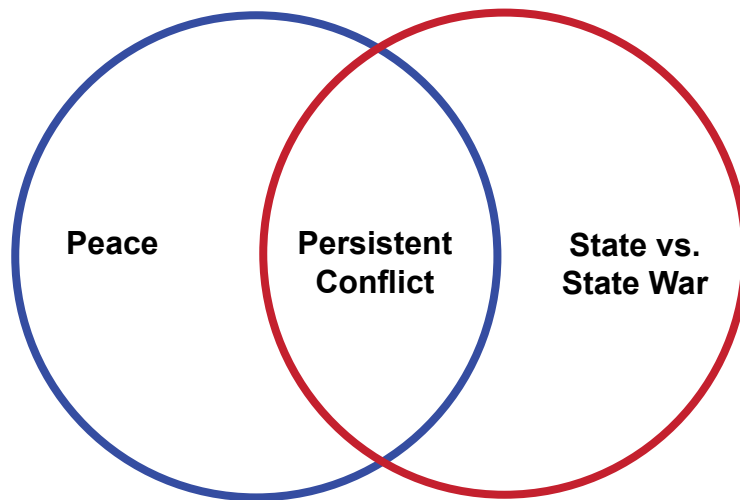
The United States must remain ready to counter insurgencies, state-supported guerrilla wars, and transnational terrorism—the hallmarks of persistent conflict. The United States will not be able to afford large conventional deployments for these types of

persistent conflict. Nor will the nation stomach engagement in large-scale nation building after Iraq and Afghanistan. Calls within the DOD to refocus on high-intensity conflicts are consistent with analyst Martin Van Creveld's prediction that governments will literally contract out their responses to low-intensity conflicts, seeing them as not worth the blood and expense of a military designed to deter global challenges and topple states.² If the Uppsala Conflict Data Program's data are correct, the future of war will look more like the later phases of operations in Afghanistan and Iraq. However, the United States will not likely outsource its response to low-intensity threats. Low-intensity and irregular wars will continue to require U.S. action. The ability to acquire devastating weapons means that even fringe elements could strike a serious blow to the U.S. homeland, as 9/11 proved.³ All told, the next several decades will be as busy as the last. Appropriate U.S. response to calls for support from threatened partners likely will fall somewhere between relatively small, predictable peacetime engagements and full-blown deployments of hundreds of thousands of troops, with their staggering price tag. Obviously, a range of military capabilities will be needed.

A range of capabilities from USSOCOM. As part of a unified effort with other U.S. government agencies, USSOCOM has been providing support around the world that is appropriate to the context for each situation and crucial to a national strategy of persistent engagement. Historically, DOD's most public actions in foreign assistance have been responses during natural disasters. Less well known is DOD's support for strengthening foreign governments' ability to manage internal and international threats. DOD contributes through state building and assistance to foreign militaries.⁴ These operations represent an in-between world with peace on one side and complex maneuver warfare with large deployments on the other (see figure).

Nature of the Adversary

Many adversaries in persistent, irregular conflicts organize as loose, distributed networks rather than large, hierarchical military or political structures. Functioning as distributed networks helps terrorists, insurgents, and criminals remain adaptive. They form amorphous entities not bound by traditional



Persistent Conflict Between Peace and War

political borders or even by international law. Adversaries of this nature continually adapt to changing political and social environments, and these irregular conflicts become “contests for influence and legitimacy.”⁵ The defining characteristics of the conflicts come from the relationships between individuals, families, and ethnic or religious groups. The conflicts simmer over generations because of family, ethnic, or religious ties between the fighters. Persistent conflict itself becomes a network in which trust and intimate contact between individuals predominate.

According to David Tucker, a professor at the Naval Postgraduate School, the overwhelming evidence from psychology and sociology shows that the decision to pursue violence is made in the context of an established social network that aids the mobilization and recruitment of members.⁶ Ties from family, kin and tribe, ethnic group, religious organization, workplace, education, and area of residence influence choices and objectives. Conflicts drag on because the underlying causes of the violence extend across generations, regions, and countries. The nature of adversarial networks and the characteristics of persistent conflicts—including how long they continue—require a light

touch from the United States. When the United States gets involved in these conflicts, overwhelming offensive power will not be the solution.

Success in Irregular Conflicts

The United States has successfully supported partners against nonstate adversaries in El Salvador, Colombia, and the Philippines—and not entirely through military means. In the early 1980s, the Reagan administration found itself fighting a violent insurgency in El Salvador. In the same decade, the war on drugs was focused on the country of Colombia, where a significant portion of the world’s cocaine is still produced.⁷ In 2002, as part of the Global War on Terror, the Bush administration created a small task force in the Philippines to combat the Abu Sayyaf guerrillas.⁸ These efforts could be called “economy of force” actions, while the bulk of the U.S. defense establishment was engaged elsewhere. The Cold War military establishment was still protecting Europe; El Salvador was seen as a secondary theater. Sustained support to Colombia and the Philippines continued even while the focus of DOD became Afghanistan and then Iraq.

In the 1990s, the ultraviolent tri-war between the Colombian military, the independent United Self-Defense Forces of Colombia (Autodefensas Unidas de Colombia, or AUC), and the Marxist Revolutionary Armed Forces of Colombia—People’s Army (Fuerzas Armadas Revolucionarias de Colombia, or FARC) was threatening to drag the country into anarchy. In 2000, under the Clinton Administration, Congress approved a security assistance package worth over \$1 billion.⁹ In Colombia, the AUC demobilized as the Colombian security forces were better able to contain the FARC. In 2012, Colombian president Santos finally announced that FARC was willing to negotiate an end to the longest conflict in the Western Hemisphere.¹⁰ While there have been no such negotiations in the Philippines, the influx of security assistance appears to have set the stage for a peaceful settlement. The U.S. military and government agencies have been instrumental in helping the armed forces of the Philippines capture or kill leaders of the militant group Abu Sayyaf and the Moro Islamic Liberation Front, antigovernment organizations operating in the south.¹¹ Conversely, hundreds of thousands of men and vast expenditures of money failed to turn the tide in Vietnam. The Afghan surge appears to have done little, while Iraq is poised to slip back into chaos.

Why the Difference?

Common to our successes is the careful application of limited resources appropriate to each situation and over the long run. Analysts at the RAND Corporation uncovered similar conclusions in the study, *Victory Has A Thousand Fathers: Sources of Success in Counterinsurgency*.¹² Perhaps unsurprising to some, the length of time needed for concerted interagency support to a counterinsurgency (COIN) effort was inverse to how the United States preferred to fight its conventional wars. Plans in El Salvador, Colombia, and the Philippines were designed to last years, while the war against Iraq was meant to last weeks. During a COIN operation, resources were used inversely to logistically heavy conventional war.¹³ Instead of turning on the spigot to support a COIN effort, resources—both personnel and material—were

tightly controlled and often subject to regular congressional oversight.¹⁴

This strategy of persistent engagement over the long term could solve some vexing problems. First, it is an economy-of-force effort needing relatively few resources. If applied early, then the United States may be able to avoid massive and costly deployments of direct combat forces. The range of threats described in the *Capstone Concept for Joint Operations: Joint Force 2020* can be engaged early, before larger and more lethal options might be needed. Second, small special operations task forces executing a strategy of persistent engagement can avoid the public war weariness associated with long campaigns.¹⁵ Conducting persistent engagement on a small scale helps avoid drawing media attention. Remaining out of the public eye extends national perseverance.

U.S. forces deployed to El Salvador, Colombia, and the Philippines were from the special operations community. In Colombia’s case, increased support via the “Plan Colombia” began shortly before 9/11. American media attention naturally gravitated to the Middle East. In El Salvador’s case, news media did report heavily on U.S. involvement there, sensing a potential repeat of the Vietnam disaster of the previous decade. In most cases, Americans were aware of U.S. involvement in El Salvador, and they opposed large-scale intervention.¹⁶ The few U.S. casualties that did occur were framed as criminal activity, usually in cities, and far from the combat patrols of the El Salvadoran army. Additionally, since Congress had prohibited U.S. personnel from patrolling with the units they trained, only a few news reports attempted to link U.S. advisory efforts to human rights abuses. Because of its low cost and limited media attention, engagement can continue for as many years as needed. This allows a generational approach—appropriate when engaging insurgent or terrorist networks. This soft approach, with small numbers of personnel concentrating on training and appropriate nonlethal support, often decreases casualties.

The hallmark of the campaigns in El Salvador, Colombia, and the Philippines is that the main effort has not been the military, and the primary tools used by the military have not been lethal.

In El Salvador, the national campaign plan was largely the product of the U.S. embassy in San Salvador. In Colombia, the idea of the Plan Colombia was presented as early as 1998 to the Clinton administration. The support began in 2000 as an effort to stabilize Colombia with foreign military sales and Andean counterdrug initiative money. Funding from 2000 through 2010 for all types of support came to over \$7 billion.¹⁷ The original 1990s plan, Plan Colombia, has given way to a new initiative under the current Colombian administration, the National Consolidation Plan, and the Colombian government created a cabinet-level Center for Coordinated Integrated Action in 2004. The center was instrumental in integrating the overall efforts of the Colombian government (military, police, political, and economic) to consolidate gains made in the COIN effort against the FARC.¹⁸ In the Philippines, various programs such as the Peace and Order Council and the Council for Peace and Development were created by the Philippine government to coordinate national, provincial, and lower-level development plans. These have proven effective at implementing the security and civil reforms needed to bring the insurgency to an end.¹⁹

The U.S. Congress has mandated constraints on the scope of U.S. military activities in all three countries. In Colombia, U.S. military involvement began in 2000 and was limited to training Colombian counternarcotics units, although U.S. forces now train the Colombian military in COIN operations.²⁰ About 200 special forces soldiers work in Colombia, where they are limited to training in garrison, and planning and intelligence support at headquarters.²¹ U.S. forces do not accompany or serve as advisors to Colombian units conducting combat operations. In the Philippines, U.S. military operations are limited by the Philippine constitution. Foreign military forces are not permitted to participate in combat operations on Philippine territory. The U.S. military is restricted to conducting training in COIN and counterterrorism tactics, advising Philippine units, and participating in civil-military operations.²²

The Joint Combined Exchange Training conducted under Section 2011 of Title 10, United States Code; theater security cooperation plans; and the Overseas Humanitarian, Disaster, and

Civic Aid program, have provided a stable platform for unified U.S. government efforts in Colombia and the Philippines. The Joint Combined Exchange Training exercises with friendly foreign militaries are conducted ostensibly for training U.S. special operations forces. Humanitarian assistance programs such as medical and veterinary

Force caps reflect congressional and public reluctance to allow the military to expand conflicts by introducing ever-greater numbers of troops.

visits may be added to cultivate goodwill among local populations and as part of the training for foreign troops.

In 2006, Congress authorized a new “global train and equip” fund and has renewed it every year since.²³ Section 1206 of Public Law 109-163 provides the first major DOD authority to be used expressly for the purpose of training and equipping the national military forces of foreign countries. For the past half-century, DOD has trained and equipped foreign military forces under State Department Title 22 authority and through State Department programs. While there are some congressional misgivings with this blurring of State Department and DOD boundaries, combatant commanders consider the Section 1206 program “the single most important tool for the Department to shape the environment and counter terrorism.”²⁴ This authority allows USSOCOM to train and equip foreign military forces and foreign maritime security forces to perform counterterrorism operations and to participate in or support military and stability operations with the United States.²⁵ It has been used in Colombia, the Philippines, and even the Arabian Peninsula.

Congress also placed limits on the number of personnel in country, called force caps. Force caps reflect congressional and public reluctance to allow the military to expand conflicts by introducing ever-greater numbers of troops. In El

Salvador, the initial force cap was 55, although various add-ons eventually swelled the number to 150.²⁶ In Colombia, Congress has prohibited U.S. personnel from participating directly in combat and has mandated a personnel cap of 800. In an acknowledgement of the growing role of contractors, Congress capped their number in Colombia at 600.²⁷ The growth of the force cap between the two cases is reflective of each country's conflict and military capacity. The U.S. Military Group, El Salvador, was training an infantry-based force armed with simple weapons and using relatively simple tactics. In Colombia, the higher force cap reflected the need to train the Colombian navy on drug interdiction tactics and the Colombian air force in the use of sophisticated Blackhawk helicopters. In the Philippines, the United States created the Joint Special Operations Task Force-Philippines in 2002 to train the armed forces of the Philippines and to combat militants with ties to al-Qaida. The average force strength was 500

to 600, but there were surges in personnel, mostly in support of a large, annual exercise called *Balikatan*.²⁸

Despite the dilemmas force caps have posed to the military planners and commanders on the ground, they do not seem to have impaired DOD's ability to achieve its mission. The idea that using more personnel might be more effective by allowing forces to achieve objectives more quickly has two major flaws. First, Congress must weigh continuing commitments of personnel and money against future unknowns—and the certainty that increasing the number of personnel would also increase public scrutiny. Second, tens of thousands of U.S. service members in a country feed negative perceptions of invasion and occupation, as happened in Iraq and Afghanistan.

The emphasis on checks and balances in the interagency approach has meant that the purely military element could not overwhelm planning and resources. Moreover, it appears successes



Competitors conduct a static line jump from a C-130 aircraft during Fuerzas Comando 2012, a special forces skills competition at the Colombian National Training Center on Fort Tolemaida, 13 June 2012.

have included improving the ability of the host nations to contain insurgencies effectively while U.S. military influence in planning and execution waned.²⁹ This transition from open insurgency to normal political and economic life was the goal in each plan, the same as Iraq and Afghanistan. However, the evidence indicates that while the military is the best instrument to provide immediate, stabilizing security, the introduction of more military units tends to aggravate the population, driving more into insurgent activities. During these successful COIN campaigns, the interagency process worked to ensure that the military operations did not crowd out the political and economic work that was the fundamental key to success. These “whole-country” plans were developed relatively early in the campaign. In all three countries, immediate military assistance from the U.S. task forces sought to stabilize battered host-nation security forces. Military support concentrated on weapons and tactics training. There was no attempt to transform the society, as was the case in Afghanistan with the International Security Assistance Force’s focus on governance and development.

Conclusion

The Joint Force 2020 concept identifies a future security environment in which armed conflict will be inevitable and enduring.³⁰ As they always have, irreconcilable wills continue trying to dominate each other through violence. When the United States responds to conflict, its approach needs to account for political and fiscal constraints. This means working with partners and avoiding large



Sgt. Jordano Hernandez, Company A, 163rd Military Intelligence Battalion, 504th Battlefield Surveillance Brigade, speaks with members of the Afghan Border Police before attacking a possible weapons cache site during Operation Southern Strike II near Yaro Kalay, Afghanistan, 4 June 2012. (U.S. Army, Sgt. Brendan Mackie)

deployments of direct combat forces. Myriad tools and authorities that fall under theater security cooperation will allow robust and persistent engagement. Experiences in El Salvador, Colombia, and the Philippines illustrate three ongoing constraints that need not impair effectiveness:

Congressionally mandated constraints on military activities. Far from causing problems while assisting partners, congressional guidance in the form of policies and laws actually serve to clarify the working relationships between the military services and the rest of the U.S. government. Occasional hearings and mandated reports ensure that the ultimate arbiter of foreign policy—the American public—supports military involvement.

Force caps. Mandating upper limits on the deployments of personnel forces headquarters

staffs to streamline their planning processes. This necessitates delegating nonmilitary tasks to the agencies best suited to achieve objectives.

Resource limits. Limiting resources forces local U.S. commanders to innovate to achieve their goals. It helps partner nations understand they must plan and execute the hard work of COIN operations without receiving billions of dollars in aid.

Persistent conflict presents a vexing and difficult problem. Americans are adverse to the idea of limited, never-ending wars of any kind. They prefer the

clean ending of a fight to the finish against enemies seen in terms of absolute evil.³² However, DOD and the U.S. government must respond to the low-level conflicts that threaten our interests around the world. In an era of fiscal restraint, the United States must be able to influence and shape future conflicts and achieve success. Traditionally, choices were limited. The United States could stand by while partner nations engaged in their own persistent conflicts, or deploy massive resources in order to support our partners. There is a middle way. **MR**

NOTES

1. Uppsala Conflict Data Program, *UCDP Conflict Encyclopedia* (Uppsala University, Department of Peace and Conflict Research), <www.ucdp.uu.se/database>.

2. Martin Van Creveld, *The Transformation of War* (New York: The Free Press, 1991), 207.

3. Michael Horowitz, *The Diffusion of Military Power* (Princeton, NJ: Princeton University Press, 2010).

4. Congressional Research Service (CRS) Report for Congress, *The Department of Defense Role in Foreign Assistance: Background, Major Issues, and Options for Congress*, RL34639, Nina M. Serafino (Washington, DC: U.S. Government Printing Office [GPO], 2008).

5. Department of Defense (DOD), *Irregular Warfare: Countering Irregular Threats: Joint Operating Concept, Version 2.0* (Washington, DC: GPO, 17 May 2010), 4, <http://www.dtic.mil/futurejointwarfare/concepts/iw_joc2_0.pdf>.

6. David Tucker, "Terrorism, Networks, and Strategy: Why the Conventional Wisdom is Wrong," *Homeland Security Affairs*, 4(2) (June 2008), <<http://www.hsaj.org/?article=4.2.5>>.

7. United Nations Office on Drugs and Crime, *Colombia: Coca Cultivation Survey 2009* (June 2010), <<http://www.unodc.org/documents/crop-monitoring/Colombia/Colombia-Coca-Survey-2010-ENGLISH-web.pdf>>.

8. CRS Report for Congress (updated), *Abu Sayyaf: Target of Philippine-U.S. Anti-Terrorism Cooperation*, RL31265, Larry Nicksch (Washington, DC: GPO, 2007).

9. CRS Report for Congress, *Colombia: Conditions and U.S. Policy Options*, RL30330, Nina M. Serafino, (Washington, DC: GPO, 2001).

10. Chris Kraul, "Colombia President Announces Peace Talks With FARC Rebels," *Los Angeles Times*, 4 September 2012.

11. Thom Shanker, "U.S. Military Unit to Stay in Philippines," *New York Times*, 21 August 2009.

12. RAND Corporation National Defense Research Institute report prepared for the Office of the Secretary of Defense, *Victory Has A Thousand Fathers: Sources of Success in Counterinsurgency*, Christopher Paul, Colin P. Clarke, Beth Grill (Santa Monica, CA: National Defense Research Institute, RAND Corporation, 2010).

13. Russell Weigley, *The American Way of War* (Bloomington: Indiana University Press, 1977); and Thomas Mahnken, *Technology and the American Way of War since 1945* (New York: Columbia University Press, 2008). Mahnken discusses the pivotal changes following the World War II and the Korean Wars toward heavier use of technology.

14. Alfred Valenzuela and Victor Rosello, "Expanding Roles and Missions on the War on Drugs," *Military Review* (March-April 2004).

15. Eric Larson and Bogdan Savych, *American Support for Military Operations* (Santa Monica, CA: RAND Corporation, 2005).

16. Richard Sobel, "Public Opinion about United States Intervention in El Salvador and Nicaragua," *The Public Opinion Quarterly* 53(1) (Spring 1989): 114-28.

17. CRS Report for Congress, *Colombia: Issues for Congress* RL32250, June Beittel (Washington, DC: GPO, 2011).

18. RAND Corporation National Defense Research Institute report prepared for the Office of the Secretary of Defense, *From Insurgency to Stability*, Angel Rabasa, John Gordon IV, Peter Chalk, Audra K. Grant, K. Scott McMahon, Stephanie Pezard, Caroline Reilly, David Ucko, S. Rebecca Zimmerman (Santa Monica, CA: National Defense Research Institute, RAND Corporation, 2011), II: 242.

19. Donna Lynn A. Caparas, *Participation of the Public and Victims for More Fair and Effective Criminal Justice in the Philippines*, <http://www.unafei.or.jp/english/pdf/RS_No56/No56_23PA_Caparas.pdf>; and U.N. Development Program Report, *Assessment and Development Results: The Republic of the Philippines*, <<http://www.oecd.org/countries/philippines/46820404.pdf>>.

20. CRS Report for Congress, *U.S. Military Operations in the Global War on Terrorism: Afghanistan, Africa, the Philippines, and Colombia*, RL32758, Andrew Feickert (Washington, DC: GPO, 2005).

21. Kathleen Rhem, "U.S. Helping Colombian Military Cope with Drug War's Legacy," *American Forces Press Service*, 29 November 2005.

22. Feickert.

23. CRS Report for Congress, *The Department of Defense Role in Foreign Assistance: Background, Major Issues, and Options for Congress*.

24. DOD, *Fiscal Year 2010 Budget Request: Summary Justification*, Robert M. Gates (Washington, DC: GPO, May 2009), 1-13.

25. CRS Report for Congress, *Security Assistance Reform: Section "1206" Background and Issues for Congress*, RS22855, Nina M. Serafino (Washington, DC: GPO, 2011), 7.

26. Andrew J. Bacevich et al., *American Military Policy in Small Wars: The Case of El Salvador* (Washington, DC: Pergamon Press, 1988).

27. CRS Report for Congress, *Colombia: Issues for Congress*.

28. CRS Report for Congress, *The Republic of the Philippines and U.S. Interests*, RL33233, Thomas Lum (Washington, DC: GPO, 2012).

29. RAND Corporation, *From Insurgency to Stability*, 242.

30. DOD, *Capstone Concept for Joint Operations: Joint Force 2020* (Washington, DC: GPO, 2012), 2.

31. Mahnken, *Technology and the American Way of War since 1945*.

COINvasion?

Korengal and Weygal Valleys Post-Mortem

Maj. David H. Park, U.S. Army

(Photo: Max Klimburg)

DURING THE HEIGHT of the counterinsurgency (COIN) campaign in Afghanistan (between 2007 and 2010), Army units engaged in sustained combat in the narrow valleys of Korengal and Weygal in Kunar Province. Having identified Kunar as a crucial region for the Taliban, U.S. forces established several small outposts. Some came under heavy attack by insurgents, including Korengal Outpost, Combat Outpost Restrepo, and Vehicle Patrol Base Wanat. The combat actions performed by U.S. troops in these regions will be remembered as some of the most valorous and honorable in the annals of military history.

Historians, strategists, and journalists have studied and written about these battles in depth. Authors such as Bing West and Sebastian Junger have produced bestselling expositions of the campaigns. The movie *Restrepo* (aired in 2010), illustrated the grunt's view of the battle for the Korengal Valley from 2007 to 2008.

Maj. David H. Park is the executive officer for the 16th Engineer Battalion, Ready First Combat Team, 1st Infantry Division. He earned a B.S. in Foreign Service degree in international politics and an M.A. in national security studies from Georgetown University, as well as an MMAS in military history from the U.S. Army Command and General Staff College (CGSC). He was the distinguished master tactician of CGSC class 11-02. Maj. Park has deployed on five combat tours to Iraq and Afghanistan, most recently as a security force assistance team leader and brigade chief of operations in Kandahar, Afghanistan. He wrote this article in 2011.

Therefore, there is no need to rehash the campaign. Instead, this article analyzes the terrain and the sociocultural factors (sometimes called human terrain) of the Korengal and Weygal valleys, primarily from a strategic perspective. It offers an explanation for the fierce attacks on U.S. forces during the multiyear effort at Kunar-Nuristan (between 2007 and 2010). This work is offered for reflection, discussion, and further study on strategic analysis as well as to foster a productive debate.

An Alternate Analysis of Kunar-Nuristan

To the inhabitants of the mountainous region of Kunar-Nuristan, their homeland is and always has been separate from the nation of Afghanistan. In their minds, the U.S. campaign in the Korengal and Weygal valleys was an invasion of their independent homelands. From this point of view, U.S. forces, instead of conducting COIN, were invading and occupying *de facto* sovereign nations who fiercely resisted. That resistance ultimately led to the withdrawal of U.S. forces from the region in 2010.

Korengal and Weygal as Independent States

The Kunar-Nuristan region is a mountainous area north of Jalalabad and east of Kabul. It contains a large valley system created by the Kunar River, which drains into the Kabul River in the south, on the plains of Jalalabad. The Kunar subsequently drains into the Indus River of Pakistan. As such, the Kunar River valley system is a large tributary of the greater Indus Valley, which empties into the Indian Ocean (see figure 1).

The drainage basins of river valleys have defined the boundaries of distinct civilizations and cultures throughout history.¹ The traditional inhabitants of the Kunar Valley are the Nuristani tribes, who are foreign to the inhabitants of the Helmand River system (Pashtuns) and the Amur Darya River systems (Tajiks, Hazaras, and Uzbeks).

Between the various branches of the Kunar River the mountains provide natural boundaries between the river's subvalleys. At Asadabad the Kunar River splits into Kunar main and the Pech River. The Pech River again splits into the Weygal and Korengal rivers and creates corresponding valleys. Over time, the rugged terrain shaped the microcultures of these valleys to become largely self-contained and

helped local populations resist outsiders for millennia. Travel between the valleys is possible through various passes over the mountains. The historical significance of these passes is evident in that the majority are named and labeled on local maps.

The Nuristani peoples. The peoples of the Kunar-Nuristan region possess their own languages, but most are without an alphabet. They lack a written history. Therefore, to study these peoples we must study the historical writings of their more literate neighbors. The sciences



Figure 1. The Three River Basins of Afghanistan

Author's own work produced as a geographic information system overlay on Google Earth, based on 3D terrain analysis of the river basins for A688 Wanat and Pech Virtual Staff Ride, December 2011.



1st Lt. Chris Richelderfer, Executive Officer of Headquarters and Headquarters Troop, 1st Squadron, 91st Cavalry Regiment (Airborne), looks at possible enemy positions during Operation Saray Has near Forward Operating Base Naray, Kunar Province, Afghanistan, 25 April 2006. (U.S. Army, Sgt. Brandon Aird)

of genetics, archaeology, and linguistics allow us additional insights. We know that the inhabitants of Kunar are mostly Pashtun of the Safi tribe, while those in the Korengal and Weygal valleys, as well as the Nuristan Province, are considered Nuristanis. Geography partitions these two groups. The Pashtun people are limited to the valleys of the Kunar and Pech Rivers.²

The Nuristani tribes have as many as six languages, each with dialects—some numerous.³ Difficult travel over the extremely mountainous terrain of the Kunar-Nuristan region has caused many dialects of Nuristani languages to become unintelligible to speakers living in adjacent valleys. (Linguists cite the Dutch and Afrikaans languages as an example of a relatively recent language split causing a reduction in mutual intelligibility.⁴) Although the Nuristani languages belong to the Indo-Iranian family of languages, they are not mutually intelligible with Farsi, Dari, or Pashto.

History and culture. From the written history of the Pashtun Kingdom of Durrani Dynasty, we know that the Nuristani people, originally referred to as Kafiri (pagans), were the first inhabitants of

the Kunar River valley. The Pashtun people have advanced into the valleys over centuries, pushing the Nuristanis further north and into the valleys where they now reside. The Pashtun people had united under the Durrani (formerly called Abdali) tribe by the 1700s, while the Nuristanis have remained splintered at the clan and village level.⁵ The Pashtuns became Muslims between the 7th and 10th centuries, while the Nuristanis resisted Islam until the 1890s. The Pashtuns finally conquered all of Nuristan between 1895 and 1896 under Emir Abdul Rahman Khan.⁶ The Nuristanis were forcibly converted but still retain small elements of their original pagan religion. The Nuristani religion bears similarities to many of the religious practices of previous invaders, such as Persian Zoroastrianism, Indian Buddhism, and Greek Polytheism.

The Pashtun conquest converted the Nuristanis to Islam and subjugated them to the Pashtun suzerainty, but the Nuristani tribes never relinquished their independence or sovereignty within their valleys. In fact, the Pashtuns took the lower valleys of Kunar for themselves but were unable to

push into the deeper valleys of Korengal, Weygal, or Nuristan proper. The Nuristanis maintained their de facto independence in return for religious subjugation and recognizing the Pashtun king as their sovereign. This system of swearing fealty to the conquering emir in return for local autonomy is similar to the medieval European feudal system. As long as the taxes were paid, loyalty was sworn, and troops provided when needed, the local tribes were allowed relative autonomy. This ancient system of governance continues to this day within the Taliban-run parallel government of the Islamic Emirate of Afghanistan. This tribal system of governance derives its legitimacy from its sheer longevity in central Asia, where the people have known it since before the Persian conquest in the 5th century BC.

The Nuristani valley tribes are still ruled by an informal gathering of local elders. This system of governance enjoys the full support of the Nuristani peoples, who have resisted all other forms of government. The elders comprise the true legitimate government of Nuristan, using a rudimentary form of democracy through a system of shuras (referring to an approach to decision making involving a consultative council) to build valley-wide consensus. The corrupt officials of Karzai's government never achieved legitimacy in this region. Their insistence on halting the native logging trade in the name of nature conservation is a direct affront to the traditional Nuristani way of living.⁷ To the Nuristanis, unaccustomed to government meddling in their internal affairs, the Afghan officials' attempt at halting their native economy while building roads and police stations with an overt U.S. presence appeared to be an invasion by corrupt proxies of the West. The settlement pattern of the Pashay Pashtuns in the Kunar Valley leading into the Pech Valley is the historic outline, or the high water mark, of the Pashtun conquest of the Nuristanis. It also marks the furthest extent of the control and governance by the Pashtun-dominated leadership of the government of Afghanistan. This crucial fact has been glossed over during the past 10 years of war in Afghanistan.

Defensive valley civilization of Nuristan. Due to the lack of Nuristani historiography, we have to speculate as to how they conducted their wars of resistance against past invaders. However, their culture bears the scars of centuries of defensive warfare. People throughout the world prefer to live

in the most naturally comfortable locations that support their lifestyles. This means they build houses in locations that provide easy access to transportation and water. This explains the prevalence of cities and towns around the world near coastlines or by rivers, usually on a plain or a small patch of flat land. People generally do not like to live on steep slopes or on high ground away from their water source or farms. Walking from a house built on a steep slope down to the river to draw water every morning is a very tiring act, unnatural to most people in the world.

The typical layout of towns and villages in the Korengal and Weygal valleys demonstrates an unnatural pattern of settlement. While the sparse farm plots of the Nuristanis remain on the small valley floor, their houses are built in crowded formations along the steep hillsides. These multistory houses are built with stones, with small windows facing the valley floor. This uncommon style of settlement is traditional to the Nuristanis. The Pashay Pashtuns of Pech and lower Kunar live on the valley floor, using traditional mud bricks for their houses (see figure 2).

The most likely explanation for this type of village design is that the Nuristanis built their houses on steep hillsides to defend themselves against invaders who traveled up the valley floors to try to conquer them. The design of the villages is the culmination of the Nuristani tribes' two millennia of generally successful defense of their culture and their way of life (see figure 3).

The villages of Korengal and Aranas show an advanced defensive design allowing nearly all houses of a village to provide suppressive fire on the single narrow chokepoint that leads into the main valley. One can easily imagine the villages adopting this defensive formation over time in place of the more comfortable formation that would have placed the houses near the valley floors. The Nuristanis are de facto independent tribal nations, each ruled by a council of elders; their fortified towns have helped the tribes protect their autonomy for millennia.

COIN or Invasion?

U.S. COIN doctrine assumes that forces are supporting a legitimate government, however basic, with the aim of increasing its legitimacy, influence, and strength. It identifies the "people" as the center of gravity, whose support the U.S.

and host-nation forces must try to win. An assumption in this narrative is that the people—imagined, evidently, as relatively homogenous and capable of cohesion—will eventually support the government as their own once it proves itself legitimate and capable. The problem with this narrative, when it comes to the perspective of the Nuristanis, is that each tribe already has its own legitimate government, its own culture, and a nation it considers its own. We moved into these valleys to “win hearts and minds,” to “separate the people from the insurgents,” and to “protect the people from the insurgents.” We were instead invading sovereign, if internationally unrecognized, tribal nations

that did not want the Pashtun- and Dari-speaking government of Afghanistan to displace their local system of governance. The doctrine of COIN addresses the support of a legitimate government fighting an antigovernment force. Perhaps it is not the best doctrinal framework to address an outright invasion of a *de facto* nation.

Decades after the United States withdrew from Vietnam, a nebulous consensus emerged among U.S. historians that we had misconstrued a Vietnamese war of independence as a purely ideological communist insurgency. These scholars posited that in the eyes of the Vietnamese people, the corrupt South Vietnamese government was a continuation of the

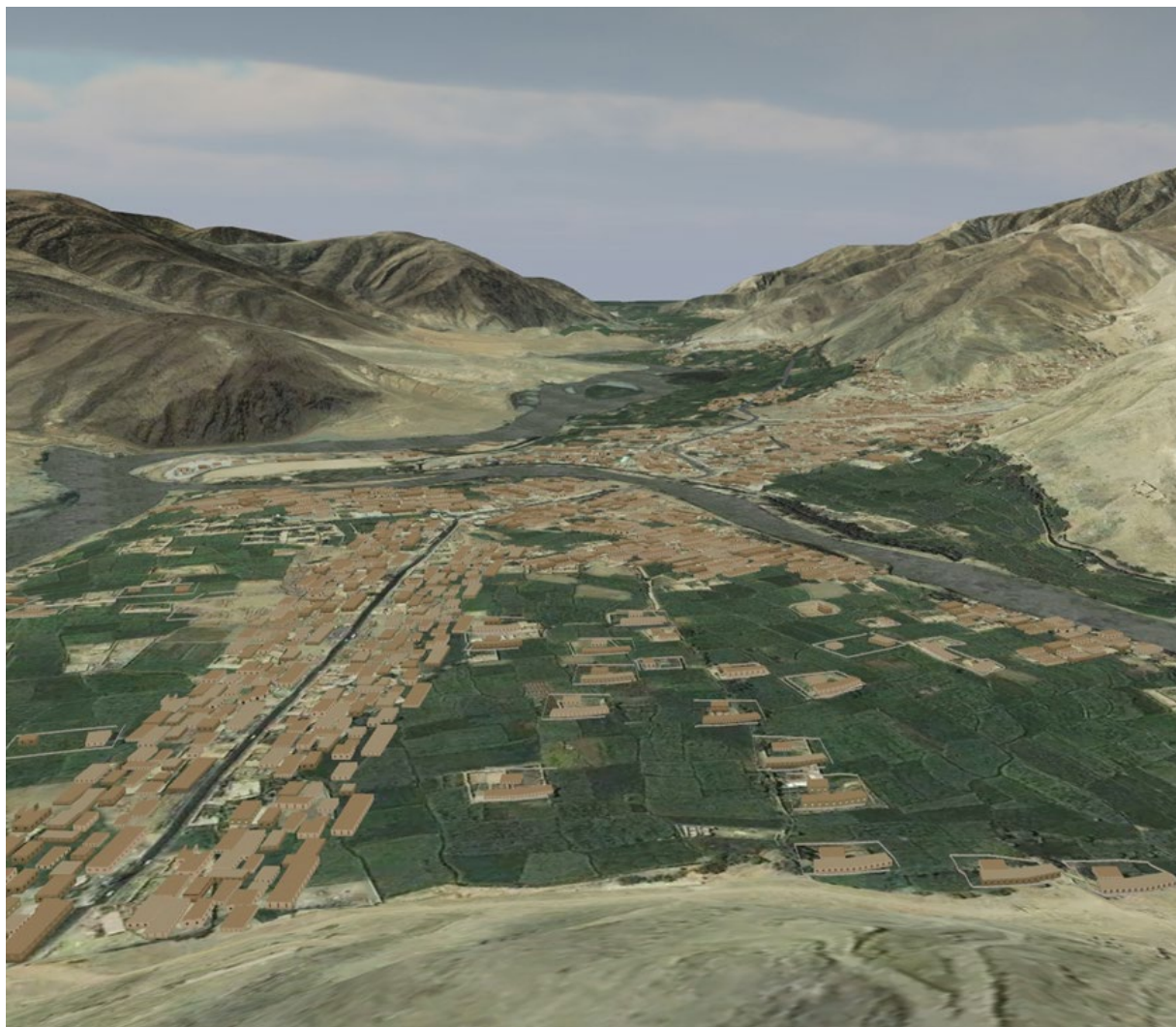


Figure 2. Pashtun Valley Floor Agricultural Settlement

Looking west from Asadabad and the Pech-Kunar River confluence, showing a typical Pashtun valley floor agricultural settlement, Kunar Province, Afghanistan (Geographical and Terrain data depicted via MedRView, supplied via A688, Wanat and Pech Virtual Staff Ride, December 2011).



Figure 3. The Korengal Valley

View of the Korengal Valley from the Korengal Outpost, Kunar Province, Afghanistan (Geographical and Terrain data depicted via MedRView, supplied via A688, Wanat and Pech Virtual Staff Ride, USACGSC, December 2011).

western colonialist regime under France. Ho Chi Min's communists were freedom fighters who happened to be using the communist ideology to assist them in fighting the greatest military power in the world. Similarly, there are those within the Army, such as Col. Gian Gentile, who think the population-centric COIN doctrine is the wrong framework with which to address Afghanistan.⁸ The debate continues, as does the fighting, and our understanding of culture and history is still incomplete. After 10 years of war in Afghanistan, most Army officers still cannot differentiate between Sunni and Shia, Arabs and Persians, and Taliban and al-Qaida.

Therefore, in the face of a pervasive lack of understanding at the strategic and operational

levels, it might be premature to declare that COIN has been the right or the wrong framework in Afghanistan. However, we should be open to that conclusion because the tribal governmental structure had never been replaced or even defeated by the host-nation government. Our insistence that the Karzai regime was the legitimate government of Afghanistan has fostered little goodwill among the Nuristanis.

Our Defeat in Afghanistan

In the future, military historians perhaps will categorize Korengal and Weygal campaigns as invasions into sovereign valley tribal states. In these areas, at least, whether the current COIN framework was the correct approach is an open question.

Limited to the tactics, techniques, and procedures within the COIN framework, our military officers did the best they could. The establishment of the combat outpost Restrepo, resulting from a sound tactical terrain analysis of the Korengal Valley, precipitated a dramatic reduction of violence in the valley. Our military leaders have not failed at the operational and tactical levels. Our national leaders who start wars from their Washington, D.C. offices do not use a rigorous framework similar to the joint operational planning process, the military decision-making process, or even “design” to keep them focused. The decision to adopt the COIN framework, pushed heavily by ideologically driven private lobbies and think tanks, resulted in the limitation of military options at the operational level.

A study of Afghan and Central Asian history shows that the land of modern-day Afghanistan was repeatedly conquered and settled by successive waves of invaders. Cyrus the Persian conquered Afghanistan in fifth century B.C., settling the area with Farsi-speaking ancestors of today’s Tajiks. Alexander’s Greeks conquered Afghanistan in the third century B.C. They established Bactria, which lasted over three centuries, in an area completely isolated from their European cousins. The White Huns, or Hephthalites, followed the Kushans, who conquered and absorbed the Greeks of Bactria. The Hephthalites are today known as the Abdali tribe of the Pashtuns. The Mongols under Genghis Khan and later under Timur and Babur also conquered and settled this land. The very presence of the Tajik, Pashtun, and Hazara people in Afghanistan shows that outside groups have successfully conquered and integrated themselves into Afghan civilization. Only western armies have failed to fully subdue Afghanistan, beginning with the British and later the Soviets and now the Americans. The successful conquerors of Afghanistan understood and respected the local tribal system of governance. Requiring little more than submission, swearing of fealty, and the payment of reasonable taxes, conquerors such as Cyrus, Alexander, Genghis Khan, Timur, and Babur brought centuries of peace to Afghanistan. Only the West, which tried to dismantle the traditional Central Asian way of life and replace it with utterly foreign, and

ultimately dysfunctional types of governance (communism in the 1980s and liberal democracy in 2000s), has failed to provide stable and lasting governance in Afghanistan.

The invasion of the Korengal and Weygal valleys represented a microcosm of the overall Afghan campaign. U.S. forces entered numerous

...each tribe already has its own legitimate government, its own culture, and a nation it considers its own.

areas in Afghanistan trying to displace cultures and systems of governance with a poorly functioning substitute, represented by the Karzai kleptocracy. In contrast, defining a small and precise end state for the operation and then allying with local governance structures to realize small goals would have been far easier. Instead of focusing on what brought us to Afghanistan to begin with, we tried to transform an ancient central Asian civilization into a replica of western democracy.

A better approach would have been to conduct a punitive expedition with an end state limited to killing Osama bin-Laden, destroying al-Qaida, punishing the Taliban for supporting it, rewarding our Northern Alliance with significant monetary resources, and then departing in victory. By trying instead to transform an ancient culture into our own image, we unwittingly placed ourselves in an invasion scenario of numerous tribal nations within Afghanistan. Having fought others for centuries, now they were galvanized against us, their common enemy, making the situation a quagmire from which we are now ignominiously withdrawing. Despite the failure of analysis at the strategic level, our soldiers managed to snatch honor and victory at the tactical level. However, good tactics do not salvage a broken strategy, and young men and women pay for this mistake with their lives. **MR**

NOTES

1. David Park, *The Geopolitical Destiny of East Asia* (Leavenworth, KS: Command and General Staff College, December 2011), 62-63, see <<http://www.dtic.mil/dtic/tr/fulltext/u2/a566063.pdf>>

2. Michael Moore and James Fussell, *Kunar and Nuristan: Rethinking US Counterinsurgency Operation, Afghanistan Report I* (Washington, DC: Institute for the Study of War, July 2009), 7.

3. See <<http://www.ethnologue.com/map/AF>> for the language groups of the Kunar-Nuristan region.

4. Charlotte Gooskens, "The Contribution of Linguistic Factors to the Intelligibility of Closely Related Languages," *Journal of Multilingual and Multicultural Development* 28, no. 6 (2007).

5. Stephen Tanner, *Afghanistan: A Military History from Alexander the Great*

to the War Against the Taliban (Boston: DaCapo Press), 114-21.

6. Martin Ewans, *Afghanistan: A Short History of Its People and Politics* (New York: Harper, 2009), 98-109.

7. It is a fact that in the recent decades Nuristani logging has resulted in mass deforestation of the region, in keeping with the acceleration of desertification in the entire Central Asia, see <<http://easterncampaign.com/2008/01/05/timberlords-and-the-deforestation-of-afghanistan/>>.

8. See Gian Gentile, *Wrong Turn: America's Deadly Embrace of Counterinsurgency* (New York: The New Press: 2013), and posts at *Small Wars Journal* blog, <<http://smallwarsjournal.com/author/gian-gentile>>, and. As of 2012, an increasing number of junior and midgrade officers with combat service in Afghanistan are agreeing with Col. Gentile, while some experts in various think tanks continue to push COIN.

Military Review



Tired of waiting between issues for great articles?

You no longer have to—MR Spotlight is online now! This new feature publishes articles bi-weekly, so you now have access to more information more often! Check out our most current and previous articles now on our website! Go to <http://usacac.army.mil/CAC2/MilitaryReview/index.asp> and click on the "MR Spotlight" link to get started.

Want to comment? *Military Review* is on Facebook and Twitter.

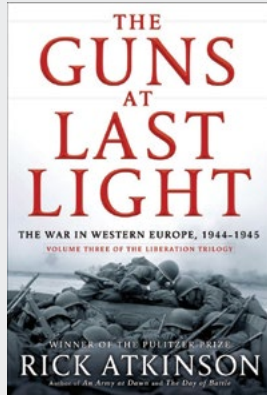
The official *Military Review* Facebook and Twitter sites are now available for readers to comment on the overall layout, design, or content of the magazine. We also strongly encourage professional discussion and debate on all articles published in *Military Review*. To comment, go to our webpage at <http://militaryreview.army.mil/> and click on the Facebook icon, or reach out to us on Twitter at [http://twitter.com/ @MilReview](http://twitter.com/@MilReview).

"Military Review is an important forum that helps shape the dialogue of our profession."

—GEN Raymond T. Odierno

THE GUNS AT LAST LIGHT

The War in Western Europe 1944-1945



Rick Atkinson, Henry Holt and Company,
New York, 2013, 896 pages, \$40.00

Col. AM Roe, Ph.D., British Army

NEARLY TWO DECADES AGO, Rick Atkinson embarked on a Herculean venture to retell the narrative of the Allied forces in Europe and North Africa during World War II. The project, consisting of three linked but stand-alone volumes, was named “The Liberation Trilogy.” The first book in the set, *An Army at Dawn: The War in North Africa, 1942-1943*, was published in 2002. Lauded by reviewers and historians alike, it won a Pulitzer Prize for history. The second volume, *The Day of Battle: The War in Sicily and Italy, 1943-1944*, appeared in 2007. It was likewise extolled and quickly became a *New York Times* best seller. In a review of the second book, *New York Times* book critic William Grimes referred to the then-unfinished trilogy as “A triumph of narrative history, elegantly written, thick with unforgettable description and rooted in the sights and sounds of battle.” The long-awaited final tome, *The Guns at Last Light: The War in Western Europe, 1944-1945*, was released in 2013. The third volume describes the struggle for Western Europe, the end of the Third Reich, and the defeat of Nazi forces. From Normandy to Berlin, the book uncovers the hardships, exhaustion, and sheer horror of warfare in the European theater of operations. It also describes in uncompromising detail the contentious Anglo-American relationship, the Blitz in England, the liberation of Paris, the horror of the labor camps, and the coming of age of the American warfighting machine. By 1944, the American military was no longer the untrained apprentice.

Atkinson’s first two books described how Allied forces fought through the challenging conditions of North Africa and Italy to the threshold of victory. *The Guns at Last Light* takes forward the narrative from D-Day through the eventual liberation of Europe and the restoration of freedom to the continent.

Col. Andrew Roe currently commands the British Army’s Operational Training and Advisory Group (OPTAG). He previously commanded 2nd Battalion, The Yorkshire Regiment (Green Howards) in Cyprus, and has held various command and staff positions in Northern Ireland, Germany, Bosnia, Afghanistan, the Falkland Islands, and Iraq. He is a graduate of the U.S. Army Command and General Staff College and the School of Advanced Military Studies, Fort Leavenworth, Kan. Col. Roe has a Ph.D. from King’s College London and is the author of Waging War in Waziristan: The British Struggle in the Land of Bin Laden, 1849-1947.

Atkinson is right to dwell on Operation Overlord, the ambitious air and sea assault of Normandy, in the early pages of his final volume. It was here that Dwight D. Eisenhower, the Supreme Allied Commander, earned his spurs—planning and executing a complex operation fraught with difficulties. Six thousand ships and landing craft—including 700 warships—and 150,000 men, undertook the greatest amphibious invasion ever mounted. American casualties were predicted to reach 12 percent of the assault force alone, with the 1st Infantry Division estimating that under “maximum” conditions, casualties could reach 25 percent. Eisenhower needed to mitigate factors such as surprise, weather, and tidal conditions. Because of bad weather, he made the key decision to push back the operation 24 hours to 6 June 1944. Any delay thereafter would risk delaying the operation until the next full moon in July.

An essential ingredient of the operation was a comprehensive deception plan—embellished by a network of British double agents—that persuaded German intelligence the main invasion would occur across the Pas de Calais. The clever deception worked, as Atkinson observes, diverting the German 15th Army—which could have acted decisively in Normandy against Allied forces. Although Operation Overlord helped set the foundations for Allied victory in Europe and was the major turning point in World War II, it came at an enormous cost to men and material. German shells and machinegun fire took their toll on the invading forces, and battles raged. Even so, the all-important conditions were set for the subsequent breakout.

Following his narrative of the Allied landings on the Normandy beaches, Atkinson expertly chronicles the major battles and activities as the Allies advanced east through Europe. He looks critically at the fighting to consolidate the beachhead before the attempted breakout by rapid armored assault, known as Operation Cobra. A description of the Falaise Pocket, the decisive engagement of the Battle of Normandy, is followed by an account of the liberation of Paris in August 1944. Operation Dragoon, the invasion of southern France in August 1944, is next to receive Atkinson’s critical gaze. Operation Market Garden, the disastrous attempt to outflank German defenses in September 1944 through Holland, is then chronicled sympathetically (Bernard Montgomery, commander of

the 21st Army Group, was held responsible for the failure). Then comes an account of the complex and exhausting fight for the Hürtgen Forest on the Belgium-Germany border in November 1944. The Siegfried Line campaign follows, before Atkinson tackles the horrific Battle of the Bulge in the Ardennes Forest—an epic of American heroism. Here, Adolf Hitler, in an all-out gamble, launched a largely fruitless counteroffensive. Hitler skillfully massed significant combat power for what Atkinson calls the “last great grapple of the Western Front.” His objective was to regain the initiative by splitting the Allied armies with a devastating armored thrust. American units were caught flat-footed, and the ensuing battle, which lasted from 16 December 1944 to 25 January 1945, was the costliest engagement ever fought by the U.S. Army. The Colmar Pocket is next to be considered, before Operations Veritable and Grenade—the crossing of the Roer in February-March 1945—are scrutinized. The last battle described is the crossing of the Rhine

...the brilliance of *The Guns at Last Light* is that it goes well beyond simply recording renowned battles and events.

in March 1945. The German surrender and VE Day—Victory in Europe—conclude the historical narrative.

In many ways, the brilliance of *The Guns at Last Light* is that it goes well beyond simply recording renowned battles and events. Atkinson introduces a cast of well-known characters—and some not-so-well-known—throughout the book, ranging from celebrated military commanders to unnamed soldiers, sailors, and aviators. The reader relives the courage, fear, and determination of those who prosecuted the battle for Europe. Through these characters, the author presents interesting anecdotes and thought-provoking analyses that cause the reader to pause and reflect. Moreover, topics such as leadership, technological sophistication, and logistics catch the reader’s imagination and add real depth and quality to the explication of the major battles.

To cite an example, the narrative describes the complicated and often fractious relationship between three of the greatest World War II commanders, Dwight D. Eisenhower, Bernard Montgomery, and George S. Patton. As Atkinson uncovers, grumbling, backbiting, and spitefulness were a routine part of the Anglo-American relationship and everyday coalition life. However, it is the tension between Montgomery—one of the most controversial leaders of World War II—and Eisenhower—the Supreme Allied Commander and Montgomery’s overall boss—that is most evident throughout the manuscript. The two did not start their relationship well. Montgomery thought Eisenhower did not fit the mold of a battlefield general. At their very first meeting, Montgomery chastised Eisenhower, a chain smoker, for lighting a cigarette in a conference room. Eisenhower never forgave Montgomery for the outburst, and the fallings-out between the two only grew worse. Montgomery dismissed Eisenhower’s initial plan for the invasion of Normandy with brutal candor, and the relationship continued to deteriorate beyond D-Day as the Allies advanced through Europe.

Although a great coalition leader (Allied unity remained the central principle of his command), Eisenhower was no strategist. Furthermore, he had proved himself to be an indifferent commander in Tunisia and Sicily. He was also cautious and prone to remaining in the rear. He often ignored logistical needs. All told, his generalship was vulnerable to external criticism. Although a good staff officer of great intelligence, Eisenhower was viewed as a “lightweight” by the unreasonably critical and conceited Montgomery.

Montgomery, as Atkinson illustrates, would often besiege Eisenhower with tactical schemes and proposals, articulated in long correspondence. Montgomery firmly believed that Eisenhower knew little about strategy and that he was an indifferent supreme commander. He particularly detested Eisenhower’s broad-front operational concept in Europe; Montgomery believed in concentrating effort in a “single thrust.” Montgomery’s arrogant intractability, numerous tactical shortcomings—and there were a good number—and smug claims finally undermined the Anglo-American relationship. It is little surprise that he drew considerable criticism. Omar N. Bradley was quick to fault Montgomery

for various sins but, as Atkinson notes, even Bradley had his shortcomings: “battlefield clairvoyance, which he [Bradley] had occasionally displayed as a corps commander in Tunisia and Sicily, often eluded him as an army group commander.” Nobody was faultless or immune from criticism. Toward the end, Eisenhower paid minimal attention to Montgomery’s pleas, and the two armies largely operated independently, despite attempts by Winston Churchill to repair friendships. Operation Market Garden, beset with intelligence shortcomings, haphazard execution, and indifferent generalship, was the last occasion of the war when Eisenhower accepted a strategic tender from Montgomery without detailed cross-examination.

The French—and particularly Charles de Gaulle—proved similarly challenging, notes Atkinson. Eisenhower told George Marshall: “Next to the weather, the French have caused me more trouble in this war than any other single factor. They even rank above landing craft.” The cohesion and internal coherence of the Allied coalition were the keys to success, and this was where Eisenhower’s hidden-hand leadership was that of a master craftsman. Churchill wisely recalls, “There is only one thing worse than fighting with Allies, and that is fighting without them.”

Such frictions were inevitable. Commanders at all levels were tired, dispirited, short of ideas, and often bad-tempered. Many were ill or weakened by anxiety. Youthful expressions were gone, replaced by the creases of tension and capricious behavior. Atkinson notes that even the seemingly indefatigable Churchill became ever more erratic and unbalanced—obsessed with inconsequential detail. Lt. Gen. Courtney H. Hodges, commander of First Army (America’s largest fighting force in Europe), was “worn by illness, fatigue, and his own shortcomings.” Although peevish and insulated, as well as lacking in dynamism and imagination, his decision making had become increasingly incoherent and unreasonable. “When the frayed commander of the 8th Division requested brief leave after his son was killed in action, Hodges sacked him,” Atkinson notes. Such irregular behavior was hardly surprising. The pressure of command, particularly considering Allied losses, was enormous. Of the 156,000 men who took part in D-Day, 3,000 Allied troops died, with a further 9,000 wounded or missing. In the Hürtgen Forest alone, one battalion in

the 110th Infantry was reduced to 57 men even after being reinforced. Losses degraded the 112th Infantry from 2,200 to 300. In less than three months, six U.S. Army infantry divisions were engaged in the Hürtgen Forest, plus an armored brigade, a Ranger battalion, and sundry other units. In total, 120,000 soldiers sustained 33,000 casualties. It is little wonder that commanders and soldiers became unhinged by constant war, mounting casualty figures, and the innumerable atrocities they came across. At Natzweiler, American soldiers overran their first concentration camp. Most of the 17,000 inmates were still alive, but clear evidence of atrocity remained—a sobering sight that was telegraphed quickly across the First Army. Atkinson observes that as the campaign progressed, enemy prisoners were beaten to obtain intelligence, captured villages were rampaged, and for some, the question of killing ceased to be a moral dilemma. More of the enemy were killed, and fewer prisoners were taken. Atkinson quotes one Canadian soldier, “When the Jerries came in with their hands up, shouting ‘*Kamerad*,’ we just bowl them over with bursts of Sten [gun] fire.” A lieutenant in the 15th Infantry wrote in his diary, “Some of our best men are the most murderous.” The horrors of war make for compelling, if unsettling, reading.

Atkinson also notes that in addition to casualties from enemy action, soldiers’ foot problems plagued the American war effort in Europe. Combat boots fitted in warm weather were often too tight to accommodate more than a single pair of socks. Trench foot—a crippling injury—became epidemic as winter approached and freezing autumn rains set in. Atkinson posits that the United States was unprepared for winter campaigning in 1944. In November and December, trench foot and other cold weather health problems hospitalized 23,000 men—nearly all of them infantrymen. By late November, trench foot accounted for a quarter of all hospital admissions. It could be argued that almost nothing relating to clothing and equipment had been learned from campaigning in the Atlas Mountains of Tunisia in 1942 or the Apennines of Italy in 1943. However, while the Army had failed to pull through the lessons of cold weather injuries, it had learned to deal with combat exhaustion. Atkinson recalls, “Most patients were treated as temporarily disabled and kept close to the front, to preserve their self-respect and emotional links to

their unit.” However, despite such an approach, most experts concluded that the soldiers were “worn out for good” after 200 to 240 days of battle.

Atkinson also uncovers another interesting facet of the war as the balance of persuasion and power transitioned over the course of the campaign. After D-Day, proportions of Allied forces changed rapidly. By May 1945, the United States predomi-

America emerged from World War II, Atkinson notes, with extraordinary advantages that would ensure prosperity for decades.

nance was about three to one. Atkinson posits that “Britain’s stature and influence seemed to diminish with each new arrival of a Liberty ship jammed with GIs; the empire’s future was uncertain at best ...” Militarily, the United States was evolving from trainee status at war to full-blown professional. By war’s end, the Americans had provided more than two-thirds of Eisenhower’s 91 divisions and half of the Allies’ 28,000 combat aircraft. “Thirteen U.S. divisions in Europe suffered at least 100 percent casualties—five more exceeded 200 percent ...” The United States also shipped 18 million tons of war material to Europe. Despite the cost—roughly \$4 trillion in 2012 dollars—America emerged from World War II, Atkinson notes, with extraordinary advantages that would ensure prosperity for decades. The Russians, too, were growing in power, reach, and influence. Having quickly rolled the Eastern Front back toward Berlin, Marshal Joseph Stalin was very much at the top table during the infamous meeting at the Crimean resort of Yalta, alongside Franklin Roosevelt and Winston Churchill. Each head of state shared native shrewdness, political acumen, and a conviction that his nation was about to become a superpower—but only two would emerge from the war with this status. This was to be the end of the period of European supremacy and the British Empire.

The author is adroit at uncovering the growing military sophistication during World War II, including the cat-and-mouse game to defeat, or at least mitigate, technological advances. This was much more than the value of “Ultra” decryptions and the wider vulnerability of German radio transmissions. For example, the advanced German radar network—stretching from Norway to Spain—was bombed for a month before Operation Overlord, with key sites receiving particular attention to include intense electronic jamming. This alone was insufficient to disguise Allied intentions, and additional trickery included balloons with radar reflectors to simulate invasion ships, and metal “confetti” to mimic the electronic signature of bomber formations. Atkinson notes, “The actual Overlord fleet deployed an unprecedented level of electronic sophistication that foreshadowed twenty-first-century warfare.” Over six hundred “jammers” were distributed to disrupt search and fire control radars. However, solutions to technological advances were often more straightforward and basic. The devastating German V-1 flying bomb, which “sucked workers from office windows, incinerated mothers in grocery stores, and butchered pensioners on park benches,” is a case in point. Despite attempts to target launch areas, supply dumps, and related sites, 2,000 barrage balloons were situated carefully on the anticipated approaches to London. The hope was that their tethering cables would bring down the bombs in flight, but, instead, the Germans fitted the V-1 wings with sharp blades to cut the cables. To help counter this, Atkinson recalls, “Fighter pilots grew adept at shooting down the bombs with 20mm cannons . . . and some even learned to use their wings to create enough turbulence to send a bomb spiralling out of control.”

While Atkinson is right to dwell on the battles in France, Belgium, and Holland, he is equally prudent to discuss in detail the challenges of logistics and resupply throughout the campaign. As a wise critic once noted, strategy is for amateurs; logistics are for professionals. By September 1944, fewer than four rounds per day were available for the largest guns. Only a month later, ammunition shortfalls were truly “critical” across the front. Shortages kept American armies largely on the defensive in October: “attacks required more firepower than sitting,” and strict firing limits were placed on some divisions. Why such shortages happened is revealed skillfully in *The Guns at Last Light*. Although U.S. plants failed to

meet demand in some areas, supply routes routinely deteriorated in poor weather conditions, and cargo became jumbled and misplaced (troops regularly had to rummage through holds to find critical items).

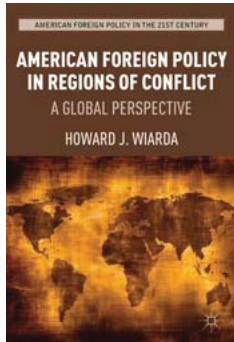
Shortages also tended to be a problem of distribution rather than supply. Fuel is another case in point. To help overcome shortages, an elaborate nexus of pipelines was built to reduce reliance on ships, vehicle transportation, and jerricans. Despite such initiatives, deficiencies were common across many items. Tent canvas was in short supply, and spare tires were stripped from vehicles in the United States and shipped to Europe. So too were uniforms, which were often “consumed” at double the War Department’s estimates. Despite this, “surfeits piled up: one quartermaster depot would report receiving 11,000 brooms, 13,000 mops, 5,000 garbage cans, and 33,000 reams of mimeograph paper.” This was all “stuff” that was not necessarily needed. Shortages were not unique to the Allies. Fuel was also a problem for the Germans. Hundreds of tanks and assault guns were immobilized on the Eastern Front because of a lack of supplies. Logistics and resupply were to pose a significant challenge throughout the campaign, often driving or impeding operations.

All told, *The Guns at Last Light* is a brilliant study of the war in Western Europe. Despite its off-putting length (almost 900 pages), it is rich with insights without getting lost in the detail. It is truly captivating and almost impossible to put it down. Simply put, Atkinson has done it again: the final volume of the Liberation Trilogy is eye opening, persuasive, brilliantly researched, and wonderfully comprehensive without being unnecessarily exhaustive. The author has tackled a bottomless subject with incredible skill, nimbleness, and aplomb. He writes stylishly and with uncommon precision and shade. The wide-ranging account is told with drama, color, and texture. Complimented by black and white photographs, exceptionally clear maps, and an invaluable wiring diagram of the Allied chain of command, *The Guns at Last Light* is a true *tour de force* and deserves to be on the bookshelf of every soldier and historian. I recommend this volume unreservedly; it stands out from the crowd. However, a single question remains: how definitive is this account? Time will tell, but I would be surprised if *The Guns at Last Light* did not prove to be an authoritative version of the Allied triumph in Europe during World War II. **MR**

AMERICAN FOREIGN POLICY IN REGIONS OF CONFLICT: A Global Perspective

Howard J. Wiarda, Palgrave MacMillan,
New York, 2012, 194 pages, \$16.50

FEATURED REVIEW



INTERNATIONAL RELATIONS PROFESSOR Howard J. Wiarda argues that academia has become so scientific in its approach to the study of international relations that mathematical models with presumed universal applicability are usurping the humanistic and environ-

mental models of U.S. engagement. Wiarda views this development as the proximate cause of a broken link between the study of international relations and the practice of U.S. foreign policy. He illustrates and addresses this problem through a succinct historical examination of U.S. foreign policy across all regions of the world. He argues that a re-infusion of comparative politics and international relations into the thought processes of foreign policymakers will make all the difference in their effectiveness. However, the strength of his argument waxes and wanes in the context of some of his regional analyses.

Starting in western Europe, Wiarda reaches some contradictory and naïve conclusions. He claims that our “cultural, language, family origins, and political institutions that were derived from and tie us to our European allies are weakening in the face of our increasingly multicultural American demographics.” Yet, on the same page, he asserts that our economic and cultural ties to western Europe will remain strong. He also claims that the demise of the Soviet Union made the NATO alliance obsolete. Yet, if one considers all that NATO has done in the Balkans, Afghanistan (establishment of the International Security Assistance Force), and most recently in Libya, Wiarda’s argument falters. Wiarda also underestimates the influence of a

resurgent Russia, whose national interests are largely at odds with those of NATO.

Most dismaying is Wiarda’s lack of objectivity in assessing the military as an instrument of foreign policy. He highlights U.S. conquest of the Philippines in 1898, the use of atomic weapons against Japan in World War II, and the failure of United Nations forces to reunify the Korean peninsula as being detrimental to America’s relationship with Asian nations. Moreover, he ignores other facts such as Japan’s treacherous attack on Pearl Harbor, the risk of a nuclear exchange with the Soviet Union, and the risk of a third world war because of the Korean issue. Wiarda incorrectly cites the Korean War’s duration from 1950-1952, when, in fact, the armistice was signed on 27 July 1953. He also erroneously cites the “defeat of U.S. forces in Vietnam” as they attempted to aid and prop up the South Vietnamese government. In fact, U.S. political will succumbed to North Vietnamese strategy rather than U.S. troops succumbing to defeat. Clearly, Wiarda fails to comprehend the use of the military as an instrument of foreign policy.

Wiarda is at his best in advocating greater cultural, historical, geographical, and demographic empathy while understanding that democratic nation building takes generations, not decades. He recommends increased immersion of students and diplomats in troubled regions to gain and apply greater expertise in the study and practice of foreign policymaking. This recommendation is of limited utility while the military must stabilize contentious regions and compensate for the dearth of qualified diplomats. After all, when U.S. lives are at stake, U.S. political will to build other nations is a steadily emptying hourglass.

**Lt. Col. Peter G. Knight, Ph.D., U.S. Army,
Princeton, New Jersey**

THE BOXER REBELLION AND THE GREAT GAME IN CHINA

David L. Silbey, Hill and Wang, New York,
2012, 273 pages, \$26.95

THE BOXER REBELLION was simultaneously a display of colonial power politics and early 20th

century multinational operations. Numerous nations converged on China in the late 19th century as the sole remaining frontier for colonial growth, dividing primarily coastal areas—captured land—for trading posts and naval resupply stations. At the same time, the long-standing governance structures based around a Chinese emperor were quickly disintegrating.

The environment of weakening local power and increasing incursion of Western cultural, religious, and military might created a backlash among disillusioned Chinese. As in the past, conservative locals rallied around groups that adhered to the religious and cultural principles they felt were slipping away; in 1900, this took the form of the Boxers. On the other side, descriptions of how colonial nations attempted, and ultimately failed, to join forces to put down the rebellion were of particular interest.

David L. Silbey comprehensively covers the events of the Boxer Rebellion, from the dynamics creating the conflagration to the Western response and the ultimate results. He obviously knows the subject well and uses a plethora of primary and contemporary sources, as well as other analyses of the events of 1900. However, as is the case with many histories written by Western authors, the sources are predominantly those of the English-speaking nations, missing the other side of the narrative.

Overall, *The Boxer Rebellion and the Great Game in China* is a great linear description of the events of 1900. However, it leaves much to be desired as a compelling story that could educate the uninitiated. I do not recommend the book for those seeking an engaging story of the Boxer Rebellion, but I do recommend it for those who are attempting to develop a comprehensive understanding of why and how this event occurred.

Capt. Nathan K. Finney, U.S. Army,
Cambridge, Massachusetts

**THE UNITED STATES
MILITARY IN LIMITED WAR:
Case Studies in Success and Failure, 1945-1999**
Kevin Dougherty, McFarland & Co.,
Jefferson, NC, 2012, 227 pages, \$40.00

far more low-intensity conflicts than conventional wars. Recognizing this, the 1993 edition of U.S. Army Field Manual 100-5, *Operations*, recognized a separate category known as *operations other than war*. Although this term has fallen out of favor, retired colonel Kevin Dougherty argues for the continued validity of the principles it represents: perseverance, objectivity, security, unity of effort (for coalition operations), legitimacy, and restraint.

To explore this topic, the author considers eight dissimilar military actions of the post-war era. Four generally were successful—U.S. assistance during the Greek Civil War, the 1958 intervention in Lebanon, the 1965 Dominican Republic intervention, and the 1980s confrontation with Marxist Nicaragua. Four operations failed: the pacification aspects of Vietnam, and ill-defined interventions in Beirut (1982-1983), Somalia, and Haiti. Dougherty's conclusions sometimes seem self-evident, but they are useful. The keys to success, he argues, are perseverance, objective, and sufficient security to protect the troops while helping convince the population the operation is legitimate. As in any military operation, failure to specify and focus on an achievable objective often led to disaster. In the second Beirut operation, for example, he says there was no clear mission because no political agreement existed on the ground. However, U.S. forces had to operate under restrictive rules of engagement as if they were engaged in peacekeeping.

There are a few flaws with the study. The author accepts the traditional interpretation that the Greek Civil War was a deliberate communist attempt to seize power, whereas revisionists have argued persuasively that the right wing leaders of the royal government and army were so determined to repress all leftists that they forced the leftists to revolt in self-defense. Many of the events in the book are now so unfamiliar that readers would benefit from maps for general orientation.

Such minor questions do not detract from the real value of the study. In an era when internal defense, stability, and contingency deployments remain common missions for U.S. troops, this selection of case studies correctly emphasizes the enduring issues that should guide military planning and analysis. As such, Dougherty's book is worthwhile reading for professional soldiers and the general public.

Col. Jonathan M. House, U.S. Army, Retired,
Fort Leavenworth, Kansas

THROUGHOUT ITS HISTORY, and especially since 1945, the U.S. military has engaged in

**ASIA'S CAULDRON:
The South China Sea and
the End to a Stable Pacific**

Robert D. Kaplan, Random House, New York, 2014,
189 pages, \$29.00

GEOGRAPHY MATTERS. IN *Asia's Cauldron: The South China Sea and the End to a Stable Pacific*, Robert D. Kaplan uses a realist's lens and a historian's nuance to remind the reader that while globalization is a concept, geography is a fact. Kaplan believes geography is essential to analyzing the present and predicting the near future of the South China Sea. This region cannot be ignored because an astonishing amount of shipping passes through it. It is the "demographic cockpit of the globe," and there is no balance of power. China is a giant among significantly weaker nations.

Kaplan convincingly argues that geography informs world views. Specifically, a nation's relationship to three archipelagos (the Pratas, Parcels, and Spratlys) profoundly affects its foreign policy paradigm. Claimed by nearly everyone, these islands present a challenge that the United States and Asian nations will face. It is not simply about who wins territorial claims, but it is about world order and international norms versus military might (the Melian dialogue comes up frequently).

The bulk of Kaplan's work focuses on how other nations will deal with China and its "nine-dotted line"—the line that illustrates China's audacious claim to most of the South China Sea. Kaplan tours the nations who contest China's claim to see if they will be able to back up their contentions with more than rhetoric. Kaplan is at his weakest in this section, where he tends toward overgeneralizations and assessments made largely from observing luxury shopping malls and official functions. Still, the historical and cultural bits are interesting. They build to Kaplan's assessment that no other Southeast Asian nation is capable of contesting China.

Enter the United States, which at present stands to defend the status quo. Yet, if China's growth continues, China eventually will be able to replace the United States and determine the regional order.

Kaplan offers two possibilities for how this transfer of power could play out. First, if U.S. power quickly and significantly declined in the region, the region would "Finlandize." By this, Kaplan means that China's military might and the region's economic dependency on China would cause other South East Asian nations to "quietly be captured by China without the latter needing to invade."

Kaplan hopes for a second possibility. In this version, the United States would use its military dominance to encourage adherence to international norms. The United States would pressure China into playing by the rules (such as submitting its territorial disputes to international arbitration) while simultaneously encouraging other Southeast Asian nations to create diplomatic agreements until their collective strength could balance against China's. However, Kaplan has a realist's skepticism of legal frameworks, and he seems prepared to bow to the inevitable arc of history: China will dominate the region. While the vast South China Sea may be "a barrier to aggression," it offers no promise of effective U.S. influence.

This book is refreshingly clear. While the reader may disagree with the thesis that geography constrains policy, Kaplan's analysis is so strong that it is at least worthy of a good rebuttal from another perspective. Moreover, if the international relations aspect is not enough to interest the military-minded reader, Kaplan's perspective on the relevance of land forces will certainly drum up equal parts interest and inter-service rivalry. "Europe is a landscape; East Asia is a seascape." Because of this incontrovertible fact, Kaplan believes the difficulty of occupying land means that rational nations will opt for cheaper forms of power projection, namely sea denial. And Kaplan believes Asian nations are nothing if not rational.

**Capt. Roxanne E. Bras, U.S. Army,
Southern Pines, North Carolina**

**COUNTERINSURGENCY:
Exposing the Myths of the New Way of War**
Douglas Porch, Cambridge University Press Cam-
bridge, 2013, 434 pages, \$27.99

WHAT DOES IT look like when a good historian gets mad? This book offers at least one answer. The author, Douglas Porch, is an experienced and

respected military historian and author of well-regarded books on conventional warfare (such as *March to the Marne* and *The Path to Victory*) and colonial warfare (such as *The Conquest of the Sahara* and *The French Foreign Legion*). However, he opens his newest book by recalling a promising former student at the Naval Postgraduate School who was killed in a “green-on-blue” incident in Afghanistan, a war Porch describes as a “murderous errand equipped with a counterfeit doctrine that became the rage in 2007 following the publication of FM 3-24, *Counterinsurgency*.” Clearly, Porch is not a fan of counterinsurgency doctrine and its modern evangelists. Nor does he make his case in the nuanced, cautious tone of most academic scholarship.

The narrative presents a series of case studies going back to the 18th century. The focus is on the experiences of the British, French, and U.S. militaries, starting with France’s ruthless suppression of the royalist revolt in the Vendée in 1793, and extending up to the current war in Afghanistan. From these cases, he argues that the whole concept of “small wars” and counterinsurgency is based on a mythology produced “by shoddy research and flawed, selective analysis of cases.” From the false claims of French colonial officers who conquered Algeria in the 19th century, to the “triumphalism” of those who, like Tom Ricks, celebrated the “surge” in Iraq in 2007, the historical record has been pillaged and perverted to use counterinsurgency as a toolbox of surefire techniques to spread the benefits of Western culture, wealth, and political values. In Porch’s view, such history is either foolish self-delusion or outright deceit.

Not surprisingly, Porch gives special attention to well-known 20th century insurgencies such as the unhappy French experience in Algeria, the uncertain British approach to Northern Ireland, and the U.S. failure in Vietnam. In these cases and many others, Porch discovers a familiar pattern—apparent success at the tactical level tended to disguise strategic failures. Moreover, all too frequently, a “hearts and minds” approach served as a smokescreen for extra-legal brutality. Even the British and their reputation for skill in “aid to civil authority” proved, in Porch’s view, incapable of real institutional learning, with their muddled efforts in southern Iraq providing the most recent evidence. The narrative makes for grim reading, salted with occasional flashes of humor. T. E. Lawrence, for example, is mocked as “Dances with Camels.”

The deeper one gets into the book, the more Porch’s style descends from historical analysis to a sort of rant. By the time he turns his attention to the war in Iraq, his attacks extend beyond past proponents of counterinsurgency to denunciations of hero-worshipping journalists, religious fundamentalists, neo-imperialists, stupid Army generals, and even fellow faculty members at the Naval Postgraduate School. At one point, he even resorts to using “The Daily Show” as a footnote. Very odd. Nevertheless, the book has made its way onto the Chief of Staff of the Army’s new professional reading list. Its inclusion there suggests either (1) a bold willingness to endure Porch’s scathing criticism of Army leadership and doctrine, or (2) that no one on Gen. Odierno’s staff has read it. To be clear, for all its angry and sometimes repetitive tone, the author provides an impressive review of the newest scholarship on “small wars.” If approached with some reservations, the book serves as an important and entertaining counterweight to overzealous advocates of modern counterinsurgency. I cautiously recommend this book for those curious about the future of the counterinsurgency debate.

Scott Stephenson, Ph.D.,

Fort Leavenworth, Kansas

THE GREAT WAR:

A Combat History of the First World War

Peter Hart, Oxford University Press, New York, 2013,

522 pages, \$34.95

WE ARE APPROACHING the centennial of the beginning of World War I. This may be a time when a war that has faded from broad consideration rebounds into consciousness. *The Great War: A Combat History of the First World War* is a good place for the military professional to become familiar with World War I military operations. Peter Hart set about to create an operational history that would cover the globe for the duration of the war, from 1914 to 1918. Despite the immense challenge of the task, he has succeeded.

Hart is an oral historian at the Imperial War Museum in London. His previous book, *The Somme: The Darkest Hour on the Western Front*, began a reassessment of operations in a way that challenged prevailing opinion. In *The Great War: A Combat History of the*

First World War, Hart establishes a framework of leadership, equipment, tactics, and operational context as he traces the battlefield results. By analyzing the interplay of new weapons, evolving tactics, and command decisions, he traces the contours of a titanic struggle. Military leaders strove valiantly to adapt and to escape the confines of total war in an environment that challenged their ability to keep up.

Hart selects quotations from key players, from general to private, throughout *The Great War*, based on his knowledge of first-hand sources. These quotations adeptly illustrate his points of emphasis and add verve to the narrative. By capitalizing on his position as oral historian, Hart plumbs the thinking of military leaders and challenges many prevailing opinions about the adaptability of command and tactics during the war. He revisits many failed decisions, to illuminate their causes, but also provides context that reveals how the reactions of military leaders were reasonable even when they failed. Hart at least makes the challenges of adaptation and failures in command more understandable.

Hart includes the peripheral theaters of war, such as Salonika, Mesopotamia, the Sinai, and Palestine, but not in detail. Despite this, *The Great War* serves as a primer for those who have never read much about the periphery of this worldwide conflict. He provides thorough treatments of the western and eastern fronts and the war at sea. He is most successful in levels of detail and nuance in explaining the western front, as we might expect from his background and previous writing.

The book progresses by theater over time. It includes representative photographs and a map of each theater at the front of the book. This reviewer found the absence of operational maps to parallel the discussion in each chapter to be at least a distraction, though it appears to be a conscious editorial decision. The narrative would be improved by adding sketch maps to illustrate the operational movements being so carefully described.

The Great War may not satisfy the widely read World War I historian in search of new, substantial arguments with compelling proofs, but it will well serve the military professional who desires to understand World War I in a tactical, operational, and human sense, on the eve of the centennial of the conflict.

**Col. Dean A. Nowowiejski, Ph.D., U.S. Army, Retired,
Fort Leavenworth, Kansas**

AMERICAN SNIPER, Memorial Edition

Chris Kyle with Jim DeFelice and Scott McEwen,
Harper Collins, New York, 2013
466 pages, \$29.99

A*MERICAN SNIPER* was originally published in 2012. This memorial edition follows author Chris Kyle's murder by a disturbed ex-marine he was trying to help and includes tributes from friends, family, and fellow warriors. Each poignant entry reveals much about Kyle and the effect he had on others. Because Kyle worked in the special operations community, his challenge was to write an informative and relevant book without saying too much. Though this story will likely satisfy readers wanting a broad description of life as a Navy SEAL (sea-air-land team) sniper, it may disappoint others wanting a vividly told, detailed story.

Chris Kyle was a sniper assigned to SEAL Team 3, stationed in Coronado, Calif. He faced a significant hurdle in writing *American Sniper*. Special operations forces are often called the silent professionals, and they expect their members to avoid the spotlight and say little to nothing about their activities. Kyle cannot speak specifically of his fellow SEALs. Though he does provide group photos, the pictures of all living members are blacked out. Names are almost never mentioned. This is clearly the right approach, yet the requirement for secrecy makes the book, at times, read like a redacted report. Because of the need for security, the Department of Defense and the Navy review books such as this to ensure they avoid presenting details of classified military operations. Readers of *American Sniper* must keep this limitation in mind.

With 160 confirmed kills, Kyle was the most lethal sniper in U.S. military history, but he was quite humble about his reputation and ability. By his own admission, he was not the best marksman, though a confirmed kill at 2,100 yards suggests he must have been enormously skilled. Further, he suggests that his role, providing overwatch for a number of different units from different services, allowed him far more opportunities to engage the enemy than many of his legendary predecessors experienced. He is matter-

of-fact in describing his job—he killed the enemy to protect his fellow sailors, soldiers, and marines.

The book has shortcomings, though they are minor and understandable. The author speaks little about sniper tactics, techniques, and procedures for obvious reasons, yet discussion of these intricacies would greatly interest most readers. Most descriptions are generic. The unit made contact, an insurgent appeared, and Kyle delivered the killing shot. There is little in the way of psychology except for a short discussion on the challenge of the first kill and how some snipers experience slumps. Many readers might wonder why a person would wish to be a sniper or what makes a sniper different from other close combat warriors. As for tactics, how does a sniper gain the edge when dueling with an enemy sniper? Discussion of tactics is minimal.

Kyle's opinions on how recent wars have been fought make the book interesting and relevant. Though he does not belabor these points, he offers insight into the mind of the warrior in direct contact with the enemy. For example, he wholly disagreed with "putting an Iraqi face on the war," claiming that the idea was "garbage." He believed that training the Iraqi force while trying to win was preposterous, that the United States should first win the war and then worry about training the host-nation forces. Presumably, he is not alone in that viewpoint.

Further, Kyle seemed to think little of winning hearts and minds; he maintained that cooperation occurred in Ramadi only after U.S. forces had killed massive numbers of combatants. Once it was clear U.S. forces "meant business," the tribal leaders threw out the insurgents and cooperated. Kyle suggests that the United States could have killed its way to victory. This is an interesting point and worthy of consideration. Many strategic leaders repeat the claim that such an approach cannot succeed. Yet, if the soldiers on the ground disagree, we have at a minimum a failure to create shared understanding—a requirement for successful mission command.

Despite the book's limitations, Kyle tells an interesting and important story. He is honest and self-effacing, candidly discussing marital challenges, the stress of his divided loyalty between family and SEAL team, and his daughter's health scare. His point of view, one seen through a high-power scope mounted on a .300 Winchester Magnum rifle, comes across clearly. To use Chris Kyle's famous motto,

"Despite what your mamma told you, violence does solve problems."

**Lt. Col. Jim Varner, U.S. Army, Retired,
Platte City, Missouri**

BROTHERS AT WAR:
The Unending Conflict in Korea
Sheila Miyoshi Jager, W.W. Norton and Company,
New York, 2013, 605 pages

FUTURE HISTORIANS MAY one day recall the Korean War as the world's longest, strangest conflict. In *Brothers at War*, Sheila Miyoshi Jager recounts seven decades of bloodshed on the Korean Peninsula. She begins with the brutal civil war that followed World War II and continues through the North Korean invasion of 1950 and the three subsequent years of open warfare. She concludes with the current standoff between the brutal and unpredictable regime in Pyongyang and its uneasy neighbors, most notably the prosperous Republic of Korea.

The author, a professor of East Asian studies at Oberlin College, focuses the first half of her study on the devastating conflict between United Nations and communist forces. Jager's version briefly summarizes the war's key military actions. She incorporates keen observations on the political and cultural aspects of the war, particularly its waning U.S. support, the lengthy and frustrating cease-fire negotiations, and the difficult relationship between Korean premier Syngman Rhee and his United Nations allies.

These are familiar topics to Western scholars and history buffs. However, Jager also examines many of the war's less publicized issues, such as the plight of South Korean civilians hastily drafted and thrown into combat with U.S. units, the alleged war crimes by both sides, the mistreatment of prisoners of war, and the increasing role of South Korean military forces during the course of the war.

Delegates finally agreed to a cease-fire in July 1953, formally ending hostilities between communist and United Nations forces on the Korean peninsula. As Jager illustrates, the 60-year-old cease-fire has proven anything but peaceful. Subsequent decades have been marked by a seemingly endless series of bellicose and occasionally bloody incursions by the North Korean

regime, most recently its March 2013 renunciation of the cease-fire agreement itself. The author presents these events within the context of the North Korean regime's continuing struggle for legitimacy, internally and in the international community.

Meanwhile, the war's legacy has influenced political and economic development significantly on both sides of the demilitarized zone. Additionally, it has shaped events far beyond the Korean Peninsula. These include the collapse of Sino-Soviet relations, the rapprochement between Japan and South Korea, and the U.S. intervention in Vietnam—which included a significant contingent of South Korean combat troops.

There are, unavoidably, some gaps in Jager's account, most notably the decline and fall of the Rhee regime in the years after the cease-fire. Still, the author successfully presents seven decades of history within a single volume, and she paints a particularly sharp portrait of the personal and political conflicts within the communist bloc.

Jager narrates these developments in clear and elegant prose, supported by an impressive array of primary and secondary sources from Western and Eastern archives. Several dozen photographs and maps illustrate the narrative, while 91 pages of informative end notes provide additional details worthy of attention from scholars and popular audiences alike.

Sixty years after a cease-fire nominally ended the Korean War, military and political analysts still consider the Korean demilitarized zone to be the most dangerous place on earth. In *Brothers at War*, Sheila Myoshi Jager provides readers with a work of remarkable scholarship that vividly illustrates why.
Lt. Col. William C. Latham Jr., U.S. Army, Retired,
Colonial Heights, Virginia

HANOI'S WAR:
An International History of the
War for Peace in Vietnam
Llien-Hang T. Nguyen,
The University of North Carolina Press,
Chapel Hill, 2012, 464 pages, \$34.95

THIS IS ONE of the most important books on the Vietnam War to come along in some time. Llien-Hang T. Nguyen is a Vietnamese American

who was born in Saigon in 1974. She and her family fled to the United States in 1975 as their country fell to the communists. Now an associate professor at the University of Kentucky, Nguyen, who has “kin who served on both sides,” seeks to come to grips with a war that to her was “both distant and proximate.” She focused her research efforts on determining “how certain leaders made specific decisions ... that led to the deaths of approximately 58,000 Americans and an estimated 2-6 million Vietnamese.”

Using unprecedented access to the Foreign Ministry Archives in Hanoi and extensive interviews with many of the principals in Vietnam, Nguyen has produced a remarkable piece of scholarship that serves to correct many of the commonly held ideas about how the war was conducted on the other side. In most historiography on the war, the key players in North Vietnam are Ho Chi Minh and Vo Nguyen Giap. Nguyen demonstrates convincingly that the real power in Hanoi was held by the “comrades Le”—Party Secretary Le Duan and his closest ally, Le Duc Tho, who together controlled Vietnam for over half a century. Nguyen charts the rise of Le Duan from his early days in the struggle against the French in the First Indochina War to his ascendancy as First Party Secretary in 1959. Once in office, Le Duan used the police and intelligence services to eliminate rivals and consolidate his control of both the party and the state. Fully in charge, Le Duan prosecuted a total war against South Vietnam and the United States, always focused on the desired end state, which was a reunified Vietnam under communist control. In order to sustain the war effort, Le Duan skillfully walked a tight rope between the Soviet Union and China, determined to maintain “equilibrium in the Sino-Soviet split” so that he could ensure his partners provided Hanoi with the materiel and support needed to fight the war.

Le Duan was single-minded; his intense focus on the end state sometimes blinded him, particularly when he held fast to the idea of a general offensive followed by a general uprising. This approach, particularly with regard to the 1968 Tet Offensive and the 1972 Spring-Summer Offensive, often led to “staggering losses” for the North Vietnamese side. Yet, Le Duan never wavered. Failing to win the war outright on the battlefield, the “comrades Le” prosecuted the strategy of *dam va danh* (“talking while fighting”), an approach that eventually resulted in the signing of the Paris Peace Accords and the subsequent withdrawal

of U.S. troops from Vietnam. From that point on, it was just a matter of time until Hanoi achieved ultimate victory.

This groundbreaking book provides a unique and compelling perspective on the war. It clears up many misconceptions about how Vietnam fought the war. Extremely well written and meticulously researched, the book would be helpful for anyone trying to understand the complexities of this contentious conflict that continues to influence the United States and its armed forces.

**Lt. Col. James H. Willbanks, Ph.D., U.S. Army,
Retired, Fort Leavenworth, Kansas**

A MILITARY HISTORY OF THE COLD WAR: 1944-1962

Jonathan M. House, University of Oklahoma Press,
Norman, 2012, 546 pages, \$40.50

ALTHOUGH DR. JONATHAN House's *A Military History of the Cold War: 1944-1962* focuses on the operational level of war, there may be no clearer, more comprehensive evidence for Clausewitz's contention that "war is but the continuation of politics by other means" than this book provides. In conflict after conflict, the reader sees that if one side did not achieve its desired end state, the reason was that it failed to address the political components of the conflict sufficiently.

House shows that no military action has value in and of itself. What matters instead are political questions such as these: Does a military action create more enemies than it eliminates from the battlefield? Does it gain support from allies? Does it drive a wedge between the enemy and its base of popular support? Does it help address legitimate political grievances? Does it increase the likelihood of broader war, or worse, nuclear holocaust? These things really matter in war, especially in the nuclear and information age.

House shows that the Cold War provides especially fertile ground for the study of counterinsurgency. This stands to reason, since the United States and the Soviet Union—the two great nuclear superpowers of the conflict—avoided direct confrontation, relying largely instead on proxies

to fight each other. House discusses 13 insurgencies in detail. After reading these case studies, the counterinsurgent comes away with a better understanding of which military actions could be successfully employed again and which, due to local peculiarities or changes in global conditions, only could have worked when and where they did.

Additionally, the book enhances the military student's understanding of the current security environment. For example, the British Army's counterinsurgency experience in the 1960s in what was then called Aden illuminates the outlook and motivations of warring parties in Yemen today.

Another great strength of the book is its in-depth treatment of the Soviet Union. House is a retired military intelligence colonel who spent more than a decade of his service during the Cold War. He has co-written four books on the largest German and Soviet battles of World War II. His knowledge of the Soviet Union is deep. This, coupled with the fact that many primary Soviet sources from this period only recently became accessible to Western historians, ensures that the U.S. and Soviet perspectives are balanced and the sections discussing the Soviet Union are fresh and interesting.

The reader needs to be prepared, however, for some distressing discoveries. The reader may be shocked to learn, for instance, that the Department of Defense deliberately exposed 250,000 service members to varying levels of radiation over two decades to ascertain radiation's effects. They also may be surprised to learn just how close our country came to initiating nuclear war. The world's close call with nuclear war during the Cuban Missile Crisis is well known. Less well known are narrow escapes such as the Joint Chiefs of Staff recommending nuclear strikes against China five times during the 1958 Taiwan Straits crisis.

In short, the Cold War deserves to be the subject of more study at senior service schools, military academies, and Reserve Officer Training Corps programs, and this book deserves to be a textbook for any course on the conflict. In this book, instructors and students can find measured, verifiable, and insightful conclusions regarding the Cold War, along with lessons still applicable to conflict today.

**Lt. Col. Douglas A. Pryer, U.S. Army,
Fort Huachuca, Arizona**

PERSUASION AND POWER:

The Art of Strategic Communication

James P. Farewell, Georgetown University Press,
Washington, DC, 2012, 270 pages, \$29.95

AMERICANS' ABILITY TO market everything from McDonald's to the latest worldwide fad is unparalleled in history. Yet, the United States is challenged when it comes to marketing itself. James Farewell, an internationally recognized expert in strategic communication and cyberwarfare, has written an insightful work on what strategic communication is and why we as a nation are failing at it.

Farewell explores the U.S. government's vain quest to engage foreign audiences throughout the world. The United States often finds itself in "the react mode" in response to more effective and efficient efforts of state and nonstate actors. The nation's inability to communicate strategically reflects a lack of emphasis by our senior leaders, parochial turf wars between agencies, and the absence of a single comprehensive approach. Farewell describes the view held by many in the U.S. government, especially in the Department of Defense, that strategic communication is a process rather than an art. Farewell counters that communication is partly a process but we need to think of it more as an art. The Department, moreover, exacerbates its strategic communication problems by conceiving of strategic communication in terms of inform and influence. The author counters that smart public affairs is about influence. He states that "smart public affairs always seeks to influence, if for nothing else than to bolster credibility."

Farewell proposes viable solutions to maximize the effectiveness of U.S. strategic communication efforts. These include centralizing control of strategic communication for the U.S. government within the White House, revising current definitions (which are inconsistent and undercut our creditability), improving military training in information operations, improving State Department efficiency, measuring effectiveness better, holding people accountable, and realizing that strategic communication equals military strategy.

The strength of *Persuasion and Power* is its exhaustive research, demonstrated by vignettes that

illustrate successful strategic communication efforts and their benefits, as well as failures and their consequences. Scholars and strategic communicators alike will be impressed with Farewell's extensive research and proposed solutions to enhance strategic communication. *Persuasion and Power* is a must read for those with an interest in strategic communication or marketing.

Jesse McIntyre III,
Fort Leavenworth, Kansas

THE SECOND NUCLEAR AGE:

Strategy, Danger, and the New Power Politics

Paul Bracken, Times Books, New York, 2012
306 pages, \$29.00

THE ARMY STOPPED thinking about nuclear weapons soon after the weapons were removed from its inventory in the early 1990s. Few in the ranks regretted this parting. A decade of humanitarian interventions, followed by another of counterinsurgency, has further distanced the military and the nation's civilian leadership from the world of nuclear weapons, operationally and intellectually. This trend alarms Yale professor and long-time security commentator Paul Bracken. He reminds us that in spite of appeals to the "better angels of our nature" and well-intentioned nonproliferation policies, nuclear weapons have not "gone gently into that good night."

This well-structured book flows conversationally as Bracken describes the implications of the bomb's comeback and what it portends for the United States—the only nuclear power that has not modernized its arsenal. Bracken draws on history and personal experience to derive lessons related to U.S. nuclear policy and the role of the bomb during the Cold War. Several "enduring truths" remain applicable, but policymakers have failed to appreciate the meaning behind the emergence of a new nuclear paradigm.

The distinguishing feature of the second nuclear age is multipolarity. Unlike the global contest that dominated the latter half of the 20th century, the present drama plays out on a number of regional stages among diverse, independent actors—some of

whom may be inclined one day to use nuclear weapons deliberately. The fact that many have sought more “usable” weapons through advanced designs would strengthen the author’s case in this respect. However, Bracken eschews technical explanations, preferring to dwell on the complex dynamics of politics and strategy. He details the challenges of the second nuclear age in the Middle East, South Asia, and East Asia.

In pressing for “thinking about the unthinkable,” Bracken seems aware of his delicate position. Warren Kozak writes in *LeMay: The Life and Wars of General Curtis LeMay* that when Gen. Curtis LeMay joined the ticket as the vice presidential candidate in 1968, he embarrassed the Wallace campaign when he remarked on the American people’s “phobia” about the use of nuclear weapons. Even if Bracken found this phobia as unfortunate as LeMay did, he knew better than to take this tone. While no Dr. Strangelove, the author is indeed a voice crying in the wilderness. The possibility of mutual assured destruction may be remote, but the chances of regional war have grown uncomfortably higher. Possessing fewer escalation options than potential adversaries such as Russia or China, the United States stands to find itself at a disadvantage in future crises.

The country’s nuclear forces and institutions have atrophied alongside its critical thinking about nuclear-related matters. What the United States needs, asserts Bracken, is a “Nuclear Strategy 101” course to rouse the security community out of its dangerous slumber and acquaint it with managing the complexity and increased risk of a new era. As a primer to spur this reawakening, *The Second Nuclear Age* serves remarkably well.

**Lt. Col. James S. Powell, Ph.D., U.S. Army,
Washington, D.C.**

**MOMENT OF BATTLE:
The Twenty Clashes That Changed the World**

James Lacey and Williamson Murray,
Bantam Books, New York,
2013, 479 pages, \$30.00

IN *MOMENT OF Battle*, authors James Lacey and Williamson Murray tackle an interesting

endeavor—to pick the 20 battles that most affected the world. The authors undertake this task to address their concern about a trend among some U.S. academic circles—namely, the belief that “wars and military and strategic history are irrelevant to the study of the past” and that great figures of history have actually played minor roles.

The authors contend “that wars and battles have had a direct and massive impact on the course of history, one that is essential to understanding the world in which we live.” However, they agree that studying battles in isolation can be misleading. Readers must understand the cultural context in which a battle occurred.

In deciding which battles to include in the book, the authors have followed Edward Creasy’s direction in *Fifteen Decisive Battles of the World*. Lacey and Murray selected battles for their “long-term impact on the course of history,” and not for their importance to military art. Still, Lacey and Murray concede that using their criteria forced them into the “precarious game of counterfactual history,” where they had to imagine how a different outcome of a battle might have fundamentally changed the course of history. Given the number of battles throughout history, even with these criteria there is bound to be controversy in the authors’ choices. However, readers will be impressed by the authors’ logic and rationale.

For each of the 20 battles, the authors explain the cultural context at the time of the battle and the events leading up to it. They describe what was transpiring on the ground and what was going on at the critical moment in each battle. Yet, within their descriptions, the authors never lose sight of the fact that death, destruction, and sacrifice were occurring. When describing the decisive moment at the Battle of Gaugamela, the authors write that what the Persians “needed to do was find some way to maneuver. What they did do however was stand toe-to-toe against an invincible juggernaut. Darius stood in mute horrified witness as the best of Persia’s’ infantry was pulverized.”

An interesting aspect of the book is the authors’ ideas on what would have happened had the battle turned out differently. Here, the authors show true skill in leading the reader through the possible outcomes. The authors are not afraid to challenge other theories with their conclusions. For example, while

discussing the barbarian invasion, some academics claim the barbarians inflicted little damage as they moved through the Roman Empire. The authors say that “only academics who have spent their entire lives sequestered in school and with scant knowledge of the real world could gin up such nonsense.”

The book is enjoyable, well researched, and easy to read. The authors achieve their objective, and their conclusions are worthy of consideration. I highly recommend it to those interested in military history.
**Lt. Col. Robert J. Rielly, U.S. Army, Retired,
Fort Leavenworth, Kansas**

ADMIRAL NIMITZ:

The Commander of the Pacific Ocean Theater
Brayton Harris, Palgrave Macmillan, New York, 2012,
238 pages, \$26.00

A *DMIRAL NIMITZ: THE Commander of the Pacific Ocean Theater* is a welcome addition to the few studies that analyze the career of fleet admiral Chester W. Nimitz. Brayton Harris uses U.S. Naval Institute oral histories from the 1960s and 1970s and other secondary sources to compose his biography of Nimitz. He examines Nimitz’s life and naval career, particularly his service in World War II.

Harris sets the stage by summarizing Nimitz’s early years in Texas and as a student at the U.S. Naval Academy. He recounts Nimitz’s naval service from his naval academy graduation in 1905 through his assignment as the chief, Bureau of Navigation, which began in 1939. Harris tells of Nimitz’s numerous *afloat* commands, particularly those associated with submarines.

The author rightfully focuses much of the book on Nimitz’s World War II record. President Franklin D. Roosevelt personally selected Nimitz to take command of the battered Pacific Fleet at Pearl Harbor and, subsequently, the Pacific Ocean areas. As Commander in Chief, Pacific Command, and Commander in Chief, Pacific Ocean Area, Nimitz led extensive maritime efforts across the south and central Pacific through the war’s end. Harris devotes nearly half of the biography to Nimitz’s involvement in the planning and execution of operations in Guadalcanal, Tarawa, the Marianas, Philippines, Iwo Jima, and Okinawa.

In the final chapters, Harris looks at Nimitz’s role as Chief of Naval Operations, when Nimitz grappled with complex demobilization issues, unification of the services, and naval transformation in the atomic era.

Harris is at his best exploring Nimitz’s often-complex professional relationships with Admiral Ernest King, General Douglas MacArthur, Secretary James Forrestal, and President Harry S. Truman. In addition to the Naval Institute oral histories and other resources used, Harris taps E.B. Potter’s definitive biography, *Nimitz*, to convey his analysis. Harris ends his book with a bibliography that identifies key sources used throughout the study and an extensive list of the oral histories consulted for the biography.

For those looking to become acquainted with the life and career of this flag officer, *Admiral Nimitz: The Commander of the Pacific Ocean Theater* is an excellent place to start. The book is a quick, enjoyable read that carefully chronicles the leadership of this U.S. senior commander.

**Stephen D. Coats, Ph.D.,
Fort Leavenworth, Kansas**

MR WE RECOMMEND



THE GREAT WAR SEEN FROM THE AIR: In Flanders Fields, 1914–1918

Birger Stichelbaut, Mercatorfonds, Brussels, Belgium, 2014, 352 pages, \$74.81

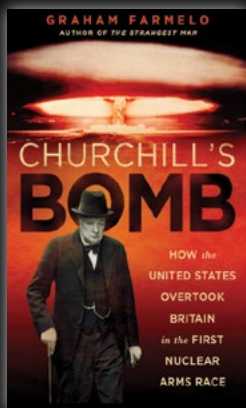
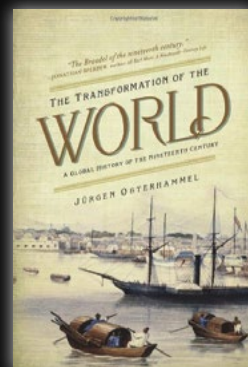
AERIAL PHOTOGRAPHY WAS a relatively new technology at the onset of World War I and was embraced as an indispensable tool of wartime intelligence by all nations involved in the conflict. This illuminating volume, the results of a collaboration between the In Flanders Fields Museum, Ypres, the Imperial War Museum, London, and the Royal Army Museum, Brussels,

features hundreds of photographic case studies, illustrating in unprecedented detail the physical extent of World War I and the shocking environmental damage it left in its wake. Supplementing aerial images with maps, documents, and photos taken from the ground, this one-of-a-kind visual record stands as an important contribution to World War I history, revealing the wartime landscape of Flanders Fields as rarely seen before. *From the publisher.*

THE TRANSFORMATION OF THE WORLD A Global History of the Nineteenth Century

Jurgen Osterhammel, trans. by Patrick Camiller, Princeton University Press, Princeton, NJ, 2014, 1,192 pages, \$29.67

A MONUMENTAL HISTORY OF the nineteenth century, *The Transformation of the World* offers a panoramic and multifaceted portrait of a world in transition. Jürgen Osterhammel, an eminent scholar who has been called the Braudel of the nineteenth century, moves beyond conventional Eurocentric and chronological accounts of the era, presenting instead a truly global history of breathtaking scope and towering erudition. He examines the powerful and complex forces that drove global change during the “long nineteenth century,” taking readers from New York to New Delhi, from the Latin American revolutions to the Taiping Rebellion, from the perils and promise of Europe’s transatlantic labor markets to the hardships endured by nomadic, tribal peoples across the planet. Osterhammel describes a world increasingly networked by the telegraph, the steamship, and the railways. He explores the changing relationship between human beings and nature, looks at the importance of cities, explains the role slavery and its abolition played in the emergence of new nations, challenges the widely held belief that the nineteenth century witnessed the triumph of the nation-state, and much more. *From the publisher.*



CHURCHILL'S BOMB: How the United States Overtook Britain in the First Nuclear Arms Race *Graham Farmelo, Basic Books, New York, 2013, 576 pages, \$21.76*

PERHAPS NO SCIENTIFIC development has shaped the course of modern history as much as the harnessing of nuclear energy. Yet the 20th century might have turned out differently had greater influence over this technology been exercised by Great Britain, whose scientists were at the forefront of research into nuclear weapons at the beginning of World War II.

As award-winning biographer and science writer Graham Farmelo describes in *Churchill's Bomb*, how the British set out to investigate the possibility of building nuclear weapons before their American colleagues. Prime Minister Winston Churchill did not make the most of his country’s lead and was slow to realize the Bomb’s strategic implications. He also failed to capitalize on Franklin Roosevelt’s generous offer to work jointly on the Bomb, and ultimately ceded Britain’s initiative to the Americans.

Development and deployment of the Bomb placed the United States in a position of supreme power at the dawn of the nuclear age. Contrasting Churchill’s often inattentive leadership with Franklin Roosevelt’s decisiveness, *Churchill's Bomb* reveals the secret history of the weapon that transformed modern geopolitics. *From the publisher.*



(U.S. Army)

Announcing the 2014 General William E. DePuy Combined Arms Center Writing Competition

How can the Army maintain its adaptability and agility and find innovative solutions to face future threats during this time of work force reductions and budget cuts?

Contest Closes 7 July 2014

1st Place \$1,000 and publication in *Military Review*

2nd Place \$750 and consideration for publication in *Military Review*

3rd Place \$500 and consideration for publication in *Military Review*

For information on how to submit an entry, go to <http://militaryreview.army.mil>

MEDAL of HONOR

WORLD WAR II KOREAN WAR
VIETNAM WAR

TWENTY-FOUR VETERANS from three wars were awarded the nation's highest military decoration, the Medal of Honor, during a ceremony at the White House on 18 March 2014.

Three Vietnam veterans—Master Sgt. Jose Rodela, Sgt. 1st Class Melvin Morris, and Sgt. Santiago J. Erevia—received their awards from President Barack Obama. Posthumous awards were presented to the families of the other 21 recipients.

The medals were an upgrade of previously awarded Distinguished Service Crosses for various acts of uncommon bravery during World War II, the Korean War, and the Vietnam War. The upgrades resulted from a congressionally mandated review of awards to ensure heroism of veterans was not overlooked due to prejudice or discrimination. The recipients were of Hispanic, Jewish, and African-American descent.

President Obama said during his remarks, “For their gallantry under fire each of these soldiers was long ago recognized with the Army’s second-highest award—the Distinguished Service Cross. But ask their fellow veterans, ask their families, and they’ll tell you that their extraordinary deeds merited the highest recognition. And today, we have the chance to set the record straight.”

Secretary of Defense Chuck Hagel inducted the soldiers into the Pentagon Hall of Heroes the next day. Secretary Hagel said the 24 soldiers’ “acts of gallantry in battle merit our highest recognition.”



Sgt. 1st Class Melvin Morris, Master Sgt. Jose Rodela, and Sgt. Santiago J. Erevia, stand in the East Room of the White House, Washington, 18 March 2014, after receiving the Medal of Honor for their heroic deeds during the Vietnam War.

WORLD WAR II



Pvt. Pedro Cano



Pvt. Joe Gandara



Staff Sgt. Salvador J. Lara



Staff Sgt. William F. Leonard



Master Sgt. Manuel V. Mendoza

KOREAN WAR



Sgt. Alfred B. Nietzel



1st Lt. Donald K. Schwab



Cpl. Joe R. Baldonero



Sgt. Victor H. Espinoza



Sgt. 1st Class Eduardo Corral Gomez



Pfc. Leonard M. Kravitz



Master Sgt. Juan E. Negrón



Master Sgt. Mike C. Pena



Pfc. Demensio Rivera



Pvt. Miguel A. Vera

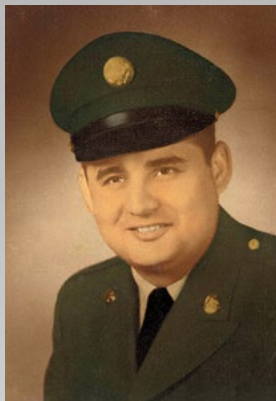
VIETNAM WAR



Sgt. Jack Weinstein



Spc. 4 Leonard L. Alvarado



Staff Sgt. Felix M. Conde-Falcon



Sgt. Ardie R. Copas



Sgt. Jesus S. Duran



Sgt. Santiago Erevia



Sgt. Candelario Garcia



Sgt. 1st Class Melvin Morris



Master Sgt. Jose Rodela