Military Review

THE PROFESSIONAL JOURNAL OF THE U.S. ARMY

NOVEMBER-DECEMBER 2020

Military Review

THE PROFESSIONAL JOURNAL OF THE U.S. ARMY

November-December 2020, Vol. 100, No. 6
Professional Bulletin 100-20-11/12
Commander, USACAC; Commandant, CGSC; DCG for Combined Arms, TRADOC:
Lt. Gen. James E. Rainey, U.S. Army

Provost, Army University, CGSC: Brig. Gen. Donn H. Hill, U.S. Army
Director and Editor in Chief: Col. Paul E. Berg, PhD, U.S. Army
Managing Editor: William M. Darley, Col., U.S. Army (Ret.)
Editorial Assistant: Chris Gardner
Operations Officer: Lt. Col. David B. Rousseau, U.S. Army
Senior Editor: Jeffrey Buczkowski, Lt. Col., U.S. Army (Ret.)
Writing and Editing: Beth Warrington; Allyson McNitt, PhD;
Crystal Bradshaw-Gonzalez, Contractor
Graphic Design: Arin Burgess
Webmasters: Michael Serravo; James Crandell, Contractor
Editorial Board Members: Col. Rich Creed—Director, Combined Arms Doctrine Directorate; Dr. Lester W. Grau—Director of Research, Foreign Military Studies Office; Col. Sam Saine—Director, Center for Army Profession and Leadership; Col. Christopher J. Keller—Director, Center for Army Lessons Learned; Howard Brewington—Deputy Director, MCCoE; Edward T. Bohnemann, Col., U.S. Army (Ret.)—Deputy, Combined Arms Center-Training; Richard J. Dixon, Col., U.S. Army (Ret.)—Deputy Director, School of Advanced Military Studies
Consulting Editors: Col. Ricardo Yoshiyuki Omaki—Brazilian Army, Portuguese Edition; Maj. Zachary Griffiths, 10th Special Forces Group (Airborne), Special Operations; Maj. Thomas Fox, International Affairs—Asian Affairs, USMA

Submit manuscripts and queries by email to usarmy.leavenworth.tradoc.mbx.armyu-aup-military-review-public@mail.mil; visit our web page for author submission guidelines at https://www.armyupress.army.mil/Publish-With-Us/#mr-submissions.

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. A limited number of hard copies are available for distribution to headquarters elements of major commands, corps, divisions, brigades, battalions, major staff agencies, garrison commands, Army schools, reserve commands, cadet command organizations, medical commands, hospitals, and other units as designated. Information on subscriptions may be obtained by consulting *Military Review*, which is available online at https://www.armyupress.army.mil/Military-Review/.

Military Review (US ISSN 0026-4148) (USPS 123-830) is published bimonthly by the Department of the Army, Army University Press, Fort Leavenworth, KS 66027-1293. Periodical postage paid at Leavenworth, KS, and additional mailing offices.

Yearly paid subscriptions are for $42 US/APO/FPO and $58.80 for foreign addresses and are available through the U.S. Government Publishing Office (GPO) at https://bookstore.gpo.gov/products/military-review-professional-journal-united-states-army.

ADDRESS CHANGES: For personal subscriptions, contact GPO at 1-866-512-1800 or contactcenter@gpo.gov. For military units and other official government subscribers, contact usarmy.leavenworth.tradoc.mbx.military-review-public-em@mail.mil.

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.

By Order of the Secretary of the Army:

JAMES C. MCCONVILLE
General, United States Army
Chief of Staff

Official:

KATHLEEN S. MILLER
Administrative Assistant
to the Secretary of the Army
2030203

Cover photo: A creative photo featuring Tech Sgt. Kyle Hanslovan, a cyberwarfare specialist serving with the 175th Cyberspace Operations Group of the Maryland Air National Guard taken 30 October 2017 in Catonsville, Maryland. (Photo by J. M. Eddins Jr., U.S. Air Force)

Next page: Army helicopters participate in an aerial gunnery event 20 July 2020 at Grafenwoehr Training Area, Germany. (Photo by Sgt. Justin Ashaw, U.S. Army)

ARMY UNIVERSITY PRESS

2020 General William E. DePuy

Special Topics Writing Competition

This year's theme was "Finding the enemy in 2035—What technological, doctrinal, organizational, or other advances or changes must we make to find our adversaries on the battlefield of the future?"

WINNERS!

1st Place

"Finding the Enemy on the Data-Swept Battlefield of 2035"

Capt. T. S. Allen, U.S. Army

2nd Place

"Human-Machine Paradox: A Balanced Approach to Finding and Fixing in 2035"

Capt. Michael P. Ferguson, U.S. Army; Chief Warrant Officer 4 Jessie R. Crifasi, U.S. Army; and Chief Warrant Officer 3 Nick Rife, U.S. Army

3rd Place

"Hunting the Adversary: Sensors in the 2035 Battlespace"

Maj. Hassan M. Kamara, U.S. Army

Honorable Mention

"Leveraging Multi-Domain Military Deception to Expose the Enemy in 2035"

Lt. Col. Stephan Pikner, PhD, U.S. Army

For information on how to submit an entry, please visit https://www.armyupress.army.mil/DePuy-Writing-Competition/.

TABLE OF CONTENTS

November-December 2020
Volume 100 ◆ Number 6

Suggested Themes and Topics

A U.S. Military Academy cadet participates in an obstacle course 20 July 2020 during training at West Point, New York. (Photo by Matthew Moeller, U.S. Army)

Large-Scale Combat Operations/ Multi-Domain Operations

- Division as a formation
- Air and antimissile defense
- Deep operations
- Information advantage/military deception
- Field Manual 3-0—Competition continuum (competition, crisis, conflict)
- Multi-domain task force
- Recon and security/cavalry operations
- Protection and security (air defense artillery, engineer, chemical, biological, radiological, nuclear, cavalry)

Joint Operations

- Air/sea/land integration
- Joint/long-range precision fires
- Air and antimissile defense
- Joint forcible entry

Europe/Central Command/ Indo-Pacific Command

- Contiguous and noncontiguous operations
- New operational environment: adversaries operating in their "near abroad" (close proximity to own borders)
- Peer and near-peer adversaries contesting U.S. joint force in all domains

Other Topics

- What must be done to adjust junior leader development to the modern operational environment?
- What logistical challenges does the U.S. military foresee due to infrastructure limitations in potential foreign areas of operation, and how can it mitigate them?
- Defending against biological warfare—examination of the war waged by other than conventional military weapons
- Military role within interagency responses to the COVID-19 pandemic and other natural or humanitarian disasters
- What is the role for the Army/Reserve components in homeland security operations? What must the Army be prepared to do in support of internal security? Along our borders?
- Role of security force assistance brigades (SFAB) in the gray-zone competition phase drawn from experience of an SFAB in Africa or Europe


BONTE

History and Heritage in the Operational Force

An Action Plan

Col. Charles R. Bowery Jr., SES, U.S. Army, Retired

History will not give us solutions to today's problems but, properly used, it will give us insight and get us to ask ourselves the right questions.

—Dr. Peter Knight, U.S. Army Center of Military History

In 1965, American author James Baldwin remarked, "The great force of history comes from the fact that we carry it within us, are unconsciously controlled by it in many ways, and history is literally present in all that we do."[1] In no organization is this statement truer than in the U.S. Army. The profession of arms carries with it an instinctual awareness of the past. Unit and individual experiences are a constant presence in the lives of Army soldiers and civilians and can be powerful tools for analysis, critical thought, self-reflection, and esprit de corps. But these tools must be built and maintained in an intentional manner if they are to be useful outside of a classroom setting. The vehicle for building a state of historical-mindedness in an Army unit is a historical program. The building blocks for a historical program include a unit historical file, a process for completing an annual historical summary, a process for maintaining unit lineage and honors, and a deliberate plan to use unit history for professional development.

The sad fact, however, is that across the Army's operating units, historical programs are in a state of increasing decay. This decay has two underlying causes, one intellectual and one structural, but the causes feed and accelerate each other. Historical instruction in Army schools and training, from Reserve Officer Training Corps and West Point precommissioning through the Noncommissioned Officer Education System (NCOES), mid-career training, and the Army War College, is rigorous, well-resourced, and highly regarded by Army senior leaders. In these environments, the value of historical analysis is a given, at least for most people. But leaders frequently struggle with transferring concepts learned in historical programs from the classroom to the operating force, where the imperatives of contingency operations, mission readiness, training, and sustainment drive everything and fill schedules. Commanders never have enough time to do everything, and they are constantly evaluating risk and prioritizing tasks. Unit historical programs usually lose in this environment because they are not seen as mission essential. This is the intellectual

Previous page: Sgt. 1st Class James Bowie (*left*) of the 138th Military History Detachment (MHD) conducts a field oral history interview with a member of 3rd Squadron, 278th Armored Cavalry Regiment, 9 April 2019 as part of an external evaluation of their training at Fort Hood, Texas. The 138th MHD of the Indiana National Guard, along with three additional MHDs from the U.S. Army Reserve and U.S. Army Forces Command, participated in the first-ever multicomponent collective training evaluation of MHDs. (Photo courtesy of the U.S. Army Center of Military History)

Col. Charles R. Bowery Jr., SES, U.S. Army, retired, is the executive director of the U.S. Army Center of Military History, Washington, D.C. He holds an MA from North Carolina State University. During his active duty career, Bowery served in Army aviation units in the United States, Korea, Germany, Iraq, and Afghanistan, where he commanded an attack helicopter battalion. He also taught military history at West Point and served on the joint staff.

cause of decay in historical programs.

As a result of this widespread perception that historical programs are not mission-essential activities, they are not resourced with time or people, leading to the structural problem of having no trained historians in command historian positions. Army Regulation 870-5, *Military History: Responsibilities, Policies, and Procedures,* which governs Army historical programs, specifies that Army units at division-level and above will have assigned command historians, either military or civilian.[2] As figure 1 indicates, however, this requirement is honored mostly in the breach, and these positions are either unfilled or eliminated from manning documents across the operational force. Only one Army division currently maintains a command historian; this is the structural cause of decay in historical programs. In three active component Army divisions, the local museum director is considered the division historian, delegating to those museum professionals an unrealistic workload. The intellectual and structural causes of decay reinforce each other over time because the Army grows generations of leaders who have no experience with the value of unit historical programs and so do not think of or know how to maintain them. As these leaders rise through the ranks, there is also no command-driven requirement from above to comply with the regulation. Left unchecked, this decay will continue.

(Figure by author)

Figure 1. Current Status of Regular Army Command Historians (as of September 2020)

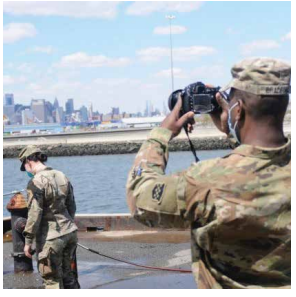
The effects of this decay go far beyond a degraded level of soldier awareness of unit history and heritage, which in itself lessens unit effectiveness. Commanders increasingly have little or no perspective on unit performance over time and have a decreased awareness of the cultural and political dimensions of the theaters of operation they encounter. This latter effect compounds itself as these leaders advance in rank and responsibility, and it further limits their ability to embrace and function within the strategic and policy levels of war.

As the Army's lead for historical programs, the Center of Military History (CMH) has developed a five-point action plan to address shortfalls in history and heritage programs across the operational force.

Five lines of effort

1) Insert historical programs content into the Army Strategic Education Program
2) Assign 5X command historians (individual mobilization augmentee/reserve officers) to commands
3) Insert historical programs training into battalion/brigade precommand courses
4) Establish the unit historical officer program
5) Enhance additional skill identifiers 5X for military historians

Real time



Real perspectives

Real transitions

Outcomes

✓ Actionable historical programs for leaders at all levels

✓ Resilient, inspired, culturally engaged soldiers and units

(Figure by author)

Figure 2. History in the Operational Force—Center of Military History Initiatives

Its initial focus has been on the Active Component but will seek to build interest and momentum that can cross over to the Army National Guard and the Army Reserve as these programs take root. This is a "train the trainer" approach to building programs, with CMH providing subject-matter expertise, constant reachback, and ongoing synchronization. It focuses on the idea that a unit historical program is a commander's program, not one that is administered by a staff officer or an external agency. Figure 2 depicts the five lines of effort of this action plan.

In order to reinforce a culture of lifelong learning, assist the Army in developing strategic thinkers, and establish senior leader advocacy for history and historians, the first component of this action plan will be to insert historical programs training into the Army Senior Leader Education Program. The first opportunity to do so will occur in January 2021, when CMH will provide an orientation to CMH products and services at the Army Senior Leader Education Program event for newly selected brigadier generals. As a part of this line of effort, CMH will partner with Army University Press (AUP) and the Army War College to offer senior leaders relevant historical content in a variety of formats and platforms that will maximize their time. CMH's Field Programs and Historical Services Directorate also continues to develop nontraditional staff rides aimed at engaging senior officers and civilians on strategic topics such as national military policy, strategy, mobilization, and civil-military relations. This portion of the program truly focuses on positioning "actionable history" as a strategic enabler for Army senior leaders.

The Army's general officer leaders are accustomed to seeking historical support, so CMH must continue to rebuild command history offices to provide them with that support. Thus, the second component of the action plan involves assigning U.S. Army Reserve officers as command historians at Army service component command, corps, and division levels in the Active Component. These officers will be assigned to CMH, with reserve duty specified at the headquarters location to which they are assigned, and their duties will be structured to include potential deployment with their headquarters. Command historians will have three primary duties: the development and maintenance of unit historical files, the compilation and submission

of annual historical reports for their units, and the supervision and coordination of subordinate command historians (at Army service component command and corps levels) or brigade and battalion unit historical officers (UHO, additional-duty officers below division level) within their commands. As these officers' time and capabilities permit, they will also be encouraged to answer commander and staff requests for information and develop unit professional development programs such as staff rides. CMH will advertise these command historian positions, interview applicants, make selections for the historian positions, and provide the officers with initial training and ongoing technical support. The command historian will wear the insignia of the supported unit and will conduct regular drill periods and annual training at the unit in order to accomplish his or her primary missions.

Because command historians will be expected to do historical work and because some will not have historical training, CMH will coordinate attendance for all at the Army Field and Unit Historian Course, a distributed learning course taught by AUP. All selected command historians will also have a short temporary-duty onboarding at CMH in order to familiarize themselves with the products and services available for their use. Command historians without history degrees will also be encouraged to earn a graduate degree in history from an accredited institution. In all cases, CMH staff will be available for assistance and support, but the success of this aspect of the program is dependent upon both the individual command historian's doctrinal grounding, staff, and interpersonal skills, and the unit commander's understanding of the historian's role in the staff.

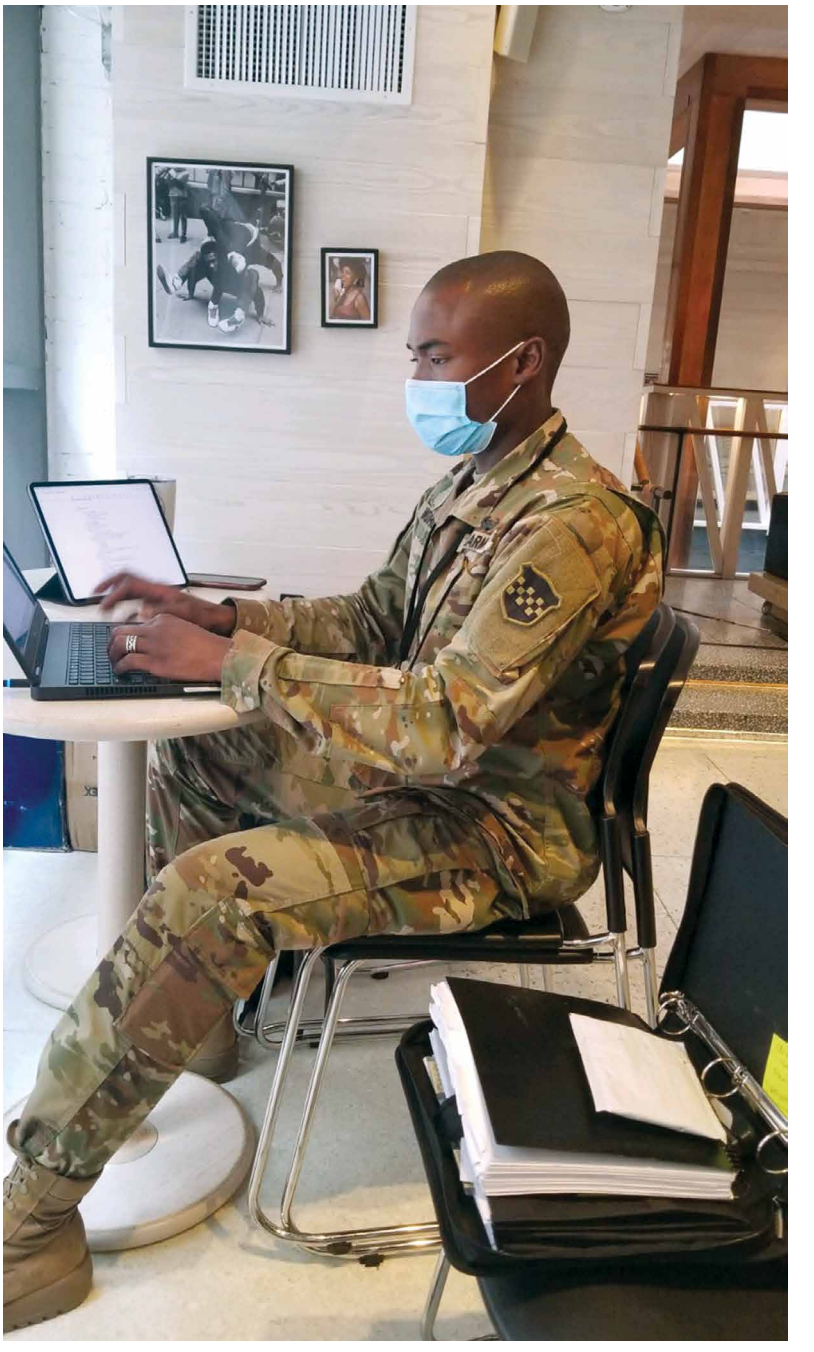
In an effort to grow senior leaders with experience in maintaining and using historical programs, we have begun to integrate instruction on these programs into the U.S. Army Training and Doctrine Command battalion and brigade commanders' training courses. Each basic branch in the Army teaches these courses for incoming commanders, and the Combined

Dr. Peter Knight, U.S. Army Center of Military History Field Programs Directorate, describes the action at Pointe du Hoc, Normandy, France, on the anniversary of D-Day 5 June 2019 for Secretary of Defense Mark Esper during the seventy-fifth anniversary celebration. (Photo courtesy of HQDA Public Affairs)

Arms Center's School for Command Preparation conducts a centralized Army-level course. CMH executed the first iteration of this instruction for the Maneuver Center of Excellence at Fort Benning, Georgia, which runs a pre-command course for armor- and infantry-unit commanders. CMH will continue to deliver the instruction virtually, with interactive exercises that expose commanders to the resources available to them and to their historical officers on CMH and AUP digital platforms. Over the course of fiscal year (FY) 2021, CMH will develop a version of this instruction for the Army-level course at Fort Leavenworth.

Because of the sheer number of brigades and battalions across the Army, it is unrealistic to plan to staff them with full-time historians. What commanders need at this level is an additional duty officer or noncommissioned officer (NCO) who can build and maintain a unit historical file and who can submit periodic summaries of these files to command historians at the division level. CMH will accomplish these tasks via the UHO program, which will become Army policy in the new version of Army Regulation 870-5, due out in FY 2021.

A word first about what the UHO is not. He or she is not expected to perform the analytical or publishing functions of a historian; rather, the UHO is expected to maintain a unit file of historical documents such as command and staff rosters, orders, concept documents, training guidance, readiness reports, command inspections, and after action reviews. CMH is developing a standard operating procedure to guide UHOs in their duties; is testing and fielding a SharePoint-based digital tool that will give UHOs the ability to compile and submit annual summaries to their higher headquarters; and is developing a distance learning UHO training module. This module will help UHOs both to accomplish their doctrinal duties and potentially expand their personal skill sets to include developing unit heritage and professional development programs for their units.



Capt. Julian Woodhouse, officer in charge of the 315th Military History Detachment, reports on COVID-19 operations supporting the Department of Defense's Task Force New York 22 April 2020 from one of the primary operations centers, the Moxy Hotel in Times Square. Woodhouse is part of the team of U.S. Army historians mobilized across the continental United States documenting COVID-19 operations for the U.S. Army. (Photo by Sgt. 1st Class Lamont Bradford, U.S. Army)

When units deploy for combat or humanitarian assistance operations, CMH will offer support to UHOs and command historians in a two-phase process. Before units deploy, CMH will conduct an in-person or virtual mobile training team to provide them with predeployment training in document collection and interface with theater military history detachments. Upon a unit's return, another CMH team will facilitate UHO after action reviews, provide expertise in the completion of unit command reports (the deployment version of an annual historical summary), and advise on the completion of updates to unit awards and campaign participation credit.

Rounding out this action plan will be continued program enhancements for the Skill Identifier (SI) 5X, Army Historian, and the expansion of the historical program to embrace NCOs. To this point, a master's degree in history has been a baseline requirement for earning the 5X SI, which is administered by CMH's Field Programs directorate. Expanding this opportunity will generate more interest in historical programs and thus professionally develop the force. With this in mind, CMH will partner with the U.S. Army Human Resources Command to expand the 5X program to begin in precommissioning education and the NCO Education System. For example, officer cadets who complete a bachelor's degree in history will be eligible to earn an apprentice-level 5X SI, with tiered levels of achievement leading to UHO and command historian positions, as well as opportunities to compete for advanced civil schooling and assignments as a history instructor. In the enlisted ranks, the new Project Development Skill Identifier H6B, Historian, will differentiate NCOs in the public affairs military occupational specialty from those who are assigned to military history detachments. This program enhancement will also deepen the Army's bench of officers and NCOs capable of serving in demanding staff positions across the Army and the joint force.

After FY 2021, the next phase of historical programs improvement will focus on developing more effective content for unit historical programs. As the Army historical program continues to branch out into social media, documentaries, podcasts, audiobooks, and virtual staff rides, the time is now to consider how CMH can provide historical content to soldiers in ways that will engage and inspire them, and create in them the desire to learn more. CMH will seek to partner with AUP, the Army War College, the history faculties at West Point and Fort Leavenworth, and Training and Doctrine Command's Military History and Heritage Office to do this. This action plan will be much more effective through synergy among Army historians and museum professionals.

The time is now for innovative thinking to reverse the longstanding decay of historical programs across the Army. To revive historical programs is the intent of this action plan. By coaching successive generations of officers and NCOs to establish and maintain historical programs in their units, equipping them with the tools (command historians, UHOs, and historical products), and encouraging lifelong learning and self-development, the five lines of effort described here will reestablish historical mindedness across the force. This action plan will also foster further collaboration and professional development among the Army's civilian and military historians, museum professionals, and archivists. The Army's return on this small investment will be a low-cost, incremental improvement in the problem-solving and critical thinking abilities, cultural awareness, resiliency, and pride of leaders, soldiers, civilians, and units. ■

Notes

Epigraph. Peter Knight, U.S. Army Center of Military History, email message to author, September 2020.

1. James Baldwin, "The White Man's Guilt," *Ebony*, August 1965, 47.

2. Army Regulation 870-5, *Military History: Responsibilities, Policies, and Procedures* (Washington, DC: U.S. Government Printing Office, 2007), para. 4-3.

A missile that analysts believe could be the North Korean Hwasong-12 is paraded across Kim Il Sung Square 15 April 2017 in Pyongyang, North Korea. The country's official Korean Central News Agency said a missile fired 14 May 2017 was a Hwasong-12 "capable of carrying a large-size heavy nuclear warhead." North Korea said that it was examining operational plans for attacking Guam, an angry reaction to UN punishment for North Korean intercontinental ballistic missile tests and a U.S. suggestion about preparations for possible preventive attacks to stop the North's nuclear weapons program. (File photo by Wong Maye-E, Associated Press)

Denuclearization through Peace

A Policy Approach to Change North Korea from Foe to Friend

Col. James M. Minnich, EdD, U.S. Army, Retired

The denuclearization of the Democratic People's Republic of Korea (hereinafter DPRK, or North Korea) is a shared global security interest. As the United States bears a large share of this common interest, U.S. policy has a disproportional impact on whether and how North Korea denuclearizes. To avert a near future where Pyongyang presents an existential threat to the United States as a nuclearized enemy state, Washington should work to change North Korea from foe to friend, which would necessitate a different policy approach than what has been pursued by Washington to the present day. This postulation is developed here through a review of thirty years of denuclearization policy approaches and an identification of Pyongyang's persistent aspiration to normalize political and economic relations and end hostile relations with Washington. Informed by previous agreements between the United States and North Korea, a policy of *denuclearization through peace* is recommended to establish conditions that could turn Pyongyang from Washington's foe to friend, a transformation that could reshape and shore up Washington's strategic interests in Northeast Asia.

Same Bed, Different Dreams

The U.S.-DPRK Singapore Summit of June 2018 produced a four-point agreement that if earnestly implemented would have ended nearly seven decades of armistice and ushered in an era of new relations that could have seen North Korea and the United States as friends and perhaps even security partners. However, while the agreement produced a respite from the 2017 rancorous days of fire and fury, this stasis would soon end absent forward diplomatic progress.[1] Peace and denuclearization are the two essential elements of the Singapore Summit as agreed by both parties, which euphemistically placed Washington and Pyongyang in the same bed. The U.S.-DPRK Hanoi Summit of February 2019, however, revealed that while in the same bed, Washington and Pyongyang had different dreams. Washington pursued *peace through denuclearization* as Pyongyang sought *denuclearization through peace*. A peace through denuclearization approach shifts the burden of trust to Pyongyang, requiring it to eliminate its nuclear weapons program first with a promise to establish peaceful relations later. While this tact may be apt for a victor directing the actions of the vanquished, there is no pattern in Washington's previous interactions with Pyongyang to suggest that North Korean Chairman Kim Jong-un would reduce his country's national security to an uncertainty and then wait and see how Washington responds.

Denuclearization through peace is a different policy that advances parties along a path of parallel confidence-building measures. Denuclearization through peace is not a quick fix to end Pyongyang's nuclear weapons capabilities (for if such a panacea existed, it is unlikely that thirty years of deliberative efforts would have transpired only to fail to realize this elusive aspiration). Hasten matters in implementing a policy of denuclearization. Accordingly, half step and mark time are wrong cadences to realize this vital national security interest, which necessitates a rapid pace of quick time interspersed with double time. The transitory nature of government administrations should draw credence to this admonition of purposefully advancing a policy of denuclearization through peace. Testament of the need for quick and decisive policy execution are the fifteen heads of state in Washington (five presidents), Pyongyang (three leaders), and Seoul (seven presidents) who unsuccessfully pursued policies to denuclearize North Korea since 1991.[2] Consistent among these leaders are their failed policy attempts to approach peace building while adhering to feelings of enmity and anticipation of failure. In essence, failed policies of peace through denuclearization were the approaches of the five agreements that circumscribed the last thirty years of efforts to end Pyongyang's nuclear weapons programs. A cursory review of those policy efforts will elucidate obstacles to avoid in a proposed policy of denuclearization through peace.

Inter-Korean Agreements

In the lead-up to the 1988 Summer Olympics in Seoul, newly elected South Korean President Roh Tae-woo launched *Nordpolitik* (German for Northern Policy), a foreign policy to induce normalization of relations with Seoul's Cold War foes in Pyongyang, Moscow, Beijing, and the Eastern European capitals.[3] Roh's Nordpolitik speech in July 1988 was surprisingly magnanimous toward Pyongyang given North Korea's attempt to destabilize the Seoul Olympics with the bombing of Korean Air Flight 858 that killed 115 people just seven months prior. Perhaps belying an army career where he fought communists for three decades in Korea and Vietnam, Roh leveraged his conservative

credentials to determinedly upturn forty years of national policy. He drove a progressive path that normalized robust relations with the communist bulwark states of Hungary in February 1989; Poland in November 1989; Yugoslavia in December 1989; Czechoslovakia, Bulgaria, and Romania each in March 1990; the Soviet Union in September 1990; and China in August 1992.[4] Roh understood that South Korea's economic development and national security necessitated forward-leaning progressive policies versus backward-looking conservative principles.

The 1988 Olympics epitomized sports diplomacy. It originated as rapprochement with Hungary in the lead-up to the opening ceremony, and it progressed with Moscow just five weeks after the closing ceremony when former Soviet President Mikhail Gorbachev decided to normalize relations with Seoul and to notify Pyongyang.[5] Responding to Moscow's perceived betrayal, Pyongyang assented to distinct offers from Washington, Seoul, and Tokyo to meet.[6] Washington had extended Pyongyang a "positive, constructive" approach "to pursue an improvement of relations," leading to the first U.S.-North Korea diplomatic talks in December 1988, which produced a direct dialogue channel that met in thirty-four sessions over fifty-eight months.[7] Straddling the military demarcation line in Panmunjom, North and South Korean diplomats convened the first of eight preparatory discussions for high-level inter-Korean talks in February 1989.[8] Preparatory discussions, which had dragged on for eighteen months, were immediately elevated to high-level talks at Pyongyang's behest in September 1990 in response to Moscow and Seoul normalizing relations that same month. September also produced a triparty declaration signed by the North Korean Workers' Party, Japan Socialist Party, and Japan's Liberal Democratic Party that "strongly urged" their respective governments to normalize diplomatic relations.[9]

In late September 1991, as the Soviet Union devolved, President George H. W. Bush directed all U.S. tactical nuclear munitions returned home.[10] Undertaken as an inducement for Soviet reciprocal action, the U.S. denuclearization of its weapons from South Korea, coupled with the announced cancellation of the 1992 U.S.-Republic of Korea (ROK) Team Spirit military exercise, led to the historic signing of the Agreement on Reconciliation, Nonaggression, and Exchanges and Cooperation between the South and the North, wherein both parties "pledg[ed] to exert joint efforts to achieve peaceful unification."[11] Peaceful unification is a political end state that will first be contingent on signing a peace treaty to establish a peace regime or a comprehensive process toward creating conditions for peaceful coexistence as neighbor states.[12] In a parallel process, the two Koreas negotiated a Joint Declaration of Denuclearization (JDD) of the Korean Peninsula that entered into force on 20 January 1992. The JDD was preceded a decade earlier by Seoul's dismantlement of its own nuclear weapons program at Washington's behest.[13] Unique to the inter-Korean JDD was Pyongyang and Seoul's cooperative agreement to work toward the denuclearization of the entire Korean Peninsula. All subsequent inter-Korean assurances toward denuclearization have included recommitments toward implementing the JDD.

While early 1992 promised cooperation, late 1992 presaged crisis. Under the conservative leadership of Roh and Bush in early 1992, Pyongyang met in distinct senior diplomatic meetings with Washington and Seoul, signed agreements with Seoul on denuclearization and with the International Atomic Energy Agency (IAEA) on safeguards of its nuclear facilities, and hosted IAEA inspectors to its nuclear facilities. Later in the year, Seoul's internal politics factionalized as the country prepared

Col. James M. Minnich, U.S. Army, retired, is a professor at the Asia-Pacific Center for Security Studies (APCSS) in Honolulu. He previously worked as associate dean, senior military professor, and senior military officer at the APCSS, and he served three years in Korea as the secretary of the United Nations Command Military Armistice Commission. He earned master's degrees from Harvard University and the U.S. Army Command and General Staff College in Fort Leavenworth, Kansas, and a doctorate degree from the University of Southern California. He is also a senior service college distinguished honor graduate from the Korean National Defense University in Seoul and a graduate of the Korean Army College in Jaundae, and he holds a diploma in Korean language studies from Sogang University. Minnich has had extensive operational deployments and travels throughout Asia including fifteen years of duty in South Korea, during which he gained in-depth experience in Northeast Asia. In 2016, the South Korean president awarded him the Samil Medal of the Order of National Security Merit for his long and substantive service in the defense of the Republic of Korea. He has published several books, articles, and podcasts on various security issues.

South Korean President Roh Tae-woo (*center*) views a static display of vehicle equipment 13 March 1989 while visiting the soldiers of 5th Battalion, 14th Infantry, 25th Infantry Division (Light), during the joint South Korean and U.S. exercise Team Spirit '89 in the Republic of Korea. (Photo by Al Chang via National Archives)

for a presidential election. Roh would be the country's first president to peacefully step down after serving a single five-year elected term. Roh succumbed to lame duck paralysis as government anticommunist hawks bustled. Lead ROK diplomats working the inter-Korean implementation agreement intentionally delayed its enactment while obstructing prospects of South-North family reunions in mid-September.[14] Senior national intelligence agents illegally impeded the election process and arrested scores of people on fabricated espionage charges on 6 October.[15] Defense officials meeting in Washington on 7–8 October for the annual U.S.-ROK Security Consultative Meeting, surreptitious of Seoul, pushed for the resumption of Team Spirit in March 1993 and then publicly announced the joint decision at the meeting's conclusion.[16] On 9 March 1993, only days after the presidential inaugurations of Bill Clinton in Washington on 20 January and Kim Young-sam in Seoul on 25 February, 170,000 ROK and U.S. combat troops began the Team Spirit exercise.[17] In response, Pyongyang tendered on March 12 its ninety-day notice to withdraw from the Nuclear Non-Proliferation Treaty, which it became party to in 1985 when it operationalized its five megawatt nuclear reactor. In the end, distrust fostered over decades of bitter enmity stoked relentlessly by Pyongyang proved formidable to Roh's ability to paper over the chasm of distrust with Pyongyang and normalize relations despite successfully establishing permanent relations with eight other communist capitals including Moscow and Beijing. While Roh's inter-Korean Joint Declaration on the Denuclearization of the Korean Peninsula is unfulfilled, it has been foundational to successive denuclearization agreements.[18]

U.S.-DPRK Agreements

Normalized relations and an established peace regime on the Korean Peninsula have been Pyongyang's repeated aspirations of Washington since Moscow and Beijing normalized relations with Seoul, respectively

in 1991 and 1992. Pyongyang's overtures toward Washington have been amply evidenced in Washington and Pyongyang's joint statements, agreed statements, and public statements. DPRK founder and former Chairman Kim Il-sung introduced Pyongyang to the probability of ending animus relations with Washington through the U.S.-DPRK Joint Statement of 11 June 1993, which agreed to a principle of "peace and security in a nuclear-free Korean Peninsula."[19] However, thirteen months from the issuance of that joint statement, Kim Il-sung was dead. Chairman Kim Jong-il assumed the mantle of leadership and renewed the prospect of peace and security with Washington through the 12 August 1994 Agreed Statement between the U.S. and DPRK, and the 21 October 1994 Agreed Framework between the United States and North Korea to "move toward full normalization of political and economic relations," while agreeing to "work together for peace and security on a nuclear-free Korean Peninsula."[20] Agreement implementation seemed promising in the first few weeks as IAEA monitored the shutdown of Pyongyang's nuclear reactor and reprocessing facility. However, U.S.-led consortium provisions of heavy fuel oil and construction of light water nuclear reactors were chronically delayed, and efforts toward full normalization of U.S.-DPRK relations were elusive. Euphoria soon subsided and mutual distrust intensified. Parallel to Roh's challenges, Clinton confronted hardliners who derided engagement with Pyongyang as appeasement and political weakness.

In June 2000, Seoul's recently elected President Kim Dae-jung met without public notice in Pyongyang with North Korean leader Kim Jong-il. In the jubilation of the historic first inter-Korean summit, democratic states including the United States took actions toward normalizing relations with Pyongyang. Washington and Pyongyang exchanged envoys in October to prepare for a U.S.-DPRK summit in Pyongyang.[21] When Secretary of State Madeleine Albright met with Chairman Kim, he reaffirmed his desire to establish peace with Washington, offering that it would allow him to transition domestic priorities from defense to the economy.[22] However, détente ended when U.S. President George W. Bush took office in January 2001. Bush was determined to end the Agreed Framework, believing it a flawed agreement wherein Pyongyang clandestinely developed nuclear weapons.[23] History now seemed to rhyme. Like Seoul hardliners who discarded Roh's inter-Korean Joint Denuclearization Declaration of the previous decade at the presidential transition, U.S. neoconservatives of the Bush administration now expressed disdain for Clinton's Agreed Framework. This pattern of discarding a previous administration's joint statements and agreements with Pyongyang was cyclically repeated in Seoul and Washington without exception each time opposition parties transitioned executive power.

> "In the end, distrust fostered over decades of bitter enmity stoked relentlessly by Pyongyang proved formidable to Roh's ability to paper over the chasm of distrust with Pyongyang and normalize relations."

In August 2003, Bush replaced the Agreed Framework as a bilateral security agreement to achieve the denuclearization of the Korean Peninsula with Six Party Talks between Washington, Pyongyang, Beijing, Seoul, Tokyo, and Moscow as a multilateral security architecture to achieve the same. While two years and four sessions of Six Party Talks eventually produced the Joint Statement of 19 September 2005, its pledge toward the denuclearization of North Korea in exchange for normalized diplomatic and economic relations and a peace regime on the Korean Peninsula was substantively similar to the Agreed Framework.[24] Six Party Talks collapsed after the seventh session in December 2008 when Seoul, Tokyo, and Washington terminated heavy fuel oil shipments to Pyongyang for its refusal to accept stringent written verification protocols advanced by Seoul and Tokyo. As with termination of the Agreed Framework that coincided with an administration change between opposition parties in Washington, cessation of Six Party Talks was concurrent with administration changes

between opposition parties in Seoul and Washington and between pragmatic and nationalist leaders in Tokyo.

In August 2009 during U.S. President Barack Obama's administration, former President Clinton met with Chairman Kim Jong-il in Pyongyang where Kim expressed an alternate reality wherein all U.S.-DPRK agreements had been implemented and an environment was created where Washington had in Pyongyang a "new friend in Northeast Asia."[25] That alternate reality was never realized for Kim Jong-il, who unexpectedly died two years later in December 2011. Chairman Kim Jong-un, groomed for succession in the last years of his father's life, immediately sought improved relations with Washington through a series of bilateral discussions that culminated in the coordinated release of statements from Pyongyang and Washington on 29 February 2012 that has colloquially been termed the Leap Day Deal to suspend North Korea's "long-range missile launches, nuclear tests, and nuclear activities at Yongbyon" for improved bilateral relations, peaceful coexistence, and nutritional assistance.[26] Pyongyang's April 2012 satellite launch in contravention to United Nations Security Council resolutions ended all prospects of rapprochement with the Obama administration. Six years after the Leap Day Deal failed, Pyongyang's aspiration to "establish new U.S.-DPRK relations" and "build a lasting and stable peace regime on the Korean Peninsula" became prominent terms of the June 2018 Joint Statement between President Donald J. Trump and Chairman Kim Jong-un at the Singapore Summit.[27]

Four politically alternating U.S. administrations between the Democratic (D) and Republican (R) parties of Clinton (D), Bush (R), Obama (D), and Trump (R) have issued joint agreements or statements with Pyongyang since the early 1990s to achieve three policy objectives: denuclearization of the Korean Peninsula, normalization of U.S.-DPRK relations, and implementation of an enduring peace regime on the Korean Peninsula. These policy objectives are not partisan (liberal or conservative) issues but national security interests. Each agreement and statement has failed. The failures have not been with the policy objectives but with the policy approach. Peace through denuclearization has consistently been the failed policy approach of each administration, which consistently has been unable to generate the mutual trust necessary to evolve Washington and Pyongyang from foes to friends. While Pyongyang shares this thirty-year desire to normalize U.S.-DPRK relations and build a lasting peace regime on the Korean Peninsula as successively manifested by each of its leaders, its first interest is Kim dynastic (national) security.[28] Therefore, if Washington wants to successfully implement a denuclearization policy with Pyongyang, the policy approach will have to buttress the Kim dynasty. Stated simply, Pyongyang will not negotiate away its national security.

> "Washington should work to change North Korea from foe to friend, which would necessitate a different policy approach than what has been pursued by Washington to the present day."

Washington and Pyongyang do not need another agreement to achieve a policy of denuclearization through peace; they merely need to implement the terms of the 2018 Singapore Summit Joint Statement in the order that the top three articles appear: (1) "establish new U.S.-DPRK relations," (2) "build a lasting and stable peace regime on the Korean Peninsula," and (3) "work toward the complete denuclearization of the Korean Peninsula."[29]

Washington's chronic view of Pyongyang as a distant, regional threat led to decades-long containment-policy approaches that sought to contain or ameliorate a North Korean security threat. Pyongyang now possesses strategic nuclear capabilities in an era when Washington's alliance relations are stressed. Foresight girded in hindsight and insight portends two possible futures: the one wherein North Korea is a nuclearized enemy state and the other where it is an interim-nuclearized friendly state. This next section

elucidates risks and interests in both futures.

Much to Gain, More to Lose

A policy of denuclearization through peace could establish robust friendly U.S.-DPRK relations during a single U.S. administration and eliminate North Korea's nuclear weapons and associated programs in a generation. National security is a state's foremost vital interest, which is equally germane to Kim Jong-un, who perceives that threats abound. Neither economic sanctions, international isolation, nor military force have dissuaded Pyongyang from safeguarding its interests with its hard-purchased nuclear capabilities. Therefore, sustainable peace, security, and stability must first be realized for Pyongyang to willingly eliminate its nuclear capabilities. Capabilities do not constitute a threat, which is why Washington does not posture against the nuclear forces of France and the United Kingdom and why Pyongyang does not perceive military threats from China and Russia. Threat is the combination of capability plus intent. This is why Washington will more easily eliminate Pyongyang's intent (or willingness) to use nuclear weapons before it gains Pyongyang's willful elimination of its nuclear weapons.

North Korean leader Kim Jong-un shakes hands with President Donald J. Trump after taking part in a signing ceremony 12 June 2018 at the end of their historic U.S.-North Korea summit at the Capella Hotel on Sentosa Island, Singapore. (Photo by Shealah Craighead, Official White House)

Agreement implementation has proven enormously difficult. Enmity forged in warfare and hardened over seven decades of animus has fostered deep distrust of Pyongyang by many of Washington's legislators, diplomats, and military leaders who perceive rapprochement with Pyongyang as anathema to national security, which has complicated implementation of previous agreements on denuclearization. Therefore, many in Washington prefer status quo adversarial relations that manifest strength and conserve resources requisite to resolve what would be a major political undertaking. Achieving

A truck transporting North Korean soldiers 5 September 2010. With little fuel and no cars for the soldiers, the army often uses this style of transportation. (Photo courtesy of Roman Harak, Flickr)

a policy of denuclearization through peace will require the Washington establishment to objectively consider the nation's interest in establishing an amicable relation with Pyongyang and what could be lost by failing to do so. Three of the last five South Korean administrations have sought and failed to normalize relations with Pyongyang. Seoul's progressives see Washington as obstructing inter-Korean endeavors for peace, and they wrestle politically with how to reconcile the dichotomy of valuing Seoul's military alliance with Washington and advancing inter-Korean peace with Pyongyang.[30] As all parties hedge that diplomatic inter-Korean peace initiatives will fail, each successive discordant statement, sanction enforcement, weapon test, or military exercise imperils overtures of peace as they reinforce suspicions of malign intent. Staunch nationalists in Seoul and Washington who postured against a North Korean enemy during the four decades that spanned the 1950s Korean War and the Cold War that ended in 1989 are a rapidly fading group. In another generation, no one will possess a living memory of the Korean War and there will be few remaining Cold War warriors. Consequently, for the U.S.-ROK alliance to endure, it will need more to bind it than a shared history of the forgotten war. Washington and Seoul should not wait for the coming demographic change; they should take actions now to realize their national interests on a peaceful and secure nuclear-free Korean Peninsula.

Understanding what obstacles strew the policy path toward denuclearization through peace is essential if Washington is to avoid duplicating earlier missteps. Framed by hindsight of previous denuclearization efforts and insight of overlapping national security interests, foresight is gained by considering two likely divergent security futures where Pyongyang is either a nuclearized enemy state or an interim-nuclearized friendly state.

Nuclearized Enemy State

Pyongyang's most probable future, absent active intervention, is a credible nuclearized enemy state that militarily threatens Washington and its allies while propagating malignant mayhem globally. Conservative estimates peg Pyongyang's strategic arsenal at thirty nuclear devices with fissile material for thirty-to-sixty

additional warheads and hundreds of nuclear capable ballistic missiles and large caliber rockets.[31] As one of just nine countries with nuclear weapons, the U.S. Northern Command has suggested that Pyongyang's modest stockpile of nuclear weapons is on course to challenge the U.S. homeland's antiballistic missile defenses by 2025.[32] Nuclear yield, missile capability, and sanction severity are three factors of a security threat posed by Pyongyang as a nuclear enemy state.

Nuclear yields. Between October 2006 and September 2017, Pyongyang conducted six nuclear detonations. The last test, Pyongyang claimed, was a thermonuclear device that had a measured yield of upward of 250 kilotons, or nearly seventeen times more powerful than the fifteen-kiloton bomb dropped by the United States on Hiroshima in August 1945.[33] In September 2017, executive leaders of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack testified before a subcommittee of the House Committee on Homeland Security that the "nation faces a potentially imminent and existential threat of nuclear EMP attack from North Korea."[34] The commission postulated that a high-altitude EMP detonated over the U.S. mainland would bring down the U.S. electrical grid for years, producing cascading calamities that could result in the death of upward of 90 percent of all Americans within one year. An extreme position, perhaps, but if such a scenario killed just 10 percent, or thirty million Americans, a retaliatory U.S. response would seem a pyrrhic victory.

Missile capabilities. Before 2016, North Korea's proven missile capabilities were limited to short-range ballistic missiles. Pyongyang has since conducted some seventy missile tests of much of its known inventory of ballistic missiles and long-range rockets, advancing both its technical and operational capabilities.[35] To that end, the Korean People's Army has demonstrated significant nuclear-capable weapon systems, including more than six hundred short-range ballistic missiles that range throughout the Korean Peninsula, over two hundred medium-range ballistic missiles that range Japan, about fifty intermediate-range ballistic missiles that range Guam, and a limited number of intercontinental ballistic missiles that range the U.S. Eastern Seaboard (see figure, page 23).[36]

Sanctions severity. Since 2006, when Pyongyang first tested a nuclear device, there have been eleven United Nations Security Council resolutions (S/RES) to sanction North Korea in response to six nuclear tests (S/RES 1718, 1874, 2094, 2270, 2321, 2375), three missile tests (S/RES 1695, 2371, 2397), one satellite launch (S/RES 2087), and nuclear weapons and ballistic missile development (S/RES 2356).[37] While seven resolutions target the military and the elites with trade prohibitions on defense articles and luxury items, the later resolutions are broadly leveled at Pyongyang's economic sectors, making illegitimate 99 percent of export revenues, or the near totality of all international trade opportunities, including bans on coal, iron, lead, oil, petroleum, seafood, textiles, and labor.[38] The severity of the sanctions is well characterized by the UN Panel of Expert's noninclusive list of restricted trade items under S/RES 2397 that, among many other items, includes agricultural tools (e.g., greenhouses, handheld tools, irrigation, harvesting and threshing equipment); medical apparatuses (e.g., neonatal equipment, X-ray machines, surgical equipment, wheelchairs, and crutches); food, water, and sanitation security implements (e.g., veterinarian kits, milk pasteurizers, refrigerants, generators, water tanks, and drilling parts); and all metallic items (e.g., screws, bolts, nails, and staples).[39] Onerous exemption request procedures have resulted in but few instances of applicants seeking approval for humanitarian exceptions.[40] The effects of these sanctions transcend the application of maximum pressure upon the Kim regime as the whole of DPRK society absorbs severe humanitarian consequences.[41] Excised by sanctions from conventional trade, Pyongyang increasingly exploits illicit activities such as cybercrime, arms trade, counterfeiting, and human trafficking.[42] Malicious cyber activities have proven very lucrative for Pyongyang, which reportedly netted more than US$2 billion in recent years in cyber-enabled theft across ten countries.[43] Trafficking in sanctioned licit trade is also profitable and increasingly less controlled as evidenced by US$47.9 million of bilateral trade between Russia and North Korea in 2019—a 40.6 percent increase from 2018—of which petroleum accounted for US$27.2 million.[44] North Korea's bilateral trade also expanded with China in 2019 to 95 percent of Pyongyang's US$2.47 billion trade, which further fetters Pyongyang to Beijing.[45] This grossly slanted trade partnership with China is a direct response to economic sanctions upon North Korea. Before Pyongyang was sanctioned for its first nuclear test in 2006, its total trade was US$6 billion (US$7.8 billion in today's dollars) and was diversified

among ten Indo-Pacific economies of which bilateral trade with China was 38 percent.[46] After years of additive UN sanctions, Pyongyang's bilateral trade with Beijing rose to 59.3 percent by 2015 and then by more than 90 percent following the UN's series of enhanced sanctions that began in 2016.[47]

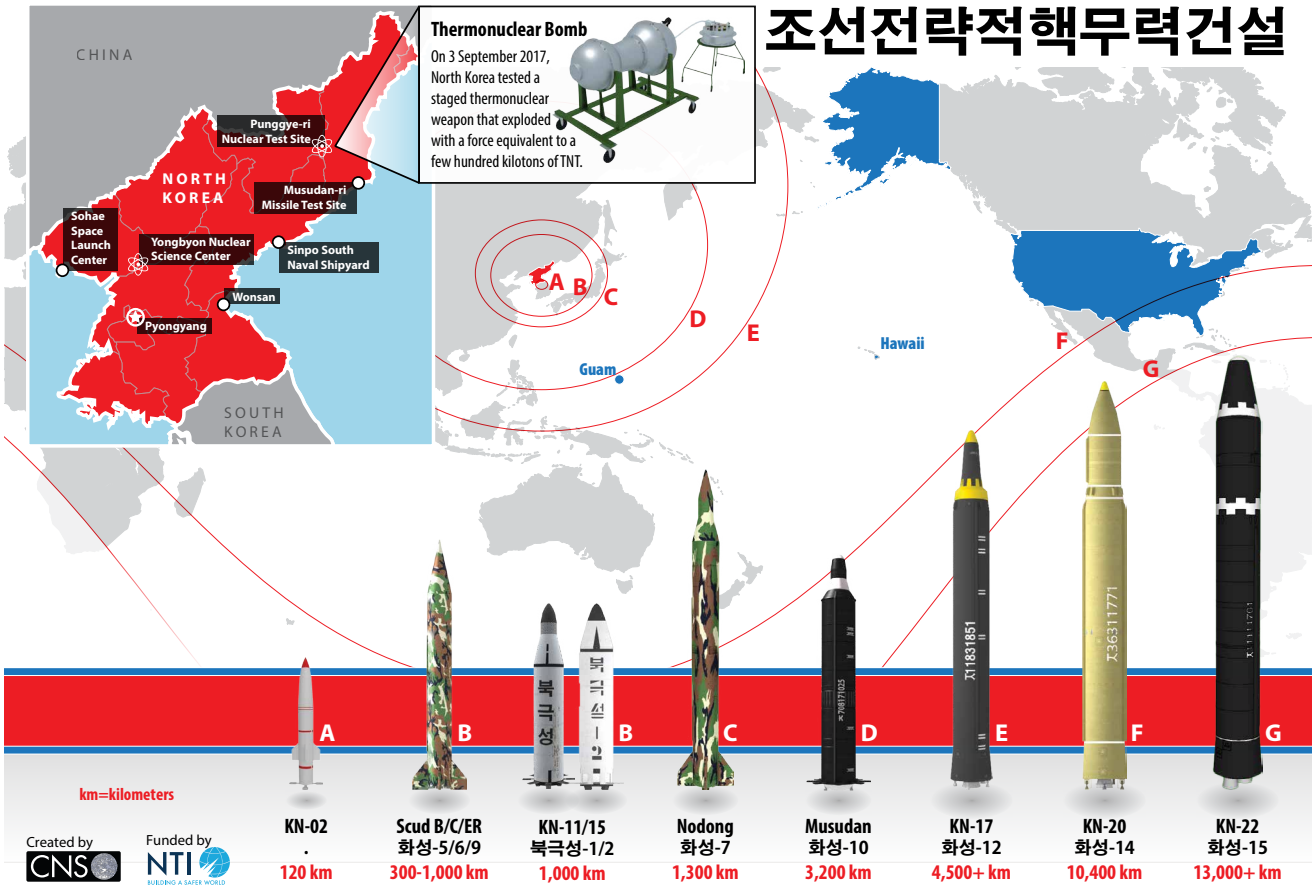
While Pyongyang's most plausible future is as a nuclearized enemy state, such a future is neither preferable nor preordained. Consequently, Washington would do well to induce Pyongyang into its security circle, understanding that this approach would establish Pyongyang as an interim-nuclearized friendly state but definitively not a recognized nuclear state.

Interim-Nuclearized Friendly State

As China and Russia actively contest U.S. influence in the Indo-Pacific, Washington should seize the opportunity to draw Pyongyang into its security architecture with Seoul and Tokyo.[48] This act could reshape Northeast Asia for the next century as Washington shores up its military alliances and shifts a unified security focus from a North Korean threat to strategic security challenges that emanate from Beijing and Moscow. Past diplomatic efforts presage that Seoul and Tokyo will each reciprocate Washington's lead in normalizing political and economic relations with Pyongyang.[49] In consultation with Seoul and Tokyo, Washington should approach Pyongyang purposefully with an expressed willingness to pursue a policy of denuclearization through peace to implement the 2018 Singapore Summit Joint Statement. Such a policy would be purposely phased by immediate and persistent efforts to implement parallel pursuits that (1) establish new U.S.-DPRK relations, (2) build a lasting and stable peace regime on the Korean Peninsula, and (3) work toward the complete denuclearization of the Korean Peninsula. Multisectoral engagements that garner maximum benefits would be characteristics of an immediate phase to establish an era of new relations.

Establish new relations. Nations unite through robust political and economic relations. In establishing new relations between the United States and North Korea, it is necessary to immediately exchange capital city liaison offices staffed with representatives from governmental departments and agencies to build confidence by propelling the work that will implement some future agreement to operationalize the 2018 Singapore Summit Joint Statement. Economic sanctions imposed by the United Nations and United States must be relaxed early for substantive measures toward relations normalization to occur as evidenced by Seoul's fruitless efforts toward maximum engagement with Pyongyang in the face of stiff UN sanctions and U.S. secondary sanctions. Washington's support would significantly improve the prospect of lifting or relaxing UN sanctions on Pyongyang as Beijing and Moscow formally sought in December 2019.[50] To be effective, however, Washington must also relax the 2016 North Korea Sanctions and Policy Enhancement Act and the 2019 Otto Warmbier North Korea Nuclear Sanctions and Enforcement Act, which impose secondary sanctions on countries engaging with North Korea.[51] Relaxed sanctions would facilitate humanitarian and environmental assistance, encourage robust trade, and establish exchanges and cooperation in diverse fields, including agriculture, energy, public health, sanitation and welfare, medicine, safe water, mining, and tourism. Assuming sanctions relief, federal agencies would need to be directed and commercial companies incentivized to invest and engage with North Korea as no substantive engagement precedence exists.

Build a stable peace regime. The disestablishment and repurposement of opposing military forces that are arrayed to fight the next Korean War is the end state of building a stable peace regime on the Korean Peninsula. This notion has seemed to be abhorrent to politicians, diplomats, warfighters, and defense industries who dedicate purpose to and gain profit from defending their sides of the Korean demilitarized zone. It is useful to remember that the 1953 Korean Armistice Agreement is not an end state; rather, it was meant as a provisional solution to supplant war with a military pact to enforce cessation of hostilities until concerned governments could negotiate a peaceful settlement.[52] Therefore, in the interest of building a stable peace regime, protestations toward peacebuilding need to be mollified. For Pyongyang, it will necessitate creating meaningful reemployment for much of North Korea's 1.28 million strong Korean People's Army.[53] Reemployment of the North's surplus soldiers will necessitate massive social work programs throughout the country and access to overseas jobs as guest workers and peacekeepers. U.S. Forces-Korea should consider transitioning from a single-purpose force that mans, trains, and equips to defeat a North Korean threat to becoming a global



(Figure courtesy of the Nuclear Threat Initiative and James Martin Center for Nonproliferation Studies; information as of February 2018, https://www.nti.org/learn/countries/north-korea/. For more resources on North Korea, please visit www.nti.org/northkorea)

Figure. North Korean Strategic Nuclear Threat

force provider that is principally focused on deterring an expansionist communist Chinese threat.[54]

The inter-Korean Comprehensive Military Agreement of September 2018 is an ample departure point toward building confidence as demonstrated by the euphoric actions taken early after its adoption, including the destruction of several ultra-forward guard posts in the demilitarized zone.[55] The task of building a stable peace regime will be difficult unless both sides fully commit to end all pretexts of hostility and then take cooperative actions to dismantle military posturing, planning, training, and equipping that is directed to defend against and defeat the other as an opposing threat. In short, unyielding belligerents must become accommodating peacebuilders if they are to succeed at building a stable peace regime. The task will be difficult.

Work toward complete denuclearization. Complete denuclearization of the Korean Peninsula is undefined, but it is fanciful to imagine Pyongyang willfully eliminating its nuclear weapons capabilities and programs until transmogrification of political and economic relations is realized with Washington and Seoul. It is equally difficult to envision Washington and Seoul accepting from Pyongyang a denuclearization attestation absent a trust relationship because verification inspections without trust will not placate suspicions of cheating.

Denuclearization's low bar is Pyongyang's assent to persistent monitoring of its Yongbyon-based nuclear reactors and related facilities by the International Atomic Energy Agency as it did previously for eight years under the 1994 U.S.-DPRK Agreed Framework and for two years under the 2007 implementation agreement of the Six Party Talks.[56] The high bar of complete

The United Nations Command Military Armistice Commission and the North Korean People's Army Mission to Panmunjom conduct a joint repatriation ceremony of a deceased North Korean soldier 11 September 2013 in the Military Armistice Commission Headquarters Area of the Korean Demilitarized Zone. (Photo courtesy of the author)

denuclearization is Pyongyang's approbation for disposal of its nuclear weapons and long-range ballistic missiles coupled with Washington's endorsement of Pyongyang's peaceful use of nuclear energy without prescription or proscription of fuel fabrication and civil use of rockets to launch satellites, capabilities that Pyongyang has successfully demonstrated and other countries employ without censure. Pyongyang has adamantly resisted previous pressure to renounce its sovereign right to employ these technologies. Consequently, alternative options for energy production and satellite employment will need to be offered during the early stages of denuclearization until trust is built and prescriptions are ended.

Going Forward

Beijing strategically benefits as Washington and its allies tangle with a progressively complex security threat from Pyongyang. This article examined the five denuclearization policies of the last thirty years to accentuate that relations normalization and hostilities cessation are Pyongyang's desired end state with Washington. For Washington, denuclearization has been its singular interest. However, a peace through denuclearization policy— meaning that Pyongyang must first fully denuclearize before realizing normalized political and economic relations with Washington (and Seoul) and before realizing a peace agreement—has persistently been the failed U.S. policy approach of each previous agreement. Had that policy approach been possible, it would have been implemented under one of the previous agreements that was presented in the earlier section.

Denuclearization of the Korean Peninsula is not only still laudatory, but it is also still achievable.

Likewise, normalized relations with Pyongyang is not a progressive agenda, it is an acknowledged national security interest that liberal and conservative administrations in Seoul and Washington have vigorously pursued for three continuous decades. Former South Korean President Kim Dae-jung used this analogy to explain his "Sunshine Policy" of engagement with Pyongyang: "North Korea is like a mold, sunshine is the disinfectant."[57] To appropriate that analogy: a changed regime (as opposed to a regime change) in Pyongyang is the desire, a denuclearization through peace policy is the way.[58]

> As China and Russia actively contest U.S. influence in the Indo-Pacific, Washington should seize the opportunity to draw Pyongyang into its security architecture with Seoul and Tokyo.

While Pyongyang persists in its desire to normalize relations with Washington, Washington has leverage to end this deteriorating security dynamic by immediately embracing Pyongyang in a policy of denuclearization through peace as was outlined above. The 2018 U.S.-DPRK Singapore Summit Statement is the right denuclearization policy framework, and the top three agreements are correctly ordered to implement a successful denuclearization policy that could pull Pyongyang into Washington's security network and reshape the Northeast Asia security environment.

Haste and resolve in implementing a denuclearization through peace policy is essential as has repeatedly been borne out by changing policies between successive administrations in Washington and Seoul. South Korean President Moon Jae-in has met in triple summitry with Kim Jong-un and ardently advocates an engagement policy with Pyongyang; his type of progressive support will be essential to Washington successfully implementing a policy of denuclearization through peace. While this policy approach tacitly accedes to Pyongyang's interim-nuclearized status, it is the correct policy approach, and it is eminently preferable to Pyongyang possessing nuclear weapons as an enemy state. Thirty years ago, Washington rightly objected to Pyongyang's burgeoning pursuit of nuclear weapons, but back then North Korea had no nuclear capability. Less than fifteen years ago, Pyongyang had not even conducted its first nuclear detonation. Pyongyang today, according to a conservative estimate, possesses thirty nuclear warheads and has fissile material enough to increase its stockpile to about one hundred nuclear weapons.[59] Since 2017, Pyongyang has also had a promising second-strike nuclear capability with solid fuel road-mobile launchers and nascent nuclear submarine technology.[60] In 2017, a North Korean nuclear strike upon the United States was so palpable that then U.S. Secretary of Defense James Mattis reportedly remained vigil by sleeping in his clothes and frequenting the Washington National Cathedral.[61]

There is no upside to Pyongyang rising as a strategic nuclear enemy state with ardent animus toward Washington and its regional allies. Washington should abandon its reactive policies in Northeast Asia and seize the present opportunity to change Pyongyang from foe to friend by advancing a denuclearization through peace policy. ■

Notes

1. Peter Baker and Choe Sang-Hun, "Trump Threatens 'Fire and Fury' Against North Korea if It Endangers U.S.," *New York Times* (website), 8 August 2017, accessed 17 August 2020, https://www.nytimes.com/2017/08/08/world/asia/north-korea-un-sanctions-nuclear-missile-united-nations.html.

2. The fifteen heads of state who have pursued policies to denuclearize North Korea include U.S. presidents George H. W. Bush, Bill Clinton, George W. Bush, Barack Obama, and Donald Trump; North Korean leaders Kim Il-sung, Kim Jong-il, and Kim Jong-un; and South Korean presidents Roh Tae-woo, Kim Young-sam, Kim Dae-jung, Roh Moo-hyun, Lee Myung-bak, Park Guen-hye, and Moon Jae-in.

3. Tae Dong Chung, "Korea's Nordpolitik: Achievements and Prospects," *Asian Perspective* 15, no. 2 (Fall-Winter 1991): 149–78, accessed 17 August 2020, https://www.jstor.org/stable/42703974.

4. Ibid., 156.

5. Don Oberdorfer, *The Two Koreas: A Contemporary History* (Reading, MA: Addison-Wesley, 1997), 203.

6. Myonwoo Lee, "Japanese–North Korean Relations: Going in Circles," in *North Korean and Northeast Asia*, ed. Samuel S. Kim and Tai Hwan Lee (Lanham, MD: Rowman & Littlefield, 2002), 89–108.

7. Oberdorfer, *The Two Koreas*, 196.

8. Lim Dong-won, *Peacemaker: Twenty Years of Inter-Korean Relations and the North Korean Nuclear Issue* (Stanford, CA: Walter H. Shorenstein Asia-Pacific Research Center, 2012), 85.

9. Michael J. Green, *Japan's Reluctant Realism: Foreign Policy Challenges in an Era of Uncertain Power* (New York: Palgrave, 2001), 117.

10. Susan J. Koch, *Case Study Series 5: The Presidential Nuclear Initiatives of 1991–1992* (Washington, DC: Center for the Study of Weapons of Mass Destruction, National Defense University Press, September 2012), 11, accessed 17 August 2020, http://ndupress.ndu.edu/Portals/68/Documents/casestudies/CSWMD_CaseStudy-5.pdf.

11. Lim, *Peacemaker*, 85, 111.

12. Frank Aum et al., *A Peace Regime for the Korean Peninsula*, Peaceworks 157 (Washington, DC: U.S. Institute of Peace, February 2020), 2, accessed 17 August 2020, https://www.usip.org/sites/default/files/2020-02/pw_157-a_peace_regime_for_the_korean_peninsula-pw_0.pdf.

13. Kim Hyung-A, *Korea's Development under Park Chung Hee: Rapid Industrialization, 1961-79* (London: RoutledgeCurzon, 2004), 195–202; Leon V. Sigal, *Disarming Strangers: Nuclear Diplomacy with North Korea* (Princeton, NJ: Princeton University, 1998), 20–21; William Burr, "The United States and South Korea's Nuclear Weapons Program, 1974-1976," Wilson Center, 14 March 2017, accessed 14 October 2020, https://www.wilsoncenter.org/article/the-united-states-and-south-koreas-nuclear-weapons-program-1974-1976.

14. Lim, *Peacemaker*, 145.

15. Carl J. Saxer, *From Transition of Power Alternation: Democracy in South Korea, 1987-1997* (New York: Routledge, 2002), 127.

16. Sigal, *Disarming Strangers*, 46.

17. Ibid., 47.

18. Jeffrey Lewis, "Why the 1992 Joint Declaration on Denuclearization of the Korean Peninsula Still Matter," 38 North, 18 March 2011, accessed 17 August 2020, https://www.38north.org/2011/03/1992-joint-declaration/.

19. James M. Minnich, *The Denuclearization of North Korea: The Agreed Framework and Alternative Options Analyzed* (self-pub., 1stBooks, 2002): 99.

20. Robert L. Gallucci and Kang Sok Ju, "Agreed Framework of 21 October 1994 between the United States of America and the Democratic People's Republic of Korea," International Atomic Energy Agency, 21 October 1994, accessed 17 August 2020, http://www.iaea.org/publications/documents/infcircs/agreed-framework-21-october-1994-between-united-states-america-and-democratic-peoples-republic-korea.

21. "Secretary of State Madeleine K. Albright Press Conference," (press conference Koryo Hotel, Pyongyang, Democratic People's Republic of Korea [DPRK], 24 October 2000), accessed 17 August 2020, https://1997-2001.state.gov/statements/2000/001024b.html.

22. Charles L. Pritchard, "A Guarantee to Bring Kim into Line," Brookings Institution, 10 October 2003, accessed 17 August 2020, https://www.brookings.edu/opinions/a-guarantee-to-bring-kim-into-line/.

23. Ivo H. Daalder and James M. Lindsay, *America Unbound: The Bush Revolution in Foreign Policy* (Washington, DC: Brookings Institution Press, 2003), 176; Mike Chinoy, *Meltdown: The Inside Story of the North Korean Nuclear Crisis* (New York: St. Martin's Press, 2008), 43–49.

24. "Joint Statement of the Fourth Round of the Six-Party Talks," U.S. Department of State, 19 September 2005, accessed 17 August 2020, https://2001-2009.state.gov/r/pa/prs/ps/2005/53490.htm.

25. Jesse Johnson, "Hacked Memo Reveals Details of Bill Clinton's 2009 Meeting with North Korea's Kim Jong Il," *Japan Times* (website), 30 October 2016, accessed 17 August 2020, https://www.japantimes.co.jp/news/2016/10/30/world/politics-diplomacy-world/hacked-memo-reveals-details-bill-clintons-2009-meeting-north-koreas-kim-jong-il/#.XmwKUKhKhEY.

26. U.S. State Department Spokesperson and DPRK Foreign Ministry Spokesman, "US Statement on US-DPRK Bilateral Discussions" and "DPRK Statement on Result of DPRK-U.S. Talks," Veterans for Peace, 29 February 2012, accessed 17 August 2020, https://www.veteransforpeace.org/files/7913/3944/6049/2-29-2012_US__DPRK_Statements.pdf.

27. Donald J. Trump and Kim Jong-un, "Joint Statement of President Donald J. Trump of the United States of America and Chairman Kim Jong Un of the Democratic People's Republic of Korea at the Singapore Summit," The White House, 12 June 2018, accessed 17 August 2020, https://www.whitehouse.gov/briefings-statements/joint-statement-president-donald-j-trump-united-states-america-chairman-kim-jong-un-democratic-peoples-republic-korea-singapore-summit/.

28. James M. Minnich, "North Korea's Ruling Dynasty Will Continue, with Kim Yo-jong Next in Line," *Telegraph* (website), 30 April 2020, accessed 17 August 2020, https://www.telegraph.co.uk/politics/2020/04/30/north-koreas-ruling-dynasty-will-continue-kim-yo-jong-next-line/.

29. Trump and Kim, "Joint Statement at the Singapore Summit."

30. Jung-Hoon Lee and Joe Phillips, "Déjà Vu in South Korea? Lessons from the 1992 Philippines Withdrawal," *Washington Quarterly* 42, no. 4 (20 December 2019): 107–30, https://doi.org/10.1080/0163660X.2019.1694292; Andrew Salmon, "Is Anti-Americanism Rising Again in South Korea?," Asia Times, 20 December 2019, accessed 17 August 2020, https://asiatimes.com/2019/12/is-anti-americanism-rising-again-in-south-korea/; Clint Work, "Beyond North Korea: Fractures in the US-South Korea Alliance: Tracing Near-Term Structural, and Strategic Divergences in the Alliance," The Diplomat, 11 February 2020, accessed 17 August 2020, https://thediplomat.com/2020/02/beyond-north-korea-fractures-in-the-us-south-korea-alliance/.

31. Eleanor Albert, "North Korea's Military Capabilities," Council on Foreign Relations, last updated 20 December 2019, accessed 17 August 2020, https://www.cfr.org/backgrounder/north-koreas-military-capabilities; "Arms Control and Proliferation Profile: North Korea," Arms Control Association, last reviewed June 2018, accessed 17 August 2020, https://www.armscontrol.org/factsheets/northkoreaprofile.

32. Jason Sherman, "NORTHCOM: U.S. to Assume 'Increased Risk' against North Korean ICBMs in 2025," Inside Defense, 29 January 2020), accessed 17 August 2020, https://insidedefense.com/daily-news/northcom-us-assume-increased-risk-against-north-korean-icbms-2025.

33. Peter V. Pry, "Empty Threat or Serious Danger: Assessing North Korea's Risk to the Homeland," Hearing Before the Subcommittee on Oversight and Management Efficiency, Committee on Homeland Security, 115th Cong., YouTube video, 38:15, posted by "Homeland Security Committee," 12 October 2017, accessed 11

September 2020, https://www.youtube.com/watch?v=rHh85qtIGl4&-feature=emb_logo.

34. *Empty Threat or Serious Danger: Assessing North Korea's Risk to the Homeland: Hearing Before the Subcomm. on Oversight and Management Efficiency, Comm. on Homeland Security*, 115th Cong. (2017), accessed 17 August 2020, https://docs.house.gov/meetings/HM/HM09/20171012/106467/HHRG-115-HM09-Wstate-PryP-20171012.pdf.

35. Albert, "North Korea's Military Capabilities."

36. James M. Minnich, "North Korea Policy: Changed Regime," *Military Review* online exclusive, 30 August 2017, accessed 17 August 2020, https://www.armyupress.army.mil/journals/military-review/online-exclusive/2017-online-exclusive-articles/north-korea-policy/.

37. "UN Documents for DPRK (North Korea)," Security Council Report, accessed 17 August 2020, http://securitycouncilreport.org/un-documents/dprk-north-korea/.

38. Aum, "A Peace Regime for the Korean Peninsula," 44.

39. "The Human Costs and Gendered Impact of Sanctions on North Korea," Korea Peace Now, October 2019, 1, accessed 17 August 2020, https://koreapeacenow.org/wp-content/uploads/2019/10/human-costs-and-gendered-impact-of-sanctions-on-north-korea.pdf. The UN panel of Experts, established pursuant to Resolution 1874 (UN Panel of Experts), assists the UNSC 1718 Sanctions Committee.

40. Ibid.

41. Hazel Smith, "The Destruction of North Korean Agriculture: We Need to Rethink UN Sanctions," PacNet 24, 29 April 2020, accessed 17 August 2020, https://pacforum.org/wp-content/uploads/2020/04/20200429_PacNet_24-2.pdf; "Democratic People's Republic of Korea: FAO/WFP Joint Rapid Food Security Assessment," UN World Food Programme, 3 May 2019, accessed 17 August 2020, https://www.wfp.org/publications/democratic-peoples-republic-korea-dprk-faowfp-joint-rapid-food-security-assessment.

42. Justin V. Hastings, "The Complex Relationship between Sanctions and North Korea's Illicit Trade," *Asia Policy* 13, no. 3 (July 2018): 28-34, https://doi.org/10.1353/asp.2018.0038.

43. Ian Talley and Dustin Volz, "U.S. Targets North Korean Hacking as Rising National-Security Threat," *Wall Street Journal* (website), 16 September 2019, accessed 17 August 2020, https://www.wsj.com/articles/u-s-targets-north-korean-hacking-as-rising-national-security-threat-11568545202; "Alert (AA20-106A): Guidance on the North Korean Cyber Threat," Cybersecurity and Infrastructure Security Agency, last revised 23 June 2020, accessed 17 August 2020, https://www.us-cert.gov/ncas/alerts/aa20-106a.

44. "N. Korea's Trade with Russia Jumps 40 Percent Despite Sanctions: Data," Yonhap News Agency, 18 March 2020, accessed 17 August 2020, https://en.yna.co.kr/view/AEN20200318002000325?-section=nk/nk.

45. Daniel Wertz, "China-North Korea Trade: Parsing the Data," 38 North, 25 February 2020, accessed 17 August 2020, https://www.38north.org/2020/02/dwertz022520/.

46. Yarno Ritzen, "North Korea: All You Need to Know in Graphics," Al Jazeera, 17 September 2017, accessed 17 August 2020, https://www.aljazeera.com/indepth/interactive/2017/08/north-korea-explained-graphics-170810121538674.html.

47. "N. Korea Trade Deficit with China Hits Record High in 2019: KITA," Yonhap News Agency, 19 March 2020, accessed 17 August 2020, https://en.yna.co.kr/view/AEN20200319006100320?-section=search.

48. The White House, *National Security Strategy of the United States of America* (Washington, DC: The White House, December 2017), 25, accessed 17 August 2020, https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905-2.pdf.

49. Minnich, "North Korea Policy."

50. Josh Smith, "U.S.-led Pressure Fractures as China, Russia Push for North Korea Sanctions Relief," Reuters, 16 December 2019, accessed 17 August 2020, https://www.reuters.com/article/us-north-korea-usa-un-china-analysis/u-s-led-pressure-fractures-as-china-russia-push-for-north-korea-sanctions-relief-idUSKBN1YL0OX.

51. Aum, "A Peace Regime for the Korean Peninsula," 46; "Otto Warmbier North Korea Nuclear Sanctions and Enforcement Act of 2019," National Committee on North Korea (NCNK), 20 December 2019, accessed 18 August 2020, https://www.ncnk.org/sites/default/files/Warmbier_Sanctions_Act.pdf; "Summary of the North Korea Sanctions and Policy Enhancement Act of 2016," NCNK, 18 February 2016, accessed 18 August 2020, https://www.ncnk.org/sites/default/files/content/resources/publications/HR757_Summary_Final.pdf.

52. "Armistice Agreement: Volume 1, Text of Agreement," 27 July 1953" National Archives Catalog, accessed 17 August 2020, https://catalog.archives.gov/id/7062611.

53. International Institute for Strategic Studies, *The Military Balance 2019* (Washington, DC: International Institute for Strategic Studies, 15 February 2019), 222, accessed 17 August 2020, https://www.iiss.org/publications/the-military-balance/the-military-balance-2019.

54. James M. Minnich, "The Year 2012: South Korea's Resumption of Wartime Operational Control," *Military Review* 91, no. 3 (May-June 2011): 2–7, accessed 17 August 2020, http://cgsc.contentdm.oclc.org/cdm/singleitem/collection/p124201coll1/id/1141/rec/1.

55. Jo He-rim, "[News Focus] One Year On, Inter-Korean Military Pact Remains Unfulfilled Promise," *Korean Herald* (website), 17 September 2019, accessed 17 August 2020, http://www.koreaherald.com/view.php?ud=20190917000716.

56. Minnich, "North Korea Policy," 9, 11.

57. Chinoy, *Meltdown*, 55.

58. For more on the proposed denuclearization through peace policy, see Minnich, "North Korea Policy: Changed Regime," *Military Review* online exclusive, 30 August 2017, accessed 11 September 2020, https://www.armyupress.army.mil/journals/military-review/online-exclusive/2017-online-exclusive-articles/north-korea-policy/; Minnich, "Changed Regime: A Policy to Resolve the North Korean Nuclear Crisis," *Military Power Revue* 2 (December 2017): 5–8, accessed 11 September 2020, https://www.vtg.admin.ch/en/media/publikationen/military-power-revue.detail.publication.html/vtg-internet/en/publications/verwaltung/organisation/astab/mpr/MPR_2_17.pdf.html; Minnich, "North Korea Solution: Changed Regime," *Military Review* online exclusive, 12 January 2018, accessed 11 September 2020, https://www.armyupress.army.mil/Portals/7/online-publications/documents/minnich-11Jan18.pdf.

59. Albert, "North Korea's Military Capabilities"; "Arms Control and Proliferation Profile: North Korea."

60. Minnich, "North Korea Policy."

61. Peter Weber, "The U.S. and North Korea Were So Close to Nuclear War, Mattis Frequently Prayed in Church, Woodward Says," Yahoo! News, 10 September 2020, accessed 11 September 2020, https://news.yahoo.com/u-north-korea-were-close-123005352.html.

Finding the Enemy on the Data-Swept Battlefield of 2035

Capt. T. S. Allen, U.S. Army

In order to find the enemy today, armed forces point information collection assets, which may identify anything from a visual signature to a unique radio frequency, in the direction they think the enemy is until they find the enemy's location. This model is outdated, because cyberspace's growth into a global control network that connects devices has created a new, data-swept battlefield, covered by billions of networked devices that are constantly sharing information and can be exploited to find the enemy more efficiently.[1]

By 2035, armed forces on the data-swept battlefield will typically find the enemy by exploiting data in cyberspace and in the broader information environment rather than by monitoring enemy forces directly with their own information collection assets.[2] Put more plainly, the enemy is going to broadcast where it is, or third parties are going to broadcast where the enemy is, as often as armed forces are going to point a camera or antenna at the enemy to find it. Armed forces will constantly query a wide variety of databases of both publicly available and sensitively acquired cyberspace information for indicators of where the enemy is located. Rather than visually or electronically scan for the enemy, the most efficient armed forces will "Google" the enemy using intelligence tools that exploit cyberspace.

On the data-swept battlefield, the armed force best postured to leverage cyberspace to find the enemy will have a significant advantage. The U.S. Army needs to break and remake its tactical intelligence model in order to prepare to win in these conditions.

Capt. T. S. Allen, U.S. Army, is a military intelligence officer serving in the Asymmetric Warfare Group at Fort George G. Meade, Maryland. He has previously served in Afghanistan and Korea, and he is qualified to plan cyberspace and information operations. Allen holds a BS in political science and military history from the U.S. Military Academy at West Point and an MA in war studies from King's College London.

Finding Targets on the Battlefield of 2035

The transformation of tactical intelligence to become cyberspace-centric is already underway.[3] The United States' enemies have been targeting its forces based on social media posts after operational security lapses since at least 2007.[4] For its part, the U.S. Armed Forces have bombed terrorists who made the mistake of posting selfies that revealed their locations.[5] As the number of networked devices and the frequency with which people use them to intentionally or unintentionally broadcast information continues to increase, the utility of existing cyber data streams to identify the location of anything, whether a consumer or an armored fighting vehicle, will also continue to increase.[6] Eventually, cyberspace and the broader information environment will

The digital viewer application, or DVA, provides the Army with a software-based video switching solution and allows command post personnel to connect to the local area network to share all or part of their display with other individuals or on the larger command post display system. (Photo simulation courtesy of the U.S. Army)

almost certainly become the United States' main source of intelligence, including tactical intelligence about the location and disposition of enemy forces. While U.S. forces will still use traditional information collection assets to pinpoint the locations of enemy units and fix them, they will also increasingly rely on cyberspace information to determine where to aim those sensors in the first place. After all, there is no need to patrol an entire province hunting for an enemy tank column when someone tweets a selfie that shows the tanks in the background or when a tank column's movement along a highway causes a massive disruption in well-established civilian traffic patterns that can be easily identified in traffic data collected by cell phone navigation applications.

To date, the transformation of tactical intelligence by cyberspace has been most apparent in the discipline of open-source intelligence (OSINT). Since the birth of the "Social Web," also known as "Web 2.0," in the late 1990s, user-generated content on social media has been central to internet culture. Additionally, smartphones, which allow users to upload content from almost anywhere and to rapidly capture and disseminate images, have come to function as billions of networked information collection devices that publicly share many of their findings on social media. The result has been the proliferation of publicly available information of operational and intelligence value.[7] Even civilian organizations now have the ability to conduct intelligence assessments with a high degree of accuracy using this data. In one notable example, the Atlantic Council and Vice News were able to identify individual Russian soldiers covertly fighting in Ukraine based

Soldiers configure the tactical computing environment extend mode which pieces together various points on a digital map to create one, large map-view similar to what is available in larger command posts. This technology can help soldiers collaborate and increases situational awareness across a formation by sharing a near real-time common operating picture of the "data-swept battlefield." (Photo courtesy of the U.S. Army)

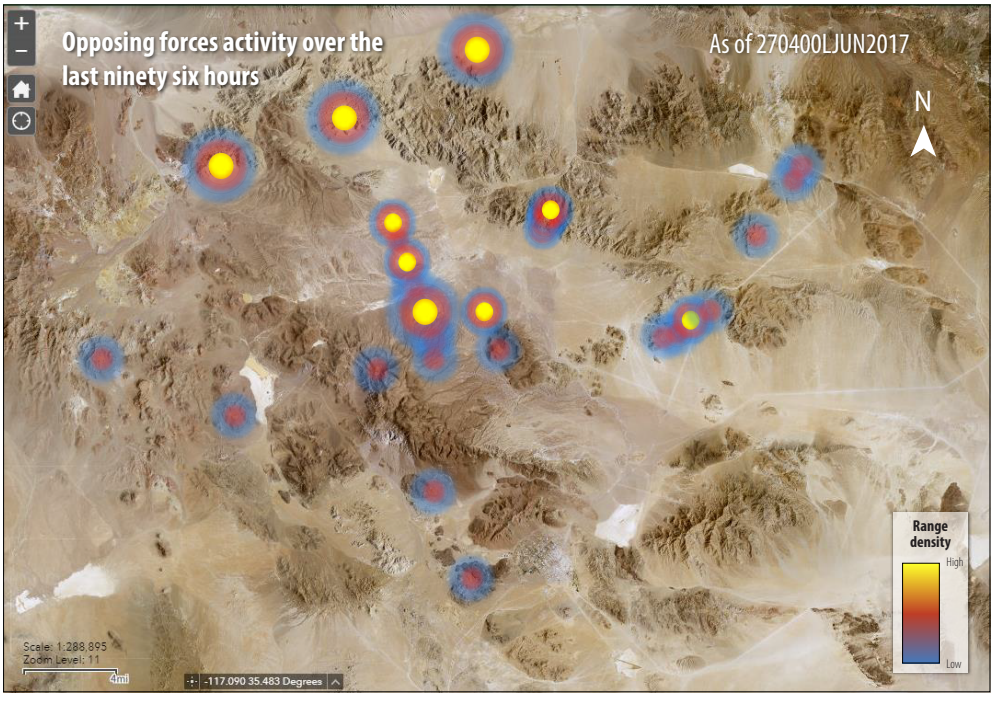
on their social media activity in 2014.[8] Similarly, the investigative journalism website Bellingcat has been able to consistently deliver high-quality intelligence assessments based almost exclusively on what it calls "open-source intelligence" derived from social media. As civilian open-source analyst Cameron Colquhoun notes, "Amongst the billions of posts, uploads, shares and likes, individuals again and again betray their interests to painstaking observers."[9]

Nonetheless, based on my experience as an intelligence officer, OSINT has not become the main source of tactical intelligence. For one thing, it relies heavily on users, who are not controlled or vetted, freely sharing information on events of interest. Users have strong reasons not to monitor military forces, which are armed and dangerous. Even when users do so, they rarely do so persistently, and since tactical intelligence is rapidly perishable, OSINT is only rarely useful for finding the enemy at the tactical level.

Between now and 2035, cyberspace will complete another massive transformation like that previously seen with smartphones and social media, and the effects of the next transformation on tactical intelligence will be even more significant. The new transformation is driven by the rise of the "Internet of Things" (IoT). Cyberspace has already transitioned from a global communication network that connects people to a global control network that connects devices, as Laura DeNardis argues in *The Internet in Everything: Freedom and Security in a Network World.*[10] Devices are now responsible for more cyberspace activity than people, and cyberspace is used to control everything from thermostats in private homes to industrial control systems in factories. Because the IoT is largely automated, the users whose uncontrollable behavior limited the tactical utility of OSINT derived from Web 2.0 are now irrelevant. "If humans suddenly vanished from the earth," DeNardis writes, "the digital world would still

vibrantly hum."[11] The Army's cyberspace doctrine will likely change to reflect this. While the current doctrinal cyberspace characteristics emphasize that cyberspace is "socially enabling," the Army already has ample reason to also characterize cyberspace as "largely automated."[12]

The IoT presents exciting tactical intelligence opportunities. If intelligence and cyber operations are integrated effectively, the IoT could become an unprecedented goldmine of intelligence, giving intelligence collectors access to a countless number of sensors to find the enemy. Whereas during the Vietnam War, the United States tried to monitor wide areas by airdropping thousands of sensors into the jungle, in the future, similar objectives could be accomplished by exploiting civilian sensors that are already in use.[13] Devices such as home security cameras have information of intelligence value if they are pointed at the right location; given how common they have become, it is certain that some IoT sensors will be pointing at areas of interest at least some of the time. Moreover, IoT devices are infamously insecure, as hackers regularly demonstrate.[14] As of early 2020, 98 percent of IoT traffic was unencrypted, making it exceptionally easy to exploit.[15] The major significant disadvantages of exploiting IoT sensors are that they cannot be technically controlled and are vulnerable to deception and manipulation, but these weaknesses will be checked by the sheer scale of data available, which can be used to add ever more information with which to make assessments.



(Figure by Capt. Gerald Prater, U.S. Army. Orthoimagery map courtesy of the U.S. Geological Survey's The National Map)

Figure. Heat Map of the Location of Opposing Forces at the National Training Center in 2017

Two innovative lieutenants produced the map by using social media location data, which could have been produced from anywhere in the world, requiring no special intelligence equipment.

As the IoT develops, one significant emerging common practice is that most vehicles broadcast data about their locations. Although the Army will not primarily find the enemy inside the United States, U.S. cyber practices frequently proliferate worldwide, so they are an important leading indicator. In the United States today, all aircraft already emit their locations through a system called automatic dependent surveillance–broadcast (ADS-B), and most ships do the same through the automatic identification system. The U.S. Department of Transportation also advocates the employment of vehicle-to-vehicle safety communications systems for most private automobiles that would broadcast location data.[16] By 2035, systems such as ADS-B, the automatic identification system, and vehicle-to-vehicle will almost certainly proliferate worldwide. While these systems are designed to ensure security and a modicum of privacy, since they still share location data, in practice they will make it possible for any appropriately equipped automated device to easily monitor all vehicular movement. Moreover, if ADS-B is any guide, fixed sensors that monitor movement activity and

automatically share it in cyberspace are likely to become common to satisfy public demand for data about traffic. As the Government Accountability Office found in a 2018 assessment of ADS-B, these systems pose grave risks to the operational security of military forces, including our own, because they could require us to broadcast the locations of sensitive military activities.[17]

There is also an emerging but contested norm that human beings share data about their locations in cyberspace via their phones and wearable IoT devices. The Department of Defense received a stunning reminder of this in 2018 when Strava, a fitness device company, published a heatmap based on users that highlighted running routes on military bases around the world.[18] It received another in 2019, when the *New York Times* reported it used cell phone location data to track the movements of a senior defense official.[19] The sharing of location data is likely to continue because, as Shoshanna Zuboff argues, corporations profit from exploiting user location data, and most users are willing to provide it. While many people are uncomfortable with the notion that they are being tracked individually, they often have little objection with the sharing of data that is labeled "aggregated" or "anonymous."[20] The COVID-19 pandemic has brought significantly more public attention to cell phone location trackers.[21] During the pandemic, Google used its database of smartphone user locations to provide detailed reports to public health officials on patterns of life around the world and publicly released them.[22] In a more germane use case, a private sector geospatial analytics company reported that Russian arms factories were slowing production by leveraging similar data to see how many factory employees were reporting to work during the pandemic.[23] Interestingly, only five days later, the Russian government banned military personnel from carrying smartphones that track user location.[24]

A 2018 heat map showing the movement of soldiers based on location data collected from the Strava fitness application at Bagram Air Base in Afghanistan. (Screenshot courtesy of Strava Labs)

By 2035, then, we will live in a world where most movement generates a cyberspace signature. Vehicular movement will be easy to track, and at the very least, broad trends in individual human movement will be visible. Chances are no one will install tracking systems on military vehicles but that will not reduce the intelligence value of this massive data source. Military forces will maneuver across a data-swept battlefield, where every "hidden" action they take sparks an easily monitored reaction. Even if they emit nothing, they will be indirectly visible in cyberspace when they disrupt normal patterns of life, when they cause traffic jams by driving down highways, when people post information about their activities on social media, and when they come into the field of view of exploitable IoT devices such as security cameras. In many cases, analysts will be able to find the enemy by identifying disruptions in normal patterns of life showing *atypical inactivity* in a given area. I term this "negative intelligence," akin to the meaningful emptiness of "negative space" in visual media. While military organizations may not necessarily deliver lethal fires on targets identified only in cyberspace, cyberspace will provide the intelligence base layer in which intelligence forces find the enemy. Traditional information collection assets will still play an important role, but they will focus on fixing enemy forces that were found in cyberspace.

The force that is best prepared to access the wide variety of information of intelligence value in cyberspace will have a decisive advantage over another force that limits itself to fewer, technically controlled information collection assets that will only be able to collect an exponentially smaller amount of data.

This is Not the Battlefield You Are Looking For

The data-swept battlefield of 2035 presents exciting intelligence opportunities, but it also presents daunting challenges for the U.S. Army. In order to achieve a decisive advantage, the Army must make fundamental changes to its tactical intelligence model, even beyond the changes outlined in *The U.S. Army in Multi-Domain Operations 2028*, which describes its future vision but does not mention the IoT.[25] These changes are imperative because if they are not implemented, the Army could find itself suffering from chronic information overload, incapable of conducting mission command, and fighting in future wars without many of its historic advantages.

First and most importantly, the Army must prepare to exploit cyberspace information at centralized, highly automated intelligence centers focused on supporting tactical decision-making that will identify information of tactical value, process it, exploit it, and disseminate it to tactical formations for action. Historically, it made sense for the Army to expect commanders to find many of their own targets because they could do so with close-access information collection assets in their formations. The data-swept battlefield will change this as most IoT devices are designed to be networked and share information globally, making close access less important. IoT devices share data through a cyberspace that will be increasingly "centralized," with massive corporations such as TenCent in China and Yandex in Russia controlling an unprecedented share of all data.[26]

While the centralization of the internet will require the centralization of intelligence collection,

Spc. Nathaniel Ortiz, Expeditionary Cyber Electromagnetic Activities (CEMA) Team, 781st Military Intelligence Battalion, conducts cyberspace operations 9 May 2017 at the National Training Center, Fort Irwin, California. More recently, the 915th Cyberspace Warfare Support Battalion activated on 1 January 2019 is the first scalable organic expeditionary capability to meet the Army's current and projected tactical CEMA requirements. (Photo by Bill Roche, U.S. Army Cyber Command)

Members of the 6th Special Operations Squadron use a tablet to upload coordinates 17 December 2019 during an exercise showcasing the capabilities of the advanced battle management system (ABMS) at Duke Field, Florida. During the first demonstration of the ABMS, operators across the Air Force, Army, Navy, and industry tested multiple real-time data-sharing tools and technology in a homeland defense-based scenario enacted by U.S. Northern Command and enabled by Air Force senior leaders. (Photo by Tech. Sgt. Joshua J. Garcia, U.S. Air Force)

Army decision-making must remain widely distributed to maintain tactical flexibility. As a result, the new intelligence centers will have to get better at disseminating what they know down to the tactical level, primarily through existing theater military intelligence brigades attached to field armies, to augment close-access sensors.[27] Because of the massive amount of data that must be processed, artificial intelligence and machine learning will become key to processing and exploitation. Intelligence collection managers on the data-swept battlefield of 2035 will be modifying algorithms to answer their information requirements. Otherwise, they will almost certainly face information overload—and intelligence failure.[28] Echeloning intelligence capabilities and taking advantage of economies of scale at higher echelons will help avoid creating information overload at lower echelons.

Second, in order to properly exploit the data-swept battlefield, the Army must break down silos between the cyber and intelligence communities. Exquisite capabilities that are currently used for cyberspace intelligence, surveillance, and reconnaissance will have to be repurposed to answer intelligence requirements for maneuver commanders.[29] Rather than simply attaining situational awareness *of* cyberspace as current doctrine states, cyber forces will have to enable intelligence forces by attaining situational awareness of *all domains through cyberspace*.[30] This will require intelligence and cyber forces to share information seamlessly in support of tactical commanders, as part of "convergence," the Army's goal of delivering the "rapid and continuous integration of all domains across time, space and capabilities to overmatch the enemy."[31]

Third, the Army needs to prepare for its own tactical-level actions to be visible in cyberspace. Every new intelligence opportunity is also a potential operational security threat. The Army's operations security model runs the risk of becoming outdated; it remains focused on emissions control, but by 2035 it will have

to control or obfuscate the emissions of the civilian devices that will constantly monitor Army forces on the data-swept battlefield. Because controlling all of these devices is impossible, obfuscation and deception will become more important, even at tactical echelons.[32] Army operations security planners must also increasingly think "two steps ahead" and prepare to fight and win even after their activities are disclosed to the entire world. The Army will have to push enhanced obfuscation and deception capabilities down to lower echelons than ever before, far below the corps level, which is currently the lowest echelon it envisions deploying military deception capabilities.[33] On the data-swept battlefield, even small tactical units will need the cyber equivalent of fog machines.

Fourth, the Army must take deliberate steps to preserve mission command when technology enables micromanagement. As Marshall McLuhan wrote in 1964, "In the long run, a medium's content matters less than the medium itself in influencing how we think and act."[34] Advanced command-and-control technology almost always undermines mission command because it makes micromanagement easy. When the telegraph was first used in military operations in the Crimean War in 1855, the French commanding general immediately found that "the paralyzing end of an electric wire" made it easier for his leaders in Paris to give him orders without adequate information and harder for him to respond to situations on the ground as they developed.[35] In the future, when a battalion commander in an operations center has more information on where an enemy force is located than a platoon leader in contact with that same enemy force, the battalion commander will be tempted to micromanage the platoon leader. However, the flexibility of mission command continues to give American forces a decisive advantage.[36] As a result, we must take careful steps to preserve human-centric mission command within our forces as technology advances.

Fifth, the Army needs to be sensitive to the civil-military-technical concerns that will arise on the data-swept battlefield. The "data" is almost all proprietary and controlled by private industry. While private companies with access to this data participate in a thriving market for data on the activities of private citizens around the world, data brokers may be hesitant to share information with armed forces that will use it for military or intelligence purposes. Relationships with these data brokers will be more important than ever before (and also likely more tense). Given privacy rights and other legitimate data protection concerns, the exploitation of data about foreign targets that is owned by businesses located in the United States or allied nations will continue to be a thorny issue. Additionally, the exploitation of civilian devices will likely raise novel law-of-war issues.

For those interested in reading more about cyber defense, *Military Review* recommends the Spring 2020 edition of *The Cyber Defense Review* (*CDR*). *The CDR* journal is a scholarly effort from the Army Cyber Institute at West Point. *The CDR* generates an intellectual multidisciplinary dialogue through thought-provoking scholarly articles and essays on the strategic, operational, and tactical aspects of the cyber domain. *The CDR* breaks down barriers and fosters innovative solutions to global cybersecurity challenges. *The CDR* compiles perspectives from preeminent thinkers across the government, industry, and academia regarding potential challenges, impacts, and initiatives for consideration as we solve over-the-horizon problems for the Army and the Nation. To view the Spring 2020 edition of *The CDR*, visit https://cyberdefensereview.army.mil/Portals/6/Documents/CDR%20Journal%20Articles/Summer%202000/CDR%20V5N2%20Summer%202020-r8-1.pdf.

Finally, the Army must recognize that there is a real chance that its adversaries will have an advantage in the cyberspace tactical intelligence fight. Many of the material advantages afforded by the Army's exquisite legacy information collection assets will be less important on the data-swept battlefield, and it will have to develop new nonmateriel advantages. Just because the United States has led the information revolution does not mean the U.S. Army is best postured to dominate future battlefields.[37]

Many of the United States' adversaries are postured to out-innovate it. As David Kilcullen demonstrates in his 2020 book *The Dragons and the Snakes: How the Rest Learned to Fight the West*, U.S. adversaries have outpaced it in part by exploiting systems the United States originally built and later made available for civilian use, such as the internet and GPS.[38] Because many cyberspace activities have relatively low resource requirements, and above all, require adaptation to an ever-changing cyber environment, nimble, unrestrained nonstate actors have an advantage over large state bureaucracies such as the Army.[39] There are promising signs that the Army can innovate too, such as the examples of soldiers who figured out how to find enemy forces by exploiting social applications like Tinder and Snapchat that reveal locational data.[40] While bottom-up innovators cannot build the centralized, scalable solutions the Army needs, the Army must do more to enable the innovative hackers in its ranks.[41]

Conclusion

The data that will sweep over the battlefield of 2035 and fundamentally change tactical intelligence is already slowly accumulating in databases around the world. On future battlefields, traditional information collection assets will still play a critical role in allowing armed forces to fix enemy forces, but because of the proliferation of networked devices that automatically broadcast staggering amounts of data in the IoT, the *find* phase of the targeting process will be cyber-centric. In order to maintain its advantages on future battlefields, the Army must enhance its ability to find the enemy is cyberspace in support of tactical intelligence, starting now. ■

Notes

1. For a discussion of the fire-swept battlefield, see Stephen Biddle, *Military Power: Explaining Victory and Defeat in Modern Battle* (Princeton, NJ: Princeton University Press, 2004), 30. The term "data-swept battlefield" is the author's and is original to this article. It is a reference to the "fire-swept battlefield," which characterizes contemporary ground combat.

2. *DOD Dictionary of Military and Associated Terms* (Washington, DC: Department of Defense, as of June 2020), 55 and 104, accessed 15 September 2020, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf?ver=2020-06-18-073638-727. "Cyberspace" is defined as "a global domain within the information environment consisting of the interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers." The "information environment" is defined as "the aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information."

3. T. S. Allen and Robert A. Heber Jr., "Where Posting Selfies on Facebook Can Get You Killed," *Wall Street Journal* (website), 26 July 2018, accessed 15 September 2020, https://www.wsj.com/articles/where-posting-selfies-on-facebook-can-get-you-killed-1532642302.

4. "Insurgents Used Cell Phone Geotags to Destroy AH-64s in Iraq," Military.com, 15 March 2012, accessed 15 September 2020, https://www.military.com/defensetech/2012/03/15/insurgents-used-cell-phone-geotags-to-destroy-ah-64s-in-iraq.

5. Walbert Castillo, "Air Force Intel Uses ISIS 'Moron' Post to Track Fighters," CNN, 5 June 2015, accessed 15 September 2020, https://www.cnn.com/2015/06/05/politics/air-force-isis-moron-twitter/index.html?mod=article_inline.

6. Stuart A. Thompson and Charlie Warzel, "Twelve Million Phones, One Dataset, Zero Privacy," *New York Times* (website), 19 December 2019, accessed 15 September 2020, https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html.

7. Heather J. Williams and Ilana Blum, "Defining Second Generation Open Source Intelligence (OSINT) for the Defense Enterprise" (Santa Monica, CA: RAND Corporation, 2018), accessed 15 September 2020, https://www.rand.org/pubs/research_reports/RR1964.html.

8. "Selfie Soldiers: Russia Checks in to Ukraine," VICE News, 16 June 2015, accessed 15 September 2020, https://www.vice.com/en_us/article/bjk9na/selfie-soldiers-russia-checks-in-to-ukraine.

9. Cameron Colquhoun, "A Brief History of Open Source Intelligence," Bellingcat, 14 July 2016, accessed 15 September 2020, https://www.bellingcat.com/resources/articles/2016/07/14/a-brief-history-of-open-source-intelligence/.

10. Laura DeNardis, *The Internet in Everything: Freedom and Security in a World with No Off Switch* (New Haven, CT: Yale University Press, 2020).

11. Ibid., 3.

12. Field Manual (FM) 3-12, *Cyberspace and Electronic Warfare Operations* (Washington, DC: U.S. Government Publishing Office

[GPO], 11 April 2017), para. 1-64, accessed 15 September 2020, https://armypubs.army.mil/ProductMaps/PubForm/Details.aspx?PUB_ID=1002097.

13. Matt Novak, "How the Vietnam War Brought High-Tech Border Surveillance to America," Gizmodo, 24 September 2015, accessed 15 September 2020, https://paleofuture.gizmodo.com/how-the-vietnam-war-brought-high-tech-border-surveillan-1694647526.

14. Joseph Cox and Samantha Cole, "How Hackers Are Breaking into Ring Cameras," VICE News, 11 December 2019, accessed 15 September 2020, https://www.vice.com/en_us/article/3a88k5/how-hackers-are-breaking-into-ring-cameras.

15. Unit 42, "2020 Unit 42 IoT Threat Report," Palo Alto Networks, 10 March 2020, accessed 15 September 2020, https://unit42.paloaltonetworks.com/iot-threat-report-2020/.

16. T. S. Allen, "Open-Source Intelligence: A Double-Edged Sword," *Proceedings* 144, no. 8 (August 2018), accessed 15 September 2020, https://www.usni.org/magazines/proceedings/2018/august/open-source-intelligence-double-edged-sword.

17. U.S. Government Accountability Office (GAO), *Homeland Defense: Urgent Need for DOD and FAA to Address Risks and Improve Planning for Technology That Tracks Military Aircraft* (Washington, DC: U.S. GAO, January 2018), accessed 15 September 2020, https://www.gao.gov/assets/690/689478.pdf.

18. Patrick Tucker, "Strava's Just the Start: The US Military's Losing War Against Data Leakage," Defense One, 31 January 2018, accessed 15 September 2020, https://www.defenseone.com/technology/2018/01/stravas-just-start-us-militarys-losing-war-against-data-leakage/145632/.

19. Thompson and Warzel, "Twelve Million Phones, One Dataset, Zero Privacy."

20. Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (New York: Hachette Book Group, 2019), 242–45.

21. Sara Morrison, "The Hidden Trackers in Your Phone, Explained," Vox, 8 July 2020, accessed 15 September 2020, https://www.vox.com/recode/2020/7/8/21311533/sdks-tracking-data-location.

22. "COVID-19 Community Mobility Reports," Google, last updated 13 September 2020, accessed 15 September 2020, https://www.google.com/covid19/mobility/.

23. Patrick Tucker, "Russian Arms Production Slowed by Coronavirus, Analysts Find," Defense One, 1 May 2020, accessed 15 September 2020, https://www.defenseone.com/technology/2020/05/russian-arms-production-slowed-coronavirus-analysts-find/165071/.

24. "Putin Bans Armed Forces Members from Carrying Electronic Devices, Gadgets," Radio Free Europe/Radio Liberty, 7 May 2020, accessed 15 September 2020, https://www.rferl.org/a/putin-bans-armed-forces-members-from-carrying-electronic-devices-gadgets/30598888.html.

25. U.S. Army Training and Doctrine Command (TRADOC) Pamphlet (TP) 525-3-1, *The U.S. Army in Multi-Domain Operations 2028* (Fort Eustis, VA: TRADOC, 6 December 2018), accessed 15 September 2020, https://www.tradoc.army.mil/Portals/14/Documents/MDO/TP525-3-1_30Nov2018.pdf.

26. Prem Tummalacherla, "The Top 3 Issues of the Centralized Internet," Medium, 14 June 2019, accessed 15 September 2020, https://medium.com/@IamPremt/the-top-3-issues-of-the-centralized-internet-1db59d5e495e.

27. TP 525-3-1, *The U.S. Army in Multi-Domain Operations 2028*, 22.

28. Tom Lamont, "Can We Escape from Information Overload?," *The Economist* (website), 29 April 2020, accessed 15 September 2020, https://www.economist.com/1843/2020/04/29/can-we-escape-from-information-overload.

29. FM 3-12, *Cyberspace and Electronic Warfare Operations*, para. 1-41.

30. Ibid., para. 1-71.

31. TP 525-3-1, *The U.S. Army in Multi-Domain Operations 2028*, iii.

32. Edward Geist and Marjory Blumenthal, "Military Deception: Ai's Killer App?," War on the Rocks, 23 October 2019, accessed 15 September 2020, https://warontherocks.com/2019/10/military-deception-ais-killer-app/.

33. TP 525-3-1, *The U.S. Army in Multi-Domain Operations 2028*, 22.

34. Marshall McLuhan, quoted in Nicholas Carr, *The Shallows: What the Internet Is Doing to Our Brains* (New York: W. W. Norton, 2010), 3.

35. Gordon Wright, "Soldiers and Statesmen in 19th Century France," in *Soldiers and Statesmen: The Proceedings of the 4th Military History Symposium*, ed. Monte D. Wright and Lawrence J. Paszek (Washington, DC: Office of Air Force History, Headquarters USAF; and United States Air Force Academy, 1973), 28.

36. B. A. Friedman and Olivia A. Garard, "Technology-Enabled Mission Command," War on the Rocks, 9 April 2020, accessed 15 September 2020, https://warontherocks.com/2020/04/technology-enabled-mission-command-keeping-up-with-the-john-paul-joneses/.

37. Kenneth Pollack, "Society, Technology, and Future Warfare," American Enterprise Institute, 6 November 2019, accessed 15 September 2020, https://www.aei.org/research-products/report/society-technology-and-future-warfare/.

38. David Kilcullen, *The Dragons and the Snakes: How the Rest Learned to Fight the West* (New York: Oxford University Press, 2020), 38–65.

39. Stephen Rodriguez, "The Fox in the Henhouse: How Bureaucratic Processes Handicap US Military Supremacy and What to Do about It," Atlantic Council, 26 February 2020, accessed 15 September 2020, https://www.atlanticcouncil.org/blogs/new-atlanticist/the-fox-in-the-henhouse-how-bureaucratic-processes-handicap-us-military-supremacy-and-what-to-do-about-it/.

40. Curt Taylor, "It's Time for Cavalry to Get Serious about Cyber Reconnaissance," eArmor, Fall 2018, accessed 15 September 2020, https://www.benning.army.mil/Armor/eArmor/content/issues/2018/Fall/4Taylor18.pdf; Gina Harkins, "A Lance Corporal's Phone Selfie Got His Marine Unit 'Killed' at 29 Palms," Military News, 7 January 2020, accessed 15 September 2020, https://www.military.com/daily-news/2020/01/07/lance-corporals-phone-selfie-got-his-marine-unit-killed-29-palms.html.

41. James Long, "Shoot, Move, Communicate, and Innovate: Harnessing Innovative Capacity in the Ranks," Modern War Institute at West Point, 16 March 2020, accessed 15 September 2020, https://mwi.usma.edu/shoot-move-communicate-innovate-harnessing-innovative-capacity-ranks/.

The Human–Machine Paradox

A Balanced Approach to Finding and Fixing in 2035

Capt. Michael P. Ferguson, U.S. Army
Chief Warrant Officer 4 Jesse R. Crifasi, U.S. Army
Chief Warrant Officer 3 Nick Rife, U.S. Army

We are under no illusions that these machines improve the nature of the information. This will always depend on the reliability of the source and the skill of the analyst.

—Allen Dulles, 1963

In Ridley Scott's 2008 spy thriller *Body of Lies*, a CIA handler played by Russell Crowe attempts to describe the complexity of modern targeting operations to moviegoers. Crowe's character narrates a

montage in which he explains how jihadists who adhere to ways of the past often favor Cold War tradecraft like dead drops to elude those who would use futuristic technology to locate them.[1] Though fictional, the film's plot syphons off the testimonies of those who led the intelligence war against al-Qaida in Iraq such as Gen. Stanley McChrystal.[2] Conceptual and disciplinary interoperability became as valuable as digital innovation in Anbar Province circa 2006. Locating the enemy in the coming era of Third Offset technologies, such as artificial intelligence (AI) and machine learning (ML)-enabled programs, will be no exception.[3] Exploring challenges and opportunities in the targeting process will lead to solutions in line with this logic.

Senior Army leaders commanding cross-functional teams (CFT) tasked with pursuing modernization initiatives are clear on the difficulties that lay ahead: "We cannot modernize to parity … We must modernize to overmatch and maintain that overmatch through incremental upgrades."[4] Current procedural and doctrinal constructs do not support the degree of technical and operational sophistication required to meet this demand. How, then, can the joint force develop reliable, resilient means of locating its enemies amidst a backdrop of such technological fluctuation?

AI and ML, or advanced analytics capabilities, are unique in that the most tangible operational implementations manifest in Hollywood movies or Arthur C. Clarke novels. Hence, the approach to advanced analytics in support of joint targeting must be driven by the synergistic effects of enhanced human knowledge and sensor capability. Rather than absolving the user of responsibility, digital systems of increasing complexity will demand more intellectual capital from the operator. This is the human-machine paradox. To capitalize on germane modernization efforts, the joint force must develop a personnel strategy that builds on recent technical innovation training initiatives by nesting them with operational doctrine and military education. Doing so creates multifunctional stakeholders to adopt and operationalize the tech, thereby balancing the weight of human and machine inputs and outputs. How the U.S. Army negotiates this concept will shape its capacity to target effectively during joint all-domain operations (JADO) in the coming years.

Previous page: Marines with Marine Corps Forces Cyberspace Command observe computer screens 5 February 2020 at Lasswell Hall in the cyber operations center at Fort George G. Meade, Maryland. (Photo by Staff Sgt. Jacob Osborne, U.S. Marine Corps)

Innovations, Limitations, and Threats

Any hypothetical discussion about the future of targeting should begin with a fundamental question: *How does one prioritize targeting efforts by separating wheat from chaff in an uncertain future environment?* With the advent of the 2018 *National Defense Strategy* and a return to training for great power competition, it is widely accepted that if such a conflict were to arise, the joint force would need to fight with at least some of its assets degraded if not completely denied.[5] This factor alone will dictate how the Army locates its enemies because it will determine the resources to which it has access during operations. Not dissimilar to the conditions that preceded the Global War on Terrorism, it is often external actors who determine where and how the United States fights next. The same is true today. Not only must the joint force train to fight in *all* domains, but it must also be ready to fight in *each* domain independently while others are degraded or denied in a form of "mosaic warfare."[6] A depth and breadth of understanding regarding digital intelligence architectures is therefore paramount to successful targeting in JADO.

In one of the conceptual frameworks of Army targeting known as F3EAD (find, fix, finish, exploit, analyze, and disseminate), finding the target is rightfully the first order of business.[7] The explosion of interconnected commercial sensors over the last ten years, known as the Internet of Things (IoT), will make hiding much more complex in the future. Comprised of some estimated two hundred billion devices capable of connecting to a wireless network—such as home security systems, fitness watches, and even refrigerators—the IoT is the aggregate of data collected by these sensors.[8] This volume of data lends to an imperative that advanced analytics support to targeting be implemented at scale to conserve limited human resources and maximize not only analytical capacity but also quality of target selection. Feedback from recent Joint All Domain Command and Control (JADC2) experiments underscores the requirement for command-and-control structures that scale numerous targets rapidly. Doing so refines the target prioritization process by delineating between scheduled and on-call

fire missions. Leveraging the IoT for military targeting purposes in such a way is a long-term endeavor, but the joint force may very well be training on the "battlefield of things" in support of the near-term fight.[9]

Discussions surrounding the role of advanced analytics platforms in the kill chain are heavy on concepts but light on specifics.[10] In part, this shortcoming is a product of the inconvenient truth that most of the technology under discussion is either not yet invented or not yet operationalized for military application, which in some cases leads to a reliance on science fiction to carve out a way ahead.[11] This challenge has long plagued integration of innovative tech. Operationalizing a new capability where it might have the greatest impact requires a unique blend of technical and operational know-how.

Digital kill chain debates focus primarily on reducing hit-to-kill times, but "sensor to shooter" (S2S) is the doctrinal framework for applying Army and joint fires to prioritized targets on the battlefield. Establishing S2S kill chains is summarized in doctrine as the "sensor to shooter challenge." It codifies two requirements for establishing a kill chain. First, it must "coordinate *multiple* sensor-to-command-to-shooter missions," and second, it must "assure *timely* execution of missions." These challenges highlight the "targeting goal": minimizing sensor acquisition times, processing times, command times, and shooter response times.[12]

Adding context to the digital kill chain, or "the life of the message," it is appropriate to look at digital frameworks that currently support targeting methodologies. Digital kill chains are simply an extension of sensor processing timeliness. The intelligence warfighting function is directly responsible for managing this timeliness from a procedural and technical perspective. However, this responsibility is not managed unilaterally. It is directly related to and contextualized by outputs of targeting methodology provided by the fires warfighting function, specifically the timeliness criteria of target selection standards (TSS). The difference in S2S between striking and missing a reported target correlates with analysis of the adversary's systems displacement doctrine. Targeting dictates that adversaries assume they have been targeted for attack and *will react appropriately* by displacing at the earliest opportunity, which is codified analytically as "target decay." Therefore, it is imperative to know how various message types traverse a theater intelligence architecture, from what sensors or domains they derive, and most critically, how much time is expended during the process.

Constructing a digital kill chain ecosystem consists of industry vendors developing and managing divergent machine language formats, such as the U.S. Air Force Universal Command and Control Interface or the Defense Department's U.S. Message Text Format systems and their associated networks. Message protocols are critical to interoperability between machines, and while the Universal Command and Control Interface may "establish a set of messages for machine-to-machine, mission level command and control for airborne systems" for the U.S. Air Force, it is not a Defense Department standard.[13] Digital modernization and convergence efforts notwithstanding, maintaining even the most basic competence in foundational interoperability requires a considerable technical pedigree.

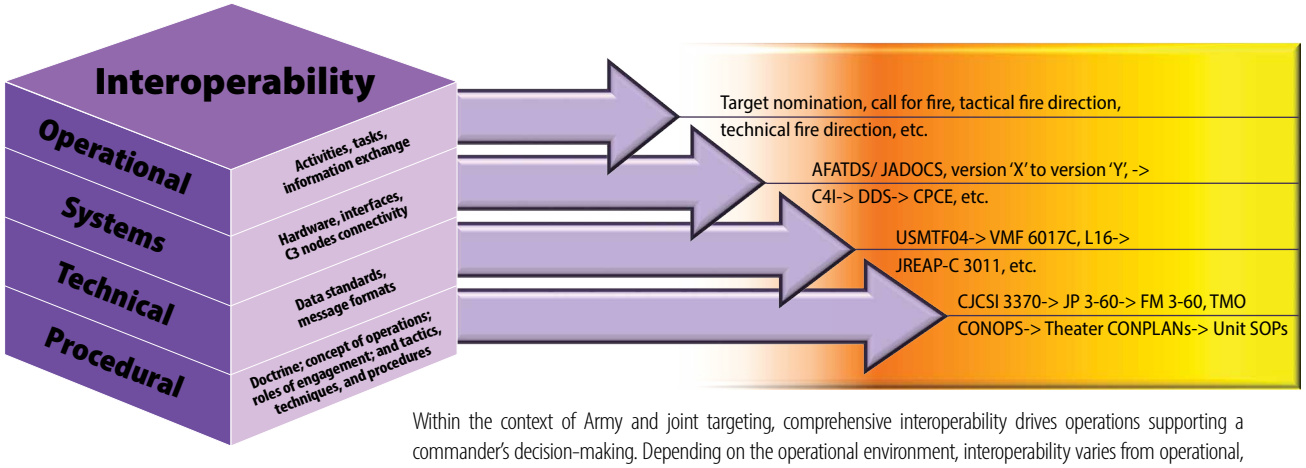
Capt. Michael P. Ferguson, U.S. Army, is a prior-enlisted all-source intelligence officer assigned to the 2nd Security Force Assistance Brigade, Fort Bragg, North Carolina. His previous assignments include the 82nd Airborne Division, 101st Airborne Division (AASLT), Ranger Training Brigade, and NATO Joint Force Command Brunssum, Netherlands. He holds a BS in organizational management and an MS in homeland security.

Chief Warrant Officer 4 Jesse R. Crifasi, U.S. Army, is the digital fires and targeting technical advisor at the Fires Center of Excellence, Capabilities Development and Integration Directorate. A former targeting officer and field artillery intelligence officer in the 82nd Airborne Division, he serves as the principal fires and targeting instructor to the Digital Intelligence Systems Master Gunner Course. He holds a BS in professional studies and an MA in international relations.

Chief Warrant Officer 3 Nick Rife, U.S. Army, is the senior all-source intelligence technician for 2nd Security Force Assistance Brigade, Fort Bragg, North Carolina, and serves as contributing member to the Army Intelligence Corps Digital Initiatives Group. He previously served at U.S. Army Forces Command G-2 as the principal developer of the Digital Intelligence Systems Master Gunner Course, fusion chief at 82nd Airborne Division G-2, and 4th Brigade Combat Team, 82nd Airborne Division.

Fire support command and control systems interoperability

Comprehensive interoperability requires familiarity with both technical and human domains. Interoperability can be process-based (standard-operating-procedure-oriented), or technical-based (systems-configuration-oriented).



Within the context of Army and joint targeting, comprehensive interoperability drives operations supporting a commander's decision-making. Depending on the operational environment, interoperability varies from operational, systems, technical, and procedural categories. However, all four must be present in any given system's targeting enterprise for targeting automation to function.

(Figure by authors)

Figure 1. Visualization of Systems Interoperability Requirements that Facilitate Army Targeting

This interoperability must meet four criteria defined by the activities, tasks, and information exchanges between systems within the kill chain. Systems interoperability is the hardware, interfaces, and connectivity between mission command nodes. Operational interoperability encompasses the routine tasks that support operations, often conceptualized as a mix of human and digital processes. Technical interoperability is the data standards and message formats between distinct machines. Lastly, procedural interoperability is the doctrine, techniques, procedures, and rules of engagement between organizations who manage those machines and systems. The joint force must consider these criteria prior to the development of any new system in the kill chain (see figure 1).

Today, the ecosystem represents a loosely banded cluster of agencies, repositories, and systems underscored by lackluster cohesion, and myopically focused on procedural interoperability criteria. To overcome this challenge, the joint force must couple its technical implementation with the operational doctrine—procedural interoperability layered with systems and technical interoperability prescribed in the same cross-functional doctrine. Beyond this consideration, additional challenges exist at echelons above corps that will influence the tactical kill chain by denying access to sensors and disrupting their communications pathways.

Competitors of the United States are already developing numerous capabilities that would circumvent, degrade, or destroy the most advanced sensors employed by their adversaries.[14] Whether in the form of weaponized satellites, electromagnetic weapons, or hypersonic missiles, nations such as China, Russia, and Iran are acutely aware of how the U.S. military fights and upon which resources it relies to do so effectively, such as space connectivity.[15] We see reflections of this concern in the Army's professional education courses that are reverting to analog training methods even as the conversation surrounding the digitization of operations intensifies. This holds true in everything from field artillery schools to military intelligence courses.[16] Clearly, the Army cannot effectively implement advanced analytics targeting methodology *at scale* without a recalibration of how it is codified in military reference material.

To give the reader an idea of the magnitude of information that will inundate future battlefields, some estimates place the annual global production of data at 175 zettabytes (175 trillion gigabytes) by 2025.[17] Defense

Intelligence Agency leaders are shaping the role of advanced analytics to support national intelligence records with the development of the Machine-Assisted Analytic Rapid-Repository System that uses ML to aggregate metadata for analysts.[18] Machines will drudge through this data, but human operators must still make sense of it to develop a lucid common intelligence picture for their principals; alas, the concept of database management, however dated it may appear, will continue to frustrate modern digital implementations.

While understandably focusing a great deal of attention on emerging technologies because of their potential, the U.S. Army would be wise to not lose sight of who is orchestrating the implementation of these sophisticated programs at echelon. Human ingenuity has, after all, handed the joint force many of its wins over the last two decades.[19] With finite resources at hand and a budget to balance, this is easier said than done, but adopting a balanced philosophy that encourages leaders to invest as much time in their thinking humans as their thinking machines is a good start. In essence, the Army must transform into a digital enterprise that evolves proportionally with the operational environment, equitably distributing the efforts and talents of the human and the machine.

Recommendation 1: Talent Management Reforms

The first step to building an advanced analytics platform capable of thriving in 2035 is to develop a component-level strategy for finding and retaining tactical leaders who serve as the connective tissue linking "big Army" ideas at echelons above corps to battlefield effects. These advocates would forge a conglomerate of future-thought leaders who can synchronize individual unit requirements with emerging capabilities and doctrine by articulating them to key decision-makers and industry shareholders through Army Futures Command liaisons and CFT representatives. Although the Department of the Army (DA) and Army Futures Command directives offer a broad vision for AI investment, most junior service members are unaware of how, when, or why this technology will be developed or applied—and they will be the ones harnessing its potential.[20]

Further challenging modernization is the lack of agility within most institutional training venues. A recent JADC2 experiment highlighted the need for a more robust joint experimentation infrastructure to test emerging concepts in live and simulated environments.[21] Creative and immersive digital problem-solving spaces go a long way in preparing a force for what lies ahead, but however relevant those conclusions might be, they are simply not a priority when measured against the backdrop of Army training and readiness requirements (see figure 2, page 44).

Discovering solutions to these challenges will take a concerted effort across every echelon of the joint force, thus extracting precious time from formations that are already stretched thin with competing demands. As emerging technologies become more prevalent and explicable, an *early* and *often* education model will be essential to bolstering the joint force's creativity in the interim. The *early* program would begin in a recruit's commissioning source or individual training pipeline where assistant professors of military science and senior instructors are trained to provide blocks of instruction on these concepts. This feeds into the objectives of the Army's Talent Management Task Force by familiarizing formations with the benefits, capabilities, and risks associated with automation and targeting.[22] In turn, this initiative could stimulate growth of critical knowledge, skills, and behaviors as service members progress in their careers, allowing the Army to "grow its own" digital warriors rather than simply recruit them (which is a mounting concern).[23] High-performing enlisted and officer recruits interested in pursuing these ideas further would be placed into a queue for attending advanced private industry training that meets the Army's targeting needs, similar to the Graduate Study Active Duty Service Obligation program. If the Army wants to lead these efforts in 2035, it simply cannot wait for junior leaders to become familiarized with them later in their careers.

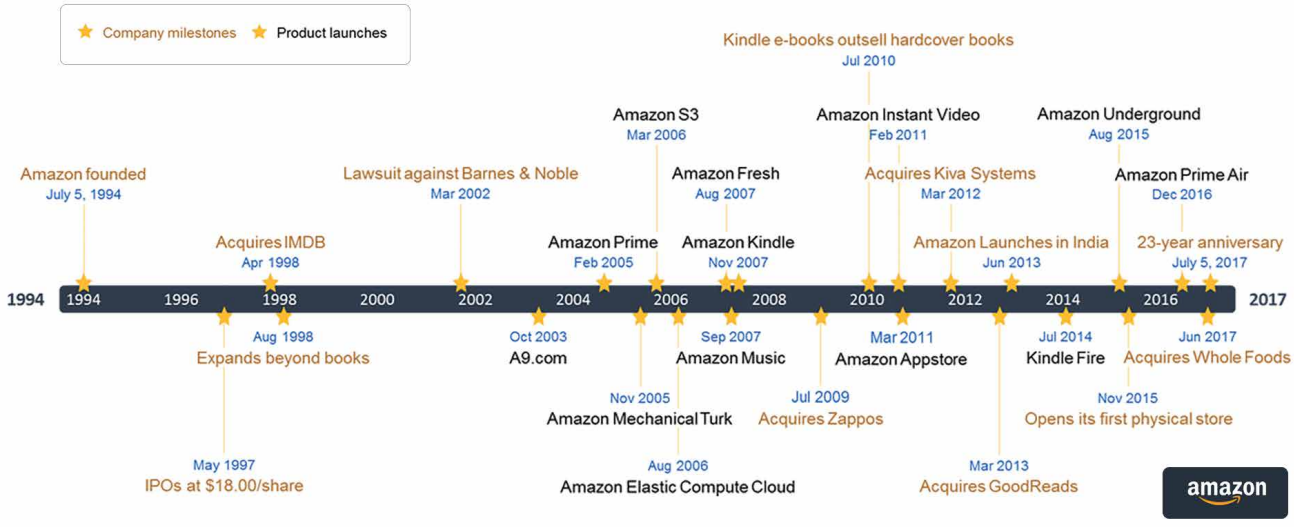
Recommendation 2: Educational Reforms

The *often* approach institutionalizes programs of self-study that foster lifelong learnership at the DA level. With the complexity inherent in future operations, now more than ever, military professionals cannot afford to let their comparatively narrow personal experiences define their understanding of the operating environment between mandated professional military education courses. Former Secretary of Defense Gen. James Mattis put this best: "If you haven't read hundreds of books, you are functionally illiterate, and you will be incompetent, because your personal experiences alone aren't broad enough to sustain

Illustration courtesy of the U.S. Army

Operational technology ethos—taking a page from the Amazon playbook

- Most attempts at change get bogged down in line and block charts instead of focusing on culture and incremental gains
- For four years, all Amazon did was sell books (still number one retailer for books, as of 2019)
- Amazon took twelve years to "establish a cloud" and fourteen years to make it profitable



When taking slow, incremental steps based on a phased approach where success is clearly defined and a brand established—trust develops slowly between supply and demand (the strategic intelligence support strategy and the common intelligence user).

Integrate the strategy **Develop the digital culture**

(Figure by authors and Rob Coon, Intelligence and Security Command. Amazon graphic courtesy of officetimeline.com)

Figure 2. Using Amazon's Model to Demonstrate the Dedication Required to Build an Effective Digital Culture

you."[24] Developing a forcing function at the DA level similar to the U.S. Marine Corps' professional reading program would provide a baseline of historical and technical understanding among Army leaders regarding modernization initiatives outside of their personal experience.[25]

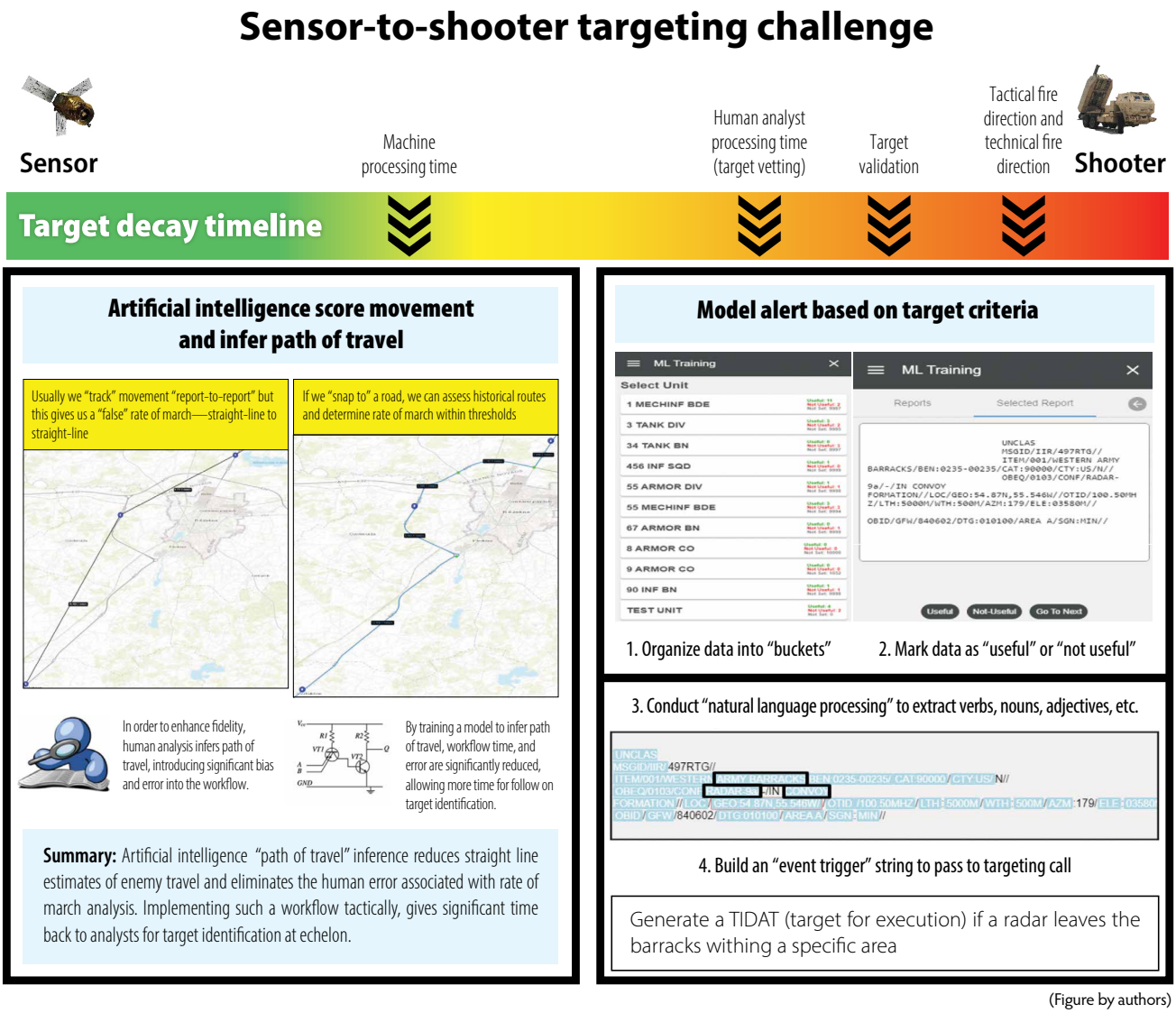
Another component to the *often* approach is the revolutionary digital training platform established by U.S. Army Forces Command (FORSCOM) with support from Intelligence and Security Command (INSCOM). By pooling local resources and technical talent, FORSCOM and INSCOM continue to develop a robust subculture of digital disciples capable of collaborating on and implementing the types of elegant solutions required to support targeting at echelon by 2035. Unconstrained by the policy and decorum that sometimes accompanies the institutional domain, FORSCOM's Digital Intelligence Master Gunner strategy seeks to build digital depth within its formations to confront the future operating environment. As a perennially evolving strategy, this FORSCOM venue is uniquely postured to deliver a service member capable of operationalizing concepts in an advanced-analytics-optimized environment.

The Digital Intelligence Systems Master Gunner Course establishes competencies in legacy intelligence

systems —joint or otherwise—with a keen eye on implications for the current and future era of digital transformation. Driven by the above strategy, the course builds capacity to support the human component involved in operationalizing the science fiction references mentioned previously. Discussion of spatial analytics and natural language processing, and how users may apply those solutions tactically, are rife throughout Digital Intelligence Systems Master Gunner Course academics (see figure 3).

In the meantime, the all-domain sensor fabric is likely to consist of tactical or local cloud capabilities that synchronize a broad suite of interconnected sensors, soldiers, and vehicles providing real-time updates to the warfighter. In the past, many of the challenges associated with finding the enemy hinged on getting the right information at the right time to the right decision-maker. In this regard, the battlefield of things might help dislodge stovepipes in information sharing processes by flattening the trajectory of information.

There is no way to say with any certainty that investing in a particular technology will enable superior targeting in the next conflict, because there is no guarantee that



(Figure by authors)

Figure 3. Example of Subject Matter Introduced in the Digital Intelligence Systems Master Gunner Course

Students problem-solve ways to reduce cognitive load on analysts in support of targeting

the joint force will have access to the full services of that technology. There is, however, strong evidence to support the notion that when properly invested in, the right people in the right place will carve out a path to success when the inevitable worst-case scenario arises. Lending to this conclusion is McChrystal's assessment that the successful targeting of al-Qaida in Iraq was as much a product of cultural and conceptual adaptability as it was technical exploitation.[26] Intuition, intellectual curiosity, and creative thinking are essential to this process because every assessment of future war is pure speculation, and to be candid, most militaries do not have a particularly sterling track record when it comes to predicting future war conditions.[27]

Conclusion

Army leaders must recognize that there is no purely organizational or technological solution to the future targeting equation. The above proposals alone will not close the loop on finding and fixing in 2035 any more than the AirLand Battle efforts of the 1980s made targeting a linear process in 2006.[28] Rather, these recommendations will arm leaders across the targeting enterprise with the ingenuity required to drive cultural change toward a more holistic shared understanding of digital targeting requirements. It is the authors' intent that this understanding might lead to a more inclusive undertaking that operationalizes the work of the various CFTs by building the human terrain necessary to support digital targeting innovations in JADO.

Advantages provided by emerging tools such as tactical cloud devices and advanced analytics in battlefield synchronization systems are real, and the U.S. Army has set up a robust architecture of cross-functional teams, integration centers, and commissions to explore the possibilities.[29] That said, if the Army truly aims to prepare for the harsh reality of great-power conflict in the twenty-first century, its development of people must evolve concomitant to its development of machines. Leaders cannot afford to be blindsided by the expanding technical expectations of the future operating environment. They have a responsibility to develop critical competencies in niche areas, including digital proficiency, to support the rapid integration and implementation of a multi-echelon targeting strategy enabled by advanced analytics. Without accompanying doctrine and innovative training venues, such as FORSCOM G-2 initiatives, the joint force will never be able to execute such an endeavor at scale.

Chief of Staff of the Army Gen. James McConville certainly endorses a human-centric philosophy toward the Army of 2035, something he underscored in his welcome letter to the force.[30] Decades ago, Allen Dulles acknowledged both the centrality of technology to intelligence support and the enduring need for human prudence and wisdom to guide the process. Even *Ghost Fleet* coauthor and future war theorist August Cole admits that the recruitment of service members who have the "capacity to decide, communicate, and act in the *hyperwar* environment will be perhaps more important than any investment in machines."[31] In times of vast technological enterprise within the defense and intelligence communities, pioneers have advocated for a balanced approach to targeting that exploits the benefits of technology by reforming the way in which organizations think about and invest in the operators actioning that exploitation. Considering the highly disruptive and uncertain nature of current threat trends, leaders navigating the human-machine paradox at every echelon should do the same. ■

The authors would like to thank Rob Coon of INSCOM for his generous support of their research.

Notes

Epigraph. Allen W. Dulles, *The Craft of Intelligence* (Guilford, CT: The Lyons Press, 2006), 59.

1. *Body of Lies*, directed by Ridley Scott (Burbank, CA: Warner Brothers, 2008), Blu-Ray Disc.

2. See Stanley McChrystal, *Team of Teams: New Rules of Engagement for a Complex World* (New York: Penguin, 2015), 18. Early in the Iraq insurgency, terror cells favored the use of couriers and face-to-face meetings to circumvent advanced coalition sensors.

3. Bob Work, "Reagan Defense Forum: The Third Offset Strategy" (transcript, Reagan Presidential Library, Simi Valley, CA, 7 November 2015), accessed 15 September 2020, https://www.defense.gov/Newsroom/Speeches/Speech/Article/628246/reagan-defense-forum-the-third-offset-strategy/.

4. Ross Coffman, "What Role Will Robots Play in Future Land Warfare?," Defense News video, 1:29, 5 September 2019, accessed 15 September 2020, https://www.defensenews.com/video/2019/09/05/what-role-will-robots-play-in-future-land-warfare/.

5. Paul Scharre, *Army of None: Autonomous Weapons and the Future of War* (New York: W. W. Norton, 2018), 15, 55–56.

6. Andrew Maher, "Accelerated Warfare and the Puzzle of the Future," The Australian Army Research Centre, 6 April 2020, accessed 15 September 2020, https://researchcentre.army.gov.au/library/land-power-forum/accelerated-warfare-and-puzzle-future.

7. Lloyd Edwards, Matt Gibson, and David McCarthy, "Fix to Finish: Impact of New Technologies on the Special Operations Approval Process," M-RCBG Associate Working Paper Series No. 56 (Cambridge, MA: Harvard Kennedy School of Government, May 2016), 20-24, accessed 15 September 2020, https://www.hks.harvard.edu/sites/default/files/centers/mrcbg/files/56_final.pdf.

8. See "A Guide to the Internet of Things," Intel, accessed 28 April 2020, https://www.intel.com/content/dam/www/public/us/en/images/iot/guide-to-iot-infographic.png. According to data collected by Intel Corporation and the United Nations, this equates to roughly twenty-six smart devices for every human on Earth.

9. "Our Services: What We Offer," Fenix Group Inc., accessed 6 May 2020, https://fenixgroup.io/our-services-2/. Fenix Group introduced and trademarked this germane term.

10. Sydney J. Freedberg Jr., "SecArmy's Multi-Domain Kill Chain: Space-Cloud-AI," Breaking Defense, 22 November 2019, accessed 16 September 2020, https://breakingdefense.com/2019/11/secarmys-multi-domain-kill-chain-space-to-cloud-to-ai/.

11. August Cole, "Science Fiction and the Military Reader: A Review of the Forever War Graphic Novel," *The RUSI Journal* 162, no. 6 (22 January 2018): 60–64; Jesse Crifasi, "The Human Targeting Solution: An AI Story," The Mad Scientist Laboratory, 3 December 2018, accessed 22 September 2020, https://madsciblog.tradoc.army.mil/102-the-human-targeting-solution-an-ai-story/.

12. Army Techniques Publication 3-09.42, *BCT Fire Support* (Washington, DC: U.S. Government Publishing Office [GPO], 1 March 2016), 5-28, 5-33.

13. "Universal Command and Control Interface (UCI)," U.S. Air Force Virtual Distributed Library, accessed 3 May 2020, https://www.vdl.afrl.af.mil/.

14. Mark Esper, "Remarks by Secretary Esper at the Air Force Association" (transcript, 2019 Air, Space & Cyber Conference, National Harbor, MD, 18 September 2019), accessed 16 September 2020, https://www.defense.gov/Newsroom/Transcripts/Transcript/Article/1964448/remarks-by-secretary-esper-at-the-air-force-associations-2019-air-space-cyber-c/.

15. Jim Sciutto, "A Vulnerable U.S. Really Does Need a Space Force," *The Wall Street Journal* (website), 10 May 2019, accessed 16 September 2020, https://www.wsj.com/articles/a-vulnerable-u-s-really-does-need-a-space-force-11557480601; Bob Dixon, "Trading Queens," The War Room, 4 May 2017, accessed 16 September 2020, https://warroom.armywarcollege.edu/articles/trading-queens/.

16. Todd South, "Tech's Nice, but to Fire Artillery's Big Guns Soldiers Must Break Out Maps, Charts and Darts," *Army Times* (website), 21 July 2019, accessed 16 September 2020, https://www.armytimes.com/news/your-army/2019/07/21/techs-nice-but-to-fire-artillerys-big-guns-soldiers-must-break-out-maps-charts-and-darts/.

17. Tom Coughlin, "175 Zettabytes by 2025," *Forbes* (website), 27 November 2018, accessed 16 September 2020, https://www.forbes.com/sites/tomcoughlin/2018/11/27/175-zettabytes-by-2025/#3097355a5459.

18. "DIA's Vision of Mars: Decision Advantage for the 21st Century," U.S. Defense Intelligence Agency, 23 May 2019, accessed 16 September 2020, https://www.dia.mil/News/Articles/Article-View/Article/1855910/dias-vision-of-mars-decision-advantage-for-the-21st-century/.

19. See Joby Warrick, Ellen Nakashima, and Dan Lamothe, "Islamic State Defector inside Baghdadi's Hideout Critical to Success of Raid, Officials Say," *The Washington Post* (website), 29 October 2019, accessed 16 September 2020, https://www.washingtonpost.com/national-security/islamic-state-turncoat-inside-baghdadis-hideout-critical-to-success-of-raid-officials-say/2019/10/29/e702c2fa-fa86-11e9-ac8c-8eced29ca6ef_story.html. Human sources led to the successful targeting of Osama bin Laden and more recently Abu Bakr al-Baghdadi.

20. Gary Sheftick, "Army's AI Task Force Taking Giant Leaps Forward," Army.mil, 7 October 2019, accessed 16 September 2020, https://www.army.mil/article/225642/ai_task_force_taking_giant_leaps_forward. Artificial intelligence committees now exist from the National Security Council to combatant commands.

21. Jay Koester, "JADC2 'Experiment 2' Provides Looking Glass into Future Experimentation," Army.mil, 23 April 2020, accessed 28 September 2020, https://www.army.mil/article/234900/jadc2_experiment_2_provides_looking_glass_into_future_experimentation.

22. "Army Talent Management Task Force," Army.mil, 11 August 2016, accessed 22 September 2020, https://www.army.mil/standto/archive_2016-08-11/.

23. See James Ryseff, "How to [Actually] Recruit Talent for the AI Challenge," War on the Rocks, 5 February 2020, accessed 16 September 2020, https://warontherocks.com/2020/02/how-to-actually-recruit-talent-for-the-ai-challenge/; James Long, "From our Foxhole: Empowering Tactical Leaders to Achieve Strategic AI Goals," War on the Rocks, 1 October 2019, accessed 16 September 2020, https://warontherocks.com/2019/10/from-our-foxhole-empowering-tactical-leaders-to-achieve-strategic-ai-goals/. Attracting and retaining such talent has proven quite difficult.

24. James Mattis and Bing West, *Call Sign Chaos: Learning to Lead* (New York: Random House, 2019), 42.

25. Marine Corps Doctrinal Publication 7, *Learning* (Washington, DC: U.S. GPO, 20 February 2020), accessed 16 September 2020, https://www.marines.mil/Portals/1/Publications/MCDP%207.pdf?ver=2020-03-30-071343-193; Susan F. Bryant and Andrew Harrison, *Finding the Ender: Exploring the Intersections of Creativity, Innovation, and Talent Management in the U.S. Armed Forces* (Washington, DC: National Defense University Press, May 2019), accessed 16 September 2020, https://inss.ndu.edu/Portals/82/Documents/Strategic%20Perspectives/SP%2031%20Bryant-Harrison%20FINAL%20for%20Web.pdf?ver=2019-05-21-111752-910.

26. McChrystal, *Team of Teams*, 235–51.

27. Michael P. Ferguson, "Don't Shoot the Messenger: Demosthenes, Churchill, and the Consensus Delusion," *Joint Force Quarterly* 90 (3rd Quarter, 2018): 78–85.

28. David E. Johnson, "Shared Problems: The Lessons of AirLand Battle and the 31 Initiatives for Multi-Domain Battle" (Santa Monica, CA: RAND Corporation, August 2018), accessed 16 September 2020, https://www.rand.org/content/dam/rand/pubs/perspectives/PE300/PE301/RAND_PE301.pdf.

29. The National Security Commission on Artificial Intelligence, Joint Artificial Intelligence Center, Defense Innovation Unit, U.S. Army AI Task Force, Army Futures Command (AFC), and the six cross-functional teams under AFC are some prominent examples.

30. Gen. James McConville's welcome letter to the force included his priorities. James McConville, "40th Chief of Staff of the Army Initial Message to the Army Team," Army.mil, 12 August 2019, accessed 1 October 2020, https://www.army.mil/article/225605/40th_chief_of_staff_of_the_army_initial_message_to_the_army_team.

31. Wendy Anderson and August Cole, "The Secretary of Hyperwar," *Proceedings* 145, no. 8 (August 2019), accessed 16 September 2020, https://www.usni.org/magazines/proceedings/2019/august/secretary-hyperwar.

The Ostrich Complex and Leadership in Crisis

Lt. Col. Kevron W. Henry, Jamaica Defence Force

The ostrich has been accused of hiding its head in the sand when frightened. Presumably he thus avoids seeing the cause of its fright. Presumably he also avoids seeing what the other ostriches are doing.

—Alvin B. Rubin and Elven E. Ponder

Concepts of effective leadership during crises are generally understood but often difficult to execute. Difficulty in concept execution results from the significant effort that is required of a commander to impose his or her mental acuity and will in order to solve a particular problem and to ensure mission success. On the fault lines of modern-day conflict, there are various knowledge management processes for commanders and other leaders. These processes are fed by information management systems that are designed to assist commanders and staff by providing a structure for them to process and communicate relevant information and make decisions.[1] Despite these processes, unexplained disruptions in their flow have led to leadership and operational setbacks; these disruptions can be categorized as examples of the "ostrich complex." The ostrich complex is defined as the disruption of a decision-maker's knowledge management processes that results in a paralysis of active leadership or state of inertia, with a subsequent distinct negative effect on the outcome of a specific operation. This complex, therefore, requires early identification and mitigation in order to prevent systematic failures.[2] The actions of Maj. Gen. Alan Jones and the U.S. Army's 106th Infantry Division during World War II's Battle of the Bulge provide historical context for the ostrich complex in large-scale combat operations. An Operation Enduring Freedom drone incident in 2010 provides a variation of the complex as it relates to sensory overload and false data-induced confidence in multi-domain operations.

The utilization of ostrich-related themes and terminology in both professional and popular culture is tied primarily to the unscientific belief that ostriches, as big and powerful as they are, bury their heads in the sand in order to hide themselves from perceived danger.[3] On the contrary, ostriches bury their eggs in the sand and routinely lower their heads to check on them, thereby giving the impression that their small heads have totally disappeared.[4] Scientific realities aside, the description has firmly embedded itself in the collective lexicon as a synonym for the either deliberate or unexplained hiding from one's fears or perceptions. In the legal profession, it is known as the "ostrich instruction," which refers to a defense's concept of a client's willful "blindness."[5] In both the financial and health-care sectors, it is the ostrich effect, and in international relations, it is the ostrich doctrine. However, all variations across the disciplines are tied to the concept of avoidance and the individual or collective complexes built upon the foundation of fear.

Carl Gustav Jung posited that a "complex" is a system of interrelated, usually repressed, emotionally charged ideas, feelings, memories, and impulses, that if allowed avenues to vent, can disrupt the normal links in the human consciousness; and as a result, the intentions of

Lt. Col. Kevron W. Henry, Jamaica Defence Force, was a student at the Command and General Staff College (CGSC), Fort Leavenworth, Kansas, academic year 2019/2020. He holds a BSc and an MSc from the University of the West Indies, Kingston, Jamaica; an MSc from the University of Leicester, United Kingdom; and an MMAS from the Command and General Staff College. His operational assignments have been primarily domestic and in the Caribbean region.

the will are impeded or made impossible.[6] Feelings of self-doubt, confusion, fear, ambition, willful ignorance, and the consequence of accountability are ever present as part of the human condition, and all of these feelings encompass possible complexes. The commander and staff who experience the ostrich complex therefore become mentally burdened. Subsequently, their ability to rapidly and accurately portray the meaning and the necessary level of information that helps the commander maintain situational understanding and update their visualization is paralyzed. This ostrich-type behavior will continue to the detriment of their unit unless the commander is able to fight through the emotional white noise and make a balanced decision.[7]

War is a fundamental unchanging human endeavor that violently pits opposing forces against each other as a result of "fear, honor, and the pursuit of interest."[8] Within this construct, commanders and staffs of opposing forces play a high-stakes cognitive chess game in which each searches for an advantage that will enhance their own probability of success. Carl von Clausewitz posited that "if the mind is to emerge unscathed from this relentless struggle, two qualities are indispensable, coup d'oeil or an intellect that even in the darkest hour retains some glimmerings of an inner light and second is determination."[9] However, what happens when our processes are disrupted by the ostrich complex and the light fades?

Maj. Gen. Alan Jones was the commanding general of the U.S. Army's 106th Infantry Division during World War II; the division was nicknamed the Golden Lions. Jones was highly regarded with a distinguished record of a long and venerable service that stretched back to World War I. However, despite his experience and service, it is his indecision and inaction during the Battle of Saint Vith that led to the disintegration of the 106th as an effective fighting force.

In December 1944, the 106th, freshly arrived in the European theater of operations, was ostensibly sent to a low-risk area of the front line. At the "ghost front," as it was known, the main enemies were perceived to be the dreaded trench foot syndrome and the cold weather.[10] The 106th's area was in the Ardennes region of Belgium in the vicinity of the critical transportation hub at Saint Vith and not too far from the German border. However, what the 106th was unaware of as it occupied its foxholes was that Saint Vith would be the focal point for a planned German offensive.

On 16 December 1944, the dynamic and intense launch of the German offensive changed the ghost front into a frenzied battlespace in a matter of moments. From the very first artillery barrage, it became evident that Jones and his staff were already failing at the high-stakes' cognition game. Unclear reports, loss of communications with frontline units, slow decision-making, and a seeming lethargy pervaded the 106th Division's headquarters.[11] Instead of seeking a more enhanced situational awareness in order to make relevant

Original graphic elements by Kirsty Pargeter and Miguel Angel, www.vecteezy.com. Composite graphic by Arin Burgess, *Military Review*.

decisions, Jones sat in his command post and "waited for some word from his corps commander."[12] Later, two of the 106th's regimental commanders, Col. George L. Descheneaux (422nd Regiment) and Col. Charles C. "Moe" Cavender (423rd Regiment), deliberated with each other after receiving numerous indecisive and inconclusive messages from their division headquarters. They subsequently decided that despite their tenuous situation, until division told them definitively to move, they were staying right where they were; the lethargy had spread.[13] It was a fateful decision because when the message to "withdraw from present positions if they became untenable" was later received, it was far too late, and the regiments were overrun.[14]

Brig. Gen. Bruce Clarke's unit was sent to assist the 106th, and when he arrived and observed the situation at the 106th Division headquarters, he provided a dire assessment. In Clarke's opinion, not only was Jones not functioning in a clear and decisive manner, but his indecision had also affected the staff.[15] In a later conversation, Jones told Clarke directly, "I've thrown in my last chips; you take over the defense of St. Vith."[16] In hindsight, this was Jones's most decisive action throughout the battle. Clarke took over the battle and was able to effectively manage the chaos and salvage a perilous situation.

Jones's actions during the Battle of Saint Vith can be attributed to the ostrich complex. His erratic behavior and overall lack of active leadership ran counter to his previously highly rated performances in command and as a staff officer. Throughout the battle, Jones was seemingly preoccupied by the realization that his first real fight as a division commander had resulted in the loss of two regiments and possibly his own son, who was serving with one of them. His behavior further indicated that the conflicting data and fear of repercussions seemingly swirled in his consciousness and forced him to psychologically retreat. The ostrich complex also paralyzed his staff and subordinates and led to a cohesive loss of mission focus, operational initiative, and ultimately an unnecessary loss of life. As a result of the 106th's chaotic actions (or inaction) during the battle and its subsequent disintegration as a cohesive fighting force, Jones and numerous members of his command team and staff later left the battle of Saint Vith in ignominy.

In the modern-day multi-domain battlespace, there has been an exponential increase in information available to commanders compared to the battlefields of World War II.[17] There is now a virtual torrent of data gathered from a plethora of sensors that feed nonstop information for enhanced situational awareness into various information management systems.[18] This proliferation of mass data has served to paralyze commanders on both sides of the leadership coin.[19] There is the danger of too much available data, but paradoxically, the existence of that data also compels commanders and staffs to seek out more data in order to enhance their visualization and battlespace management.[20] This constant search for enhanced situational awareness by commanders and staffs leads to leadership paralysis as a consequence of simply having too many choices.[21] In order to prevent cognitive overload, effective network management is therefore key to filtering the torrent of raw data into a steady stream of manageable information.

On 21 February 2010, during Operation Enduring Freedom, a seemingly routine cordon and search mission involving multiple sensors, weapons systems, and supported by personnel across continents, unfolded in Uruzgan Province, Afghanistan.

An official investigation launched in the aftermath of the incident outlined the following in the official report:

> On 21 February 2010, up to 23 local Afghan nationals were killed and 12 others injured when the convoy they were travelling in was mistaken for an insurgent force and engaged with air to ground fire … initial observations appeared to indicate a threat force. The ODA commander on the ground displayed tactical patience in letting the situation develop over several hours before the engagement. The time brought by that patience was however wasted because of the Predator crew's inaccurate reporting and the failure of both command posts to properly analyze the situation and provide, control, insights, analysis or options to the ODA commander … The tragic loss of life was further compounded by a failure of the commands involved to timely report the incident.[22]

Evidently the Predator flight crew reportedly ignored or downplayed information outlining that the convoy was anything other than an attacking force.[23] However, the information provided was supposed to have been vetted through multiple knowledge management systems at other headquarters where commanders were supposed to complete a long checklist before authorizing an attack.[24]

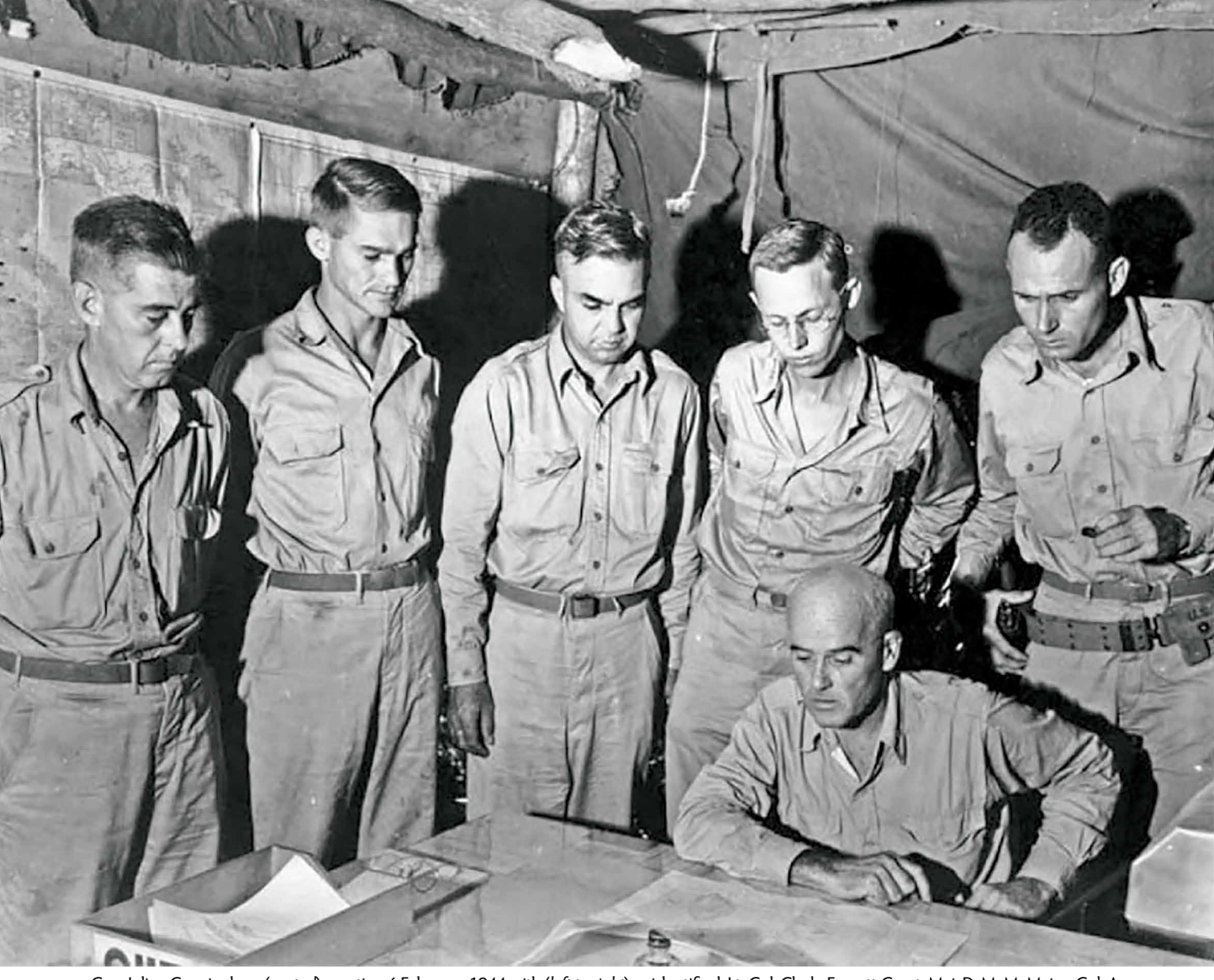
In this instance, the false confidence generated by an overreliance on the various sensors and systems and imbued with the commanders' own complexes and biases provided false situational awareness. This false positive thereby facilitated a further example of the ostrich complex where the commanders' "misperception and misinterpretation of the data" caused a paralysis of leadership and led to the unfortunate loss of life.[25]

In the modern-day battlespace, the art of command requires leaders to acknowledge and manage greater expectations in exercising authority and accepting greater responsibility for their organizations.[26] With that greater expectation and authority, there is also an increasing torrent of data, gathered from an ever increasing number of sensors.[27] There are various knowledge management processes designed to assist commanders and staff by providing them with an enhanced cognitive and situational advantage. However, the ostrich complex disrupts these processes, forcing designated commanders to retreat into their own consciousness and take a proverbial knee. This pause can be optimal under stressful conditions in order for the commander to check the "eggs" and seek clarity. However, the complex has to be quickly identified and mitigated in order to prevent commanders from burying their decisions further into the sand to the detriment of the mission. ■

Notes

Epigraph. Alvin B. Rubin and Elven E. Ponder, "The Ostrich and the Arbitrator: The Use of Precedent in Arbitration of Labor-Management Disputes," *Louisiana Law Review* 13, no. 2 (January 1953): 208, accessed 7 March 2020, https://pdfs.semanticscholar.org/bcc9/d9bad1309e3915f2244c888907f8e63ee06e.pdf.

1. Army Doctrine Publication (ADP) 6-0, *Mission Command, Command and Control of Army Forces* (Washington, DC: U.S. Government Publishing Office, 31 July 2019), 3-8.
2. Dictionary.com, s.v. "complex," accessed 7 March 2020, https://www.dictionary.com/browse/complex.
3. Garrett Hardin, *The Ostrich Factor: Our Population Myopia* (Oxford, UK: Oxford University Press, 1999), 1.
4. Ava McVean, "Ostriches Do Not Really Stick Their Heads in the Sand," Office for Science and Society, 20 August 2017, accessed 7 March 2020, https://www.mcgill.ca/oss/article/did-you-know/ostriches-do-not-really-stick-their-heads-sand.
5. Ira Robbins, "The Ostrich Instruction: Deliberate Ignorance as a Criminal Mens Rea," *The Journal of Criminal Law and Criminology 81*, no. 2 (Summer 1990): 191–234, accessed 16 March 2020, https://www.jstor.org/stable/1143906.
6. Carl Jung, *The Essential Jung: Selected Writings Introduced by Anthony Storr* (Princeton, NJ: Princeton University Press, 2013), 38.
7. ADP 6-0, *Mission Command*, 3-15.
8. H. R. McMaster, "The Pipe Dream of Easy War," *New York Times* (website), 20 July 2013, accessed 11 January 2020, https://www.nytimes.com/2013/07/21/opinion/sunday/the-pipe-dream-of-easy-war.html.
9. Carl Von Clausewitz, *On War*, ed. and trans. Michael Howard and Peter Paret (Princeton, NJ: Princeton University Press, 1984), 102.
10. Charles Whiting, *Death of a Division* (New York: Stein and Day, 1980), 21.
11. Ibid., 49.
12. Ibid.
13. Ibid., 75.
14. Ibid., 76.
15. Ibid., 78.
16. Ibid., 80.
17. Ajit Maan, *Narrative Warfare* (self-pub., CreateSpace, 2018), 9.
18. Thomas Shanker and Matt Richtel, "In New Military, Data Overload Can Be Deadly," *New York Times* (website), 16 January 2011, accessed 7 March 2020, https://www.nytimes.com/2011/01/17/technology/17brain.html.
19. Ibid.
20. Amber Corrin, "Sensory Overload: Military is Dealing with a Data Deluge," The Business of Federal Technology, 4 February 2010, accessed 7 March 2020, https://fcw.com/articles/2010/02/08/home-page-defense-military-sensors.aspx.
21. Barry Schwartz, "The Paradox of Choice," YouTube video, posted by "TED," 5:38, 16 January 2007, accessed 3 August 2020, https://www.youtube.com/watch?v=VO6XEQIsCoM.
22. Timothy P. McHale, "Executive Summary for AR 15-6 Investigation, 21 February 2010 CIVCAS Incident in Uruzgan Province" (Kandahar Airfield, Afghanistan: United States Forces-Afghanistan, 2010), accessed 7 March 2020, https://www.aclu.org/files/dronefoia/uruzgan/drone_uruzgan_attachtabA_part_01_FOIA_10-0218.pdf.
23. Ibid.
24. David Zucchino, "U.S. Report Faults Air Force Drone Crew, Ground Commanders in Afghan Civilian Deaths," *Los Angeles Times* (website), 29 May 2010, accessed 7 March 2020, https://www.latimes.com/archives/la-xpm-2010-may-29-la-fg-afghan-drone-20100531-story.html.
25. Craig Martin, "A Means-Methods Paradox and the Legality of Drone Strikes in Armed Conflict," *The International Journal of Human Rights* 19, no. 2 (2015): 142–75, https://doi.org/10.1080/13642987.2014.998864.
26. Thomas G. Bradbeer, "Lethal and Non-Lethal Fires: Historical Case Studies of Converging Cross-Domain Fires in Large-Scale Combat Operations," *Military Review* 98, no. 5 (September-October 2018): 26–32, accessed 30 July 2020, https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/September-October-2018/Bradbeer-Lethal-Nonlethal/.
27. Thom Shanker and Matt Richtel, "In the New Military Data Overload Can Be Deadly," *New York Times* (website), 16 January 2011, accessed 7 March 2020, https://www.nytimes.com/2011/01/17/technology/17brain.html.



Gen. Julian Cunningham (*seated*) meeting 6 February 1944 with (*left to right*) unidentified, Lt. Col. Clyde Everett Grant, Maj. D. M. McMains, Col. A. M. Miller, and Lt. Col. Philip Lovell Hooper in Arawe, Papua New Guinea. (Photo courtesy of U.S. Army via Wikimedia Commons)

Great Staff Officers and Great Commanders

What's the Difference?

Maj. Meghan Starr, U.S. Army

Editor's note: The author wrote this article while attending the Command and General Staff Officer Course.

To begin, I feel it is important to provide a bit of context for this article. Every author brings his or her personal bias to a project, and I feel it is prudent that I am upfront about mine. Understanding the impetus behind this article will provide the reader with the necessary perspective to approach my arguments.

About seven years ago, in the middle of my company command, I was frustrated. I had dreams of being the exceptional company commander that we all aspire to be, and that dream was not coming to fruition. Despite my aspirations, a combination of a rift between Department of the Army civilians and my soldiers, office politics, in-fighting around and above my organization seemed to cut me off at the knees whenever I started to build momentum. Someone who I highly respected, and who had seen me serve on battalion staff and in command, told me that I was just a better staff officer than a commander. Although it stung, I unquestioningly accepted that opinion. I highly respected this person, who had far more experience than me, and it was not the first time in my career that I had heard people say that to officers. Nevertheless, I finished my twenty-seven-month command, which was a perpetual roller coaster ride of successes and failures.

> A good staff officer is competent, exercises initiative, applies critical and creative thinking, is adaptable, is flexible, has self-confidence, is cooperative, is reflective, and communicates effectively.

Immediately after command, I was fortunate to have two years at a civilian graduate school that afforded me the opportunity to reflect upon my time in command. I was not used to failure in my career, and the aftermath of my command haunted me. Regardless of what my official evaluations said, I felt like a failure. For those two years, I frequently woke up in a cold sweat after having nightmares about my experience. I spent countless hours walking to and from class dwelling on what went wrong and how to do it better. By the time I graduated, I felt I had learned the lessons from the experience, and the nightmares slowly stopped. I failed to "lead up," failed to appreciate the bigger context of what my organization was doing, etc. After all, I told myself, I am a better staff officer than a commander. I just do not have what it takes to be a good commander, but at least I could do it a little better next time if I ever got the chance.

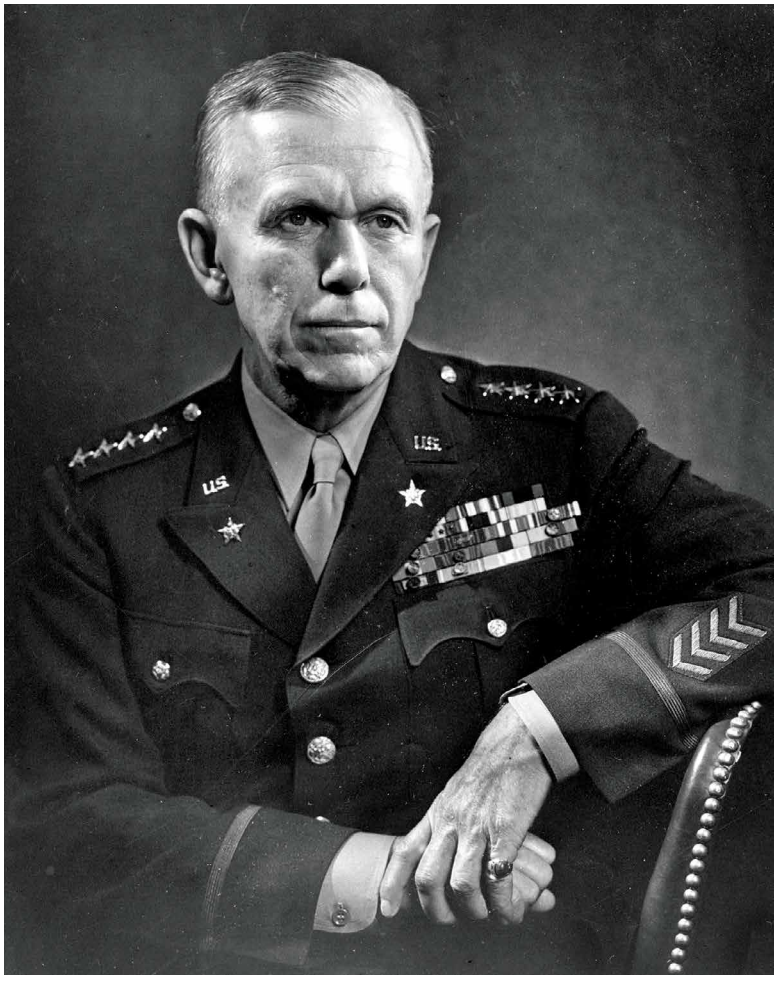
Following graduate school, I spent three years teaching at West Point, which was by far the best job of my career. I had cerebral conversations with coworkers daily, I was able to dedicate hours of my day purely to the mentorship and development of future leaders, and I was able to find and pursue my intellectual passion. "This must be what it means to be a better staff officer than commander," I told myself. Maybe success as a good staff officer did not mean "less than" success as a commander, despite many people's preconceptions; maybe it was just something different. Perhaps I could even take pride in being a good staff officer. After all, the majority of the rest of my career is going to be serving on a staff.

Now, as a Command and General Staff College (CGSC) student, I have begun to question what exactly it means to be a better staff officer than a commander. What qualities make up a good commander that a good staff officer might not have? Are there qualities that make up a good staff officer that a good commander might not have? Aren't we all supposed to be good leaders and emulate the same qualities as outlined in Army Doctrine Publication 6-22, *Army Leadership and the Profession*? If I could

Maj. Meghan Starr, U.S. Army, is a military police officer serving as the provost marshal at Joint Base Lewis-McChord, Washington. She holds a master's degree in public administration from Columbia University and a Master of Military Art and Science (Art of War Scholar) from the U.S. Army Command and General Staff College. Her previous assignments include assistant professor at the U.S. Military Academy, commander of the 73rd Military Police Detachment, plans officer for the 97th Military Police Battalion, and company executive officer and platoon leader in Company E, 7th Battalion, 101st Aviation Regiment. Starr has one combat deployment to Afghanistan.

identify the difference between the two roles, would it be something I could work to fix, or would it be an inherent trait that cannot be changed?

As a part of CGSC's Art of War Scholar program, we have spent countless hours studying officers from a wide variety of eras and nationalities. We have studied military innovators, general staff officers, thinkers, and commanders, both good and bad. The more I study these historical officers, the less I see a difference between a good staff officer and a good commander. If I had to hypothesize, I would say the one distinguishing characteristic of a good commander is charisma, but that is certainly not universal.



A portrait of Gen. George C. Marshall taken 1 January 1947. Though serving three times as a regimental or brigade commander in his career, Marshall never commanded in combat. He spent the majority of his career as a staff officer, combat developer, and instructor, rising to become chief of staff under Presidents Franklin D. Roosevelt and Harry S. Truman and attaining the five-star rank of general of the Army. During World War I, he served in France as a staff member of the American Expeditionary Forces under Gen. John J. Pershing and was a key planner for American operations. During World War II, he oversaw the largest military expansion in U.S. history and served as presidential advisor for overall management of the conflict. (Photo courtesy of the Dutch National Archives via Wikimedia Commons)

This article will analyze what the difference is between an effective staff officer and an effective commander, and if there is any difference, I will determine whether it is something "fixable." To answer this question, I used three approaches: doctrine, history, and discussions with the military community. None of these approaches are exhaustive, but they provide a baseline for leaders to think about this further.

Doctrine

I started my research where any good officer should: doctrine. Surprisingly, I found little discussion devoted to the differences between the qualities of a staff officer and those of a commander. Doctrine, generally speaking, approaches leadership as a task that all officers, regardless of assignment, must be able to perform. The leader attributes and core competencies listed in Army Doctrine Publication 6-22 are considered universal. There are no specifications as to whether certain attributes or competencies are more important than others in the context of an officer's assigned duties. The development of these traits is also universal, and it is the responsibility of all officers, not just commanders. According to Field Manual (FM) 6-22, *Leader Development*, "responsibility for leader development cuts across all leader and staff roles."[1]

The only doctrinal reference that makes a distinction between the particular attributes of a commander and a staff officer is FM 6-0, *Commander and Staff Organization and Operations*, which states that "in addition to the leader attributes and core competencies addressed in Army leadership doctrine, a good staff officer is competent, exercises initiative, applies critical and creative thinking, is adaptable, is flexible, has self-confidence, is cooperative, is reflective, and communicates effectively."[2] It goes on to articulate the role of the commander: "Commanders are responsible for all their staffs do or fail to do. A commander cannot delegate this responsibility. The final decision, as well as the final responsibility, remains with the commander. … Commanders provide guidance, resources,

and support. They foster a climate of mutual trust, cooperation, and teamwork."[3] Aside from FM 6-0, no doctrinal distinction between the qualities of a command and a staff officer exist. After reading the qualities of a good staff officer in FM 6-0, I was left wondering how an officer with all of those qualities could possibly fail to be a good commander. In search of a better answer, I turned to history to understand the evolution of the role of the military staff and its relationship with commanders.

Lt. Gen. Laura J. Richardson, commander, U.S. Army North (USARNORTH), speaks to the soldiers of Company D, 3rd Battalion, 187th Infantry Regiment, 3rd Brigade Combat Team, 101st Airborne Division (Air Assault), 24 December 2019 at a mobile surveillance camera site in Del Rio, Texas. As an Army aviator, Richardson flew Sikorsky UH-60 Black Hawk helicopters. Promoted to general officer, she subsequently served in a variety of staff and command positions including deputy commanding general–support for the 1st Cavalry Division at Fort Hood, deputy commanding general of U.S. Army Forces Command, and chief of staff for communication in the International Security Assistance Force in Afghanistan. Richardson assumed command of USARNORTH on 8 July 2019. (Photo by Staff Sgt. Mark Torres, U.S. Army)

History

The role of commanders and staffs has a complex and evolving history. Napoleon Bonaparte did his own planning. The role of his staff was to write down the plan he dictated, then deliver it to subordinate units. As other nations struggled to adapt to Napoleon's military genius, they realized that few could match him alone on the battlefield. It is impossible to discuss this without mentioning Carl von Clausewitz, who argued that two qualities are required for true military genius: coup d'oeil (the intellect) and courage d' esprit (determination).[4] Clausewitz went on to argue that to find one man with both of these qualities is rare. The solution was to equip commanders who lacked such comprehensive talents with a more robust staff so that multiple minds could combine to combat the rare military genius.

During this time, however, the American military, while taking some concepts from Prussia, still relied on the French model of command through the Civil War. Staffs were small, and the Army did not utilize staffs' potential. Napoleon's armies, with all of their successes, were the standard to which the United States aspired. It was not until 1866 and the Prussian alliance won the Battle of Königgrätz that the United States started to devote greater attention to the Prussian way of war.[5]

The Prussians realized that the battlefield was more complex with the advent of railroads, telegraphs, and other technologies, and it was impossible for one man to manage alone. Helmuth von Moltke the Elder, influenced by Clausewitz's writings, completely restructured professional development for officers and designed the *Kriegsakademie* (war academy). This led to the creation of the Prussian General Staff and a career path dedicated to developing exceptional staff officers. Units would have a commander and a general staff officer who shared in the decision-making responsibility. One officer might have robust combat experience, while the other might have significant military education and training. When Moltke passed, however, his successors failed to maintain

the system. Where Moltke had been able to integrate new technology into systems for the general staff, his successors were unable to incorporate the new technologies of their time (e.g., balloons and a more robust navy).[6] As the American military's attention turned to emulating the Prussian education system, Prussia's system was devolving. The professionalization of the American officer corps, however, was a turning point as reformers like former Secretary of War Elihu Root strove to improve the education and organization of the officer corps.[7]

The Germans maintained the general staff system, but it resembled its original concept less and less. Instead of staff officers rotating between staff assignments and command, many senior staff officers at the dawn of World War II had little command experience and minimal combat experience from World War I.[8] Admittedly, this also had much to do with the significant downsizing of the German army as a result of the Versailles Treaty. The performance of these staff officers in combat is, at best, mixed. Rather than prize its general staff officers, the army thus began to value its commanders and lost respect for those staff officers whose mistakes in command cost thousands of lives.[9] This divide between commanders and staff officers permeated the American military as well. Commanders, held in high esteem, often looked down their noses at staff officers who had an unproven track record in command.[10]

While studying the use of the military staff and how staff officers were viewed is helpful, perhaps the greatest historical insight into the different qualities of staff officers and commanders is from Gen. Kurt von Hammerstein-Equord, commander in chief of the Reichswehr from 1930 to 1934:[11]

> I distinguish four types. There are clever, hardworking, stupid, and lazy officers. Usually two characteristics are combined. Some are clever and hardworking; their place is the General Staff. The next ones are stupid and lazy; they make up 90 percent of every army and are suited to routine duties. Anyone who is both clever and lazy is qualified for the highest leadership duties, because he possesses the mental clarity and strength of nerve necessary for difficult decisions. One must beware of anyone who is both stupid and hardworking; he must not be entrusted with any responsibility because he will always only cause damage.[12]

Hammerstein-Equord's sentiment is seen today in the form of a chart (see table). I used this chart when I began the next phase of my analysis: discussions with the military community.

Table. Hammerstein-Equord's Four Types of Leaders

Types of officers	Hardworking	Lazy
Clever	Appoint to the general staff	Highest leadership duties
Stupid	Remove	Routine duties

(Table by author)

Discussions

Armed with the Hammerstein-Equord chart, I started a discussion on #miltwitter, Facebook, and with my CGSC staff group to solicit the opinions of others. The participants were a combination of enlisted (sergeant first class through command sergeant major) and officer (captain through lieutenant colonel). In all cases, the debate was impassioned and thoughtful.[13] Here I was able to finally draw some conclusions. Several themes emerged in the debate:

- *There is absolutely a difference between what makes a good staff officer and what makes a good commander.* After a long debate, the consensus on all platforms was that the attributes and competencies required of both were the same; however, they should be weighted differently. The top three attributes necessary for command are not the top three attributes required for staff work.
- *It is much easier for someone in the "stupid" category of the chart to survive on staff than in command.* Most disagreements occurred when people referred to the qualities needed to be a sufficiently competent staff officer instead of a good one. Many mediocre officers can "hide" on staff, but they cannot hide when they are eventually led to the perception that being a staff officer is easier than being a commander or

requires less skill. Once reoriented to address the qualities that make a *good* staff officer, most agreed with the first point above.

- *Two particular qualities tend to be the largest discriminators in the criteria for a good commander and a good staff officer*. These qualities are charisma (the ability to inspire soldiers to do physically hard tasks) and audacity (the ability to make decisions and accept appropriate risk). Examples of both certainly permeate history. The ability to accept risk, in particular, is tied to what Hammerstein-Equord meant by a great commander being "lazy." A commander may often need to make decisions with imperfect or incomplete information, relying on what is available to make the best decision possible. There often is not time to do further analysis or research, and a "lazy" commander is willing to accept the necessary risk to make a "good enough" decision on time rather than wait for perfect information in order to make the perfect decision or choose the perfect course of action.
- *It is possible for a great staff officer to transition into a great commander, but few know how*. The consensus was that most people had seen examples of officers who were great at both roles and that being "smart" makes that transition easier. Unfortunately, how to transition between roles was left under the umbrella of "self-development" with few tips for the officer trying to make that transition. The only consensus was that it was highly individual and could not be done through large CGSC courses. Part of the need for a solution, however, comes from little thought on this topic and too much focus on universal leadership traits or preparing for command. Most people do not receive training on the specific leadership traits required to be a great staff officer. Instead, they receive training on how to use systems (e.g., manage a budget, the military decision-making process, etc.).

Conclusion

After researching doctrine and history and combining it with excellent discussion, I agree with the conclusions of the discussion above. The skill sets required to be a great commander and a great staff officer are different but only in priority. I am still not sure if it is possible to transition from one to the other, in either direction. Personally, I have identified the areas that I need to develop in order to make that transition, and I will strive to do so. Time will only tell if I am successful. I am still left wondering, however, why being a great commander is considered superior to being a great staff officer if both require the same attributes. My best estimate is that few people take time to distinguish between the mediocre and the great staff officer, and many perceptions are colored by mediocre performances. I wonder if asking more senior commanders, those above the level of battalion command, would provide more insight. This is but one of the many remaining questions that ought to be researched further. For my own journey, however, I think I have found what I need to move my own development forward. ■

Notes

1. Field Manual (FM) 6-22, *Leader Development* (Washington, DC: U.S. Government Publishing Office, June 2015), 2-1, accessed 7 August 2020, https://armypubs.army.mil/epubs/DR_pubs/DR_a/pdf/web/fm6_22.pdf.

2. FM 6-0, *Commander and Staff Organization and Operations* (Washington, DC: U.S. Government Printing Office, May 2014), 2-4.

3. Ibid.

4. Carl von Clausewitz, *On War*, ed. and trans. Michael Howard and Peter Paret (Princeton, NJ: Princeton University Press, 1976), 102.

5. Jorg Muth, *Command Culture* (Denton, TX: University of North Texas Press, 2011), 19.

6. Ibid., 26.

7. Stephen Skowronek, *Building a New American State: The Expansion of National Administrative Capacities, 1877–1920* (Cambridge, UK: Cambridge University Press, 2003), 88.

8. Muth, *Command Culture*, 27.

9. Ibid.

10. Ibid., 27–28.

11. "Kurt Freiherr Von Hammerstein-Equord," Gedenkstätte Deutscher Widerstand (German Resistance Memorial Center), accessed 1 April 2020, https://www.gdw-berlin.de/en/recess/biographies/index_of_persons/biographie/view-bio/kurt-freiherr-von-hammerstein-equord/?no_cache=1.

12. Horst Poller, *Conquered Past: The 20th Century, Witnessed, Endured, Shaped* (Munich: Olzog Verlag, 2010), 140.

13. For transcripts of these discussions, please contact the author.

Multi-Domain Operations and Information Warfare in the European Theater

Maj. Jennifer L. Purser, U.S. Army

The U.S. military is undergoing a major doctrinal transition from a counterinsurgency-focused fight to large-scale combat operations (LSCO). In the European theater, this evolution arguably began in late 2014. The United States did not execute a palpable response to Russia's military incursion into Georgia (a U.S. partner) in 2008, and with a second bold Russian military move that was the 2014 Crimean annexation, the United States strategically needed to stage a military response of some kind. However, the Russian threat demanded a U.S. doctrinal change in order to effectively counter the near-peer adversary. Likewise, Russia is one of America's most experienced adversaries in the realm of information warfare (IW). Therefore, in contemporary warfare (i.e., LSCO), the U.S. capability of setting a theater to both apply IW and defend against enemy IW is paramount. Because of the case's relevance to LSCO, multi-domain operations (MDO), and IW, I will describe successful strategies for setting the theater from an IW perspective using a case study from the European theater between 2015 and 2019.

Relevant Terms Defined

Before fully launching into the case study details, defining a few applicable terms is necessary. According to the Center for Army Lessons Learned, "setting the theater" (STT) is a "continuous shaping activity to establish favorable conditions for the rapid execution of military operations."[1] Most Department of Defense publications provide a largely logistics-centric definition to STT; however, two key tasks annotated for STT in Field Manual 3-94, *Theater Army, Corps, and Division Operations*, include "providing force protection," and "modernizing forward-stationed Army units."[2] These tasks are critical to enabling successful MDO from an IW perspective in the European theater.

> MDO are the ways and means for the joint force [Army, Navy, Air Force, and Marine Corps] [to] counter and defeat a near-peer adversary capable of contesting the U.S. in all domains [air, land, maritime, space, and cyberspace] in both competition and armed conflict [emphasis added by author]. … … MDO provides commanders numerous options for executing simultaneous and sequential operations using surprise and the rapid and continuous integration of capabilities across all domains to present multiple dilemmas to an adversary in order to gain physical and psychological advantages and influence and control over the operational environment.[3]

A critical element to MDO is the electromagnetic spectrum (EMS), especially as it relates to IW. Joint Publication (JP) 3-0, *Joint Operations*, posits, "The joint force is critically dependent on the EMS for operations across all joint functions and throughout the OE … therefore, the joint force should strive for local EMS superiority prior to executing joint operations."[4]

A Department of Defense primer on information operations (IO) maintains that IW and IO are linked in the context of military MDO.[5] As such, JP 3-13, *Information Operations*, defines IO (and IW in this context) as the "integrated employment, during military operations, of information-related capabilities in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision making of adversaries and potential adversaries while protecting our own."[6] IO relies upon cooperation with various related entities to include strategic communications, public affairs (PAO), interagency coordination, civil-military operations, cyberspace operations, information assurance, space operations, military information support to operations (MISO), intelligence, military deception, operations security, and joint electromagnetic spectrum operations (JEMSO), among others.[7] Within this context, MISO focuses on "the cognitive dimension of the information environment" and as such, relates heavily to the effects of disinformation and cyber/electronic warfare on a society.[8] JEMSO, also referred to as cyber/electronic warfare operations, "are the coordinated efforts of EW [electronic warfare] and joint electromagnetic spectrum management operations to exploit, attack, protect, and manage the electromagnetic operational environment."[9] Examples include jamming communications (a Russian favorite), electromagnetic interference/interception, and even utilizing bots and trolls in social media. Signals intelligence (SIGINT) "is intelligence produced by exploiting foreign communications systems and noncommunications emitters. SIGINT subcategories include COMINT [communications intelligence], ELINT [electronic intelligence], and FISINT [foreign instrumentation signals intelligence]."[10] SIGINT plays a significant role in JEMSO because of its role in collection and exploitation of elements of the EMS. Planners must coordinate for all entities that affect IO in order to adequately set the theater for MDO.

Case Study: Combatting Russian IW during Atlantic Resolve Operations 2015-2019

As a response to Russia's annexation of Crimea, Operation Dragoon Ride 2015 (ODR '15) was a

Previous page: Completing the first leg of their tactical road march from Rose Barracks, Germany, to Tapa Military Training Area, Estonia, soldiers of the 2nd Cavalry Regiment drive their Strykers into Ruzyne, Czech Republic, 27 May 2016 during Operation Dragoon Ride. The soldiers were met by a crowd of Czech citizens who showed their support for the U.S. presence in the Czech Republic. On their journey, approximately 1,400 soldiers in four hundred vehicles traveled over 2,200 kilometers through six countries. Dragoon Ride is conducted to validate U.S. partnering allies' abilities to assemble forces rapidly, deploy them on short notice, and improve the ability to shoot, move, and communicate as a multinational allegiance. (Photo by Sgt. Caitlyn Byrne, U.S. Army)

high-profile and controversial U.S. Army Europe (USAREUR) tactical convoy. A squadron of 2nd Cavalry Regiment (2CR) Stryker vehicles with additional logistical and support elements traveled in a convoy almost two thousand kilometers from Estonia back to their home base in Vilseck, Germany, through the Baltics, Poland, and the Czech Republic. Largely because of the convoy's representation as a symbol against Russian adventurism, pro-Russian IW actors were prevalent during ODR '15. Associated disinformation contributed to the convoy's controversy and had a significant impact on society in the countries through which the convoy transited. As a result of ODR '15 and subsequent Atlantic Resolve convoys, combined with a changing IW landscape (an uptick in pro-Russian disinformation and IW attempts), tactics and techniques used in the European theater to counter IW have ebbed and flowed over the past five years. Two primary public relations models and counter-IW techniques have emerged, one advocating preempting enemy IW through high-profile U.S. presence in the press and the other espousing a quieter public approach. Both strategies have proven effective at setting the theater to combat disinformation and IW.

Under the leadership of Lt. Gen. Ben Hodges, USAREUR employed the active-messaging technique, specifically during ODR '15. ODR '15's intent, as Hodges explained during an interview, was fourfold in the wake of Russia's annexation of Crimea: (1) to show NATO partners that the United States was willing to defend them; (2) to show Russia that the U.S. would come to the aid of a partner in the event of a Russian incursion

U.S. Army Staff Sgt. Marion Szwcyk, weapons squad leader from Apache Troop, 1st Squadron, 2nd Cavalry Regiment, Battle Group Poland, briefs Polish army soldiers from the 15th Mechanized Brigade on range cards 7 June 2018 during Saber Strike 18 in Wyreby, Poland. (Photo by 1st Lt. Erica Mitchell, Michigan Army National Guard)

On 23 March 2015, day three of Operation Dragoon Ride, soldiers from Iron Troop, 3rd Squadron, 2nd Cavalry Regiment, visit the town of Panevezys, Lithuania. A large crowd of onlookers came out to interact with the soldiers and take pictures of themselves with the U.S. Stryker armored vehicles. (Photo by Sgt. 1st Class John Wollaston, U.S. Army)

into a NATO state; (3) to conduct a logistical reconnaissance (in preparation to defend against possible Russian hostility); and (4) to send a message to policy makers in the United States that more troops, training, and military might was needed in the European theater to ensure NATO's integrity.[11] In the meantime, Hodges aspired to make the thirty thousand U.S. troops who were then stationed and operating in Europe look and feel like a three hundred thousand-troop-strong economy of force (a significant IO undertaking in its own right). Some of USAREUR's IO-related strategies during ODR '15 included employing intelligence, signal/communications, PAO, and IO reserve entities to augment U.S. European active forces, bolstering NATO allies to enable enduring strategic defense against Russia, and maintaining a dynamic presence—meaning a moving, visible, capable, professional force—in order to deter Russian adventurism in the Baltics and potentially elsewhere.[12] The U.S. European Command (EUCOM) employed PAO and IO elements in abundance to amplify the pro-U.S. message and counter the Russian narrative to foreign and domestic audiences alike.[13] Accordingly, ODR '15 incorporated focused, preemptive PAO messaging to include press releases before mission commencement and after mission completion to discuss the U.S. military objective in the convoy. ODR '15 also placed an emphasis on conducting numerous static displays, command meet-and-greets, public commemorations, and even a concert. All these events were covered by the press.

However, because of the high-profile public messaging from the U.S. side during ODR '15, large-scale pro-Russian IW activities were lodged against convoy operations with the goal of undermining the true mission objectives of said operations. Though U.S./NATO elements tracked and tried to counter IW attempts, they were not always successful in countering falsehoods. Russian IW success made some countries less willing to host large-scale U.S. convoy events. Disinformation surrounding ODR '15 caused both public protest as well

as positive responses to opposition protests. Public activism, whether positive or negative, can be troublesome for the political environment of a host country. Further, no matter how carefully planned a convoy operation, a host nation will experience some inconvenience (e.g., traffic delays, property damage, etc.). As such, host-nation appetites for large, public convoys waned somewhat in the European theater after ODR '15.

Thus, as annual Atlantic Resolve convoys became common, the propensity for missions to be high-profile became less common. In fact, troops noticed that higher-profile convoys attracted more IW attempts. According to recent tactical leaders serving under USAREUR, sometimes the best way to combat disinformation surrounding an operation is to reduce the attention on it altogether, thus negating the likelihood of IW.[14] The "smaller footprint" approach to contemporary Atlantic Resolve convoys was exemplified during a more recent operation, 2CR's 2018 iteration of Saber Strike. At the suggestion of host-nation governments, the convoy maneuvered through neighboring countries overnight (as opposed to during the day). U.S. military and host-nation political leaders recommended the low-profile approach as a result of societal reactions to previous convoys that had experienced various negative effects from Russian IW.

Maj. Jennifer L. Purser, U.S. Army, is a military intelligence officer serving as the 101st Airborne (Air Assault) Division Analysis and Control Element (ACE) chief. Purser has served with the 201st Expeditionary Military Intelligence Brigade, U.S. Army Special Operations Command, and the U.S. Army Information and Security Command. Most recently, she was an Olmsted Scholar assigned to Brno, Czech Republic, at Masaryk University. Her studies focused on disinformation, hybrid warfare, and European security threats. She holds a BA from the College of William and Mary, an MA from American Military University, and an MA from Masaryk University.

Strategies for Setting the Theater to Counter Enemy IW

This section will discuss several unclassified tactics, techniques, and procedures (TTPs) the joint force can apply to help counter adversarial IW actions while promoting friendly operations. Core values and national narratives are important to setting the joint theater for IW success. EUCOM's former digital media chief said, "The Russian government is OK with spreading falsehoods. Conversely, U.S. culture is rooted in the belief of honesty and fact. And that is the best way to combat Russian IW—by spreading the truth."[15] A USAREUR IW expert echoed the same notion:

> Combating disinformation is all about a cultural battle of values. The U.S. military must continue to display truth, humanity, and a fairness in how we treat people, and continue to provide evidence that the disinformation reports which suggest we are willing to lie, run over people, kill people, etc., are false. If the U.S. loses credibility, it's a slippery slope.[16]

To reinforce combating disinformation, the USAREUR disinformation expert advocated publishing "fact sheets" before operations as TTP. He said,

> We publish fact sheets for Atlantic Resolve missions which contain the ground truth facts. Then we share them around social and mainstream media as much as possible. We control the narrative by publishing what is really happening before any IW or disinformation agents can put a spin on anything. When Russia Today (RT—a state-backed Russian media company) says something like "the US is deploying 400 tanks in Europe," and the previously published Fact Sheet says something completely different, it is pretty easy to see RT is spreading a falsehood.[17]

He continued,

> The Russians paid attention. They exploited what we did when we kept operations a secret, now we preclude them from that ability to exploit our secrecy because we don't keep anything a secret anymore. They cannot take advantage of that any longer.[18]

Promoting fact-checking within the journalism community can assist in setting the theater for U.S. success in the IW realm. The USAREUR IW/disinformation expert also said,

> Since Crimea, professional media outlets like AP, Reuters, and other Western media, have changed how they report things. In fact, outlets are going back to so-called "old-school" journalism and have started cracking down

After returning from supporting Battle Group Poland and NATO's Enhanced Forward Presence initiative, the 3rd Squadron, 2nd Cavalry Regiment, conducts a maneuver rehearsal of concept 27 May 2018 to prepare for its departure to Saber Strike 18. The day after the image was tweeted, *Voennoe Obozrenie* (Military Review), a Russian media outlet that covers military affairs, published an article titled "NATO servicemen are carrying out the seizure of Kaliningrad during 'Saber Strike-18' exercise." The article also stated, "We remind that in NATO countries, as well as in Russia, servicemen put on the map the symbols of likely enemies in red. You can see well that on the map the red color indicates the Russian Kaliningrad." (Photo courtesy of 2nd Cavalry Regiment Twitter. Supporting information courtesy of Atlantic Council's Digital Forensic Research Lab [@DFRLab] via Medium.com)

> on fact-checking. We don't see nearly as many examples of disinformation ending up in Western mainstream media.[19]

He added that an array of policy changes across Europe have advocated tightening good journalism rules within many countries and contributed to better reception toward U.S. operations than in the past.[20]

EUCOM's former digital media chief suggested that an effective strategy at promoting facts and winning the narrative during operations is aligning on a tagline. She endorsed this method during ODR '15, and it helped to reverse the negative social media narrative about the operation. Troops painted #DragoonRide on Strykers and other trucks.[21] The #DragoonRide tagline allowed anyone with a smartphone to tie their experience with the convoy in real time, which crippled IW attacks on social media. In fact, according to a 2015 Atlantic Resolve report about social media, using hashtags aligned with the tactical mission (e.g., #DragoonRide) in conjunction with taglines of the operational or strategic mission (e.g., #AtlanticResolve or #StrongEurope) increased visibility by up to 10 percent or more and also helped nest ODR '15's mission within the overarching framework.[22] Visibility amplified public knowledge of the operation's objectives and helped combat adversary IW.

Recent 2CR public affairs and civil affairs leaders shared some techniques for preventing the opportunity for disinformation agents to manipulate a story from the beginning. They mentioned a "no maps rule" for 2CR social media, which the unit adopted during a Saber Strike exercise in 2018. According to the team, 2CR posted a picture with various regimental leaders huddled around

(Screenshot and quote below courtesy of Atlantic Council's Digital Forensic Research Lab [@DFRLab] via Medium.com)

Headlines of Articles Published on Russian Propaganda Social Media Outlets in Response to Saber Strike 2018

> Unfortunately, few people realize that Anglo-Saxons deploy a military contingent there, this contingent in particular, because the exercise and other exercises are just a cover for military equipment transfer. In fact, it is a direct confrontation with the Russian Federation. This loss is most immediate for the civilian population, as the level of security of the countries is close to zero. We cannot but react to this situation, therefore, prostitutes are happy, political prostitutes receive money from the Anglo-Saxons to trade their national interests. Where ever you look—prostitutes win.
>
> —Alexander Zhilin, reputed Russian military expert, as said to Sputnik, 9 June 2018

a map, planning transportation routes for the exercise. The photo was intended to reflect effective communication and team camaraderie. Kaliningrad, a small Russian territory in the Baltics, was colored in red on the map to ensure no convoy movements traversed through the territory.[23] However, Pravda.ru (another state-backed Russian media company, similar to RT) used the map to spread disinformation claiming, "Saber Strike 2018 is a provocation against the Russian Federation and NATO/USA will train how to isolate and occupy Kaliningrad."[24] 2CR leaders also indicated that they collaborate with host-nation military and IW teams as much as possible, as NATO partners often have more experience with Russian IW than their U.S. counterparts.[25]

In response to other changes in U.S./NATO TTPs for setting the theater to facilitate success in the IW realm, the USAREUR IW expert suggested coordination and deconfliction as tools to combat enemy IW.[26] He said,

> U.S. leaders must understand the impact of our actions. The fewer opportunities we give platforms like RT to find a "kernel

> of truth," the more we can neutralize IW before it even begins. After ODR '15 we started anticipating more in our planning, making deliberate attempts to publish pre-coordinated information with ample lead time before the operations. We didn't want local communities to be surprised by a U.S./NATO convoy. Causing unexpected traffic backups could affect public sentiment negatively, which is opposite of the message we want to convey.[27]

Conclusion

The U.S. military doctrine shift toward LSCO with an IW-savvy Russia representing one of America's most capable adversaries makes the European theater a prime example of the importance of setting the theater for MDO from the IW perspective. IO and IW are linked to a wide array of contributing fields including JEMSO, MISO, SIGINT, cyber, PAO, and signal/communications, to name a few. This work analyzed unclassified measures U.S. military leaders have employed within the European theater after 2014 that have set the conditions for favorable friendly IW and have been successful at countering enemy IW. Examples include two broad PAO strategies, one espousing elevated operational presence in the media and among host nations, the other advocating the opposite—remaining as low profile as possible. Each represents a strategy toward enabling successful offensive and defensive IW operations. Similarly, TTPs that facilitate U.S. dominance in the IW landscape include publishing fact sheets, advertising linked operational taglines, promoting fact-checking among the journalism community, coordinating release of relevant operational plans in a timely manner, and reducing public opportunities for exploitation. Finally, relentlessly maintaining U.S. operational transparency to both foreign and domestic audiences sets the firmest foundation for enabling MDO from an IW perspective. ■

The views expressed are those of the author and do not reflect the official policy or position of the U.S. Army, Department of Defense, or the U.S. government.

Notes

1. Center for Army Lessons Learned (CALL), *Set the Theater*, Catalog No. 19-10 (Fort Leavenworth, KS: CALL, March 2019), 1, accessed 12 August 2020, https://usacac.army.mil/sites/default/files/publications/19-10.pdf.
2. Field Manual 3-94, *Theater Army, Corps, and Division Operations* (Washington, DC: U.S. Government Printing Office, 21 April 2014), 2-9.
3. Andrew Feickert, *Defense Primer: Army Multi-Domain Operations (MDO)*, No. IF11409 (Washington, DC: Congressional Research Service [CRS], 16 January 2020), 1.
4. Joint Publication (JP) 3-0, *Joint Operations* (Washington, DC: U.S. Government Publishing Office, 17 January 2017), VIII-6.
5. Catherine A. Theohary, *Defense Primer: Information Operations*, No. IF10771 (Washington, DC: CRS, 18 December 2018), 1.
6. JP 3-13, *Information Operations* (Washington, DC: U.S. Government Printing Office, 20 November 2014), ix.
7. Ibid., II-5–II-13.
8. Ibid., II-9–II-10.
9. JP 3-13.1, *Electronic Warfare* (Washington, DC: U.S. Government Printing Office, 8 February 2012), vii.
10. JP 2-0, *Intelligence* (Washington, DC: U.S. Government Printing Office, 22 October 2013), B-5–B-6.
11. Ben Hodges (former commanding general, U.S. Army Europe [USAREUR]), interview by the author, 7 November 2018, Prague, Czech Republic. Record and transcription in author's archive.
12. Ibid.
13. Ibid.
14. X. X. (three members of 2nd Cavalry Regiment), interviews by the author, 13 February 2019, Vilseck, Rose Barracks, Germany (2019 a, b, and c). Record and transcription in author's archive.
15. J. W. (former digital communications chief, U.S. European Command), telephone interview by the author, 20 November 2018; follow-up interviews via email between 21 November 2018 and 30 November 2018. Record and transcription in author's archive.
16. R. P. (USAREUR information warfare/disinformation expert), telephone and email interviews by the author, 21 November 2018. Record and transcription in author's archive.
17. Ibid.
18. Ibid.
19. Ibid.
20. Ibid.
21. J. W., interview.
22. Richard Takacs, *Atlantic Resolve Social Media Environment Baseline Assessment* (Grafenwoehr, Germany: 4th Infantry Division Mission Command Element, 2015), 10.
23. X. X., interview.
24. Lithuanian Armed Forces (LAF), *Strategic Communication Department: Disinformation Hostile Information Activity* (Vilnius, Lithuania: LAF, June 2018), 1.
25. X. X., interview.
26. R. P., interview.
27. Ibid.

Thunderbolt soldiers use their lunchtime to take advantage of a holistic health and fitness combat-mobility yoga session 26 February 2020 at the 5th Battalion, 3rd Field Artillery headquarters at Joint Base Lewis-McChord, Washington. These yoga sessions are designed to improve overall mental wellness and increase core strength and mobility. (Photo by Sgt. Casey Hustin, U.S. Army)

Leading the Change to Holistic Health and Fitness

Sgt. Maj. Jason M. Payne, U.S. Army

In fiscal year 2021, the Department of the Army will reach an initial milestone in a planned cultural shift. The Army will formalize a holistic health and fitness (H2F) program that will consolidate and overhaul existing programs and events such as the Army Physical Fitness Test, the Ready and Resilient Campaign, physical readiness training (PRT), and Army wellness centers. While the Army Combat Fitness Test (ACFT) is the most popular event related to H2F, the new system is a generational initiative that "represents a cultural shift" the Army is willing to invest in considerably.[1] Director of research for the Army Center for Initial Military Training (USACIMT) Michael McGurk acknowledges, "Holistic health and fitness is a radical change. … It is going to cost the Army money, time, and people. And we've got to be willing to give that up."[2]

According to Chad Garland of *Stars and Stripes*, "The Army, the largest branch, saw soldiers suffering

the highest rates of injury, behavioral health disorders, and sleep disorders."[3] Furthermore, "Unit training was promoted without regard to individual Soldiers' needs. H2F doctrine changes that paradigm by directing the Army to train the whole Soldier with an individualized program."[4] In order to successfully integrate an H2F program that promotes an adequate lifestyle balance within the performance triad of sleep, nutrition, and exercise, the Army must accomplish four core tasks: acquire the necessary talent, develop knowledgeable H2F senior leaders, update overlapping H2F doctrine, and provide the necessary physical resources.

The Problem and Need for Change

In 2006 and 2011, the Joint Chiefs of Staff commissioned working groups to determine the most prevalent types and causes of injury to service members. The 2006 working group ranked the leading types of injuries based on the aggregate number of days that troops were on a temporary profile, and the group correlated that data with events and activities that contributed to soldier injuries.[5] According to the Department of Defense's Military Injury Prevention Priorities Working Group, the top five most commonly occurring musculoskeletal injuries were "(1) lower extremity overuse, (2) lower extremity fractures, (3) upper extremity fractures, (4) torso overuse, and (5) lower extremity sprains and strains … [and among] the leading causes of injury were … sports and physical training."[6] During fiscal year 2016, medical costs for these injuries totaled approximately $475 million, and the Department of the Army spent an additional $27 million to cover inpatient behavioral health treatments.[7]

As such, the Army requires a comprehensive overhaul of its programs designed to ensure readiness, which includes physical training, behavioral health, and obesity reduction through nutrition-focused education. This systemic overhaul needs to align more with the Department of Defense's framework for total force fitness. The special operations community has experienced success in all of these focus areas after successfully implementing the Tactical Human Optimization, Rapid Rehabilitation and Reconditioning program; however, the Army's conventional forces lack the resources and experienced personnel to implement the Tactical Human Optimization, Rapid Rehabilitation and Reconditioning program across its ranks.

Acquire Necessary Talent

There is high demand for tangible resources for the H2F system. The Army's senior leaders are willing to pay for it, but the steepest challenge will be finding the means to do so. The new H2F program organizes healthcare professionals tasked with educating and caring for soldiers at the unit level into human performance teams (HPTs). H2F subdivides HPTs into three specialized teams—nutrition, physical therapy, and cognitive enhancement—assigned at the brigade level (see table, page 69).[8] An HPT, which may include more than thirty personnel, will be a blend of military officers and enlisted soldiers, Department of the Army civilians, and contractors. A brigade's authorized strength will determine the number of specialists and providers assigned to its HPT. H2F will classify the Army's nearly fifty brigade combat teams and training brigades as either tier 1, tier 2, or tier 3 based on authorized personnel strength. At that rate, the projected end strength of providers totals more than one thousand, and the Army will face challenges to staff all brigade HPTs.

Hiring challenges: The case for a direct commissioning program. While USACIMT and other senior leaders recognize the necessity for a full complement of registered dieticians, physical therapists and occupational therapists, athletic trainers (ATs), strength and conditioning coaches (SCC), and other healthcare specialists, the price tag for so many Army civilians and contractors presents a significant challenge. If the Army cannot afford to hire hundreds of specialists to fill these requirements, senior leaders should consider direct commissioning programs and internships to fill in the talent gap.

According to the U.S. Labor Department's Bureau of Labor Statistics, the median salary for healthcare specialists are as follows: physical therapists ($88,000/year), occupational therapists ($85,350/year), registered dieticians ($61,210/year), and ATs ($49,280/year).[9] ATs and SCCs, which represent the largest pool of the HPT construct, command the smallest salary of the aforementioned professions;

Sgt. Maj. Jason M. Payne, U.S. Army, is assigned to the U.S. Army Cyber Center of Excellence and also serves as the Fort Gordon Postpartum Pregnancy Physical Training program manager. He holds a BS in criminal justice from Troy University. His previous assignments and duties include first sergeant, drill sergeant, and master fitness trainer.

Staff Sgt. Gabriel Wright (*center*), a signals intelligence analyst with the 780th Military Intelligence Brigade, grades the hand-release push-up event 17 May 2019 as part of Army Combat Fitness Test Level II grader validation training at Fort George G. Meade, Maryland. (Photo by Sgt. 1st Class Osvaldo Equite, U.S. Army)

however, these individuals hold a requisite combination of a bachelor's degree in exercise science or kinesiology, certification(s) from the National Strength and Conditioning Association (NSCA), or a master's degree in kinesiology. In order for a transition to the H2F system to be successful, the Army needs to find a way to attract these individuals with competitive salaries nationwide and at overseas duty locations.

Col. Kevin Bigelman, H2F chief of the Army Center for Initial Military Training, believes the Army is postured to attract those individuals. Bigelman said, "We would go with a contractor hiring solution to begin with, but contractors are expensive. I think the [Army's] salary for those folks would be higher … so I think it would be attractive for many folks."[10] If the Army offered a direct commissioning program for unit-level ATs and SCCs, it would allow organizations to retain and develop essential H2F talent for longer periods while simultaneously benefiting units and providers. For example, if an individual with a baccalaureate degree and NSCA certification directly commissioned as a second lieutenant, that provider's annual base salary would be $45,456. Offering the rank of captain to a provider with a master's degree in kinesiology would yield an annual salary of $52,596. The addition of standard military benefits and allowances, promotion potential, and guaranteed experience working with hundreds of tactical athletes would allow the Army to attract and retain providers with minimum service obligations ranging from four to six years in length.

Enlisted talent development. If the cultural shift to a more health-focused and fitness-focused force is going to be successful, the Army also has the implied task of developing the brunt of its workforce—its junior enlisted soldiers and Noncommissioned Officer Corps. The HPT construct for nutrition, physical therapy, and cognitive enhancement teams currently calls for the following military occupational specialties: nutrition care specialist (68M), physical therapy specialist (68F), and occupational therapy specialist (68L) (see table, page 69). Through

Table. Sample Human Performance Team for a Tier 1 Brigade

Nutrition team	Physical therapy team	Cognitive enhancement team
(1) O3-O4 Officer in charge	(1) O3-O4 Officer in charge	(1) O3-O4 Cognitive enhancement director
(1) GS-12 Registered dietician	(2) O3-O4 Physical therapists	(1) O3-O4 Occupational therapist
(1) E4-E6 Nutrition care specialist (68M)	(1) E4-E6 Physical therapy specialist (68F)	(1) Civilian/contractor occupational therapist
(1) GS-6 Nutrition specialist	(1) Civilian/contractor physical therapist assistant	(1) Contractor cognitive enhancement specialist
	(7) Athletic trainers	(1) E4-E6 Occupational therapy specialist (68L)
		(1) Civilian/contractor occupational therapy assistant
		(14) Strength and conditioning coaches
Total=4	**Total=11**	**Total=20**

(Table by author. Sample team consists of Army commissioned officers, enlisted soldiers, Department of the Army civilians, and contractors)

its new credentialing assistance program, the Army should encourage professional credentialing through accredited associations such as the NSCA and National Academy of Sports Medicine. Furthermore, USACIMT should consider lengthening its Master Fitness Trainer Course and awarding a skill qualification identifier to soldiers who complete the course. This would provide units with more qualified enlisted subject-matter experts at company and battalion echelons.

Develop Knowledgeable H2F Senior Leaders

Following the results of the 2006 injury prevention working group, the Army identified a need to change its previous physical fitness training doctrine, Field Manual (FM) 21-20, *Physical Fitness Training*. This change led to FM 7-22, *Army Physical Readiness Training*, in September 2012, which was an adaptation of the Army Training and Doctrine Command's Standardized Physical Training Program.[11] PRT faced immense skepticism Army-wide, and many commanders were reluctant to incorporate principles of PRT into their unit's physical training programs. Some of the key changes of PRT included a heightened emphasis on the precision of functional movements, dynamic warm-up activities replaced static stretching, and forty-four new exercises and drills were incorporated into the manual.[12] Ultimately, the doctrine failed to gain traction because many leaders and their soldiers simply did not understand the changes from an exercise science standpoint.

As the Army prepares to embrace the newest updates to service-wide physical readiness training, USACIMT and the Army's most senior leaders have attempted to generate preemptive support from commanders and the rest of the force through strategic messaging campaigns. Additionally, the Army now requires field-grade officers identified to compete for battalion command positions to pass the new ACFT, among other screening requirements, before selection for command.[13] Moreover, the soldier performance health readiness database is a centralized database the Army is launching to provide commanders with a holistic view of individual and unit

readiness. The soldier performance health readiness database, currently monitored by the U.S. Army Research Institute of Environmental Medicine during the ongoing ACFT pilot, retrieves information from existing Army databases and programs such as the digital training management system and substance use disorder clinical care program.[14] According to Bigelman, "Commanders and command sergeants major can look at the unit and assess their state of readiness, which could be measured in the physical domain, sleep, [or] cognitive [domains]."[15] The Army could further increase service-wide knowledge and understanding of the H2F program by providing lessons developed by the U.S. Army Physical Fitness School to attendees of the Battalion and Brigade Pre-Command Course and installation-level Company Commander/First Sergeant Pre-Command Courses.

Update Doctrine

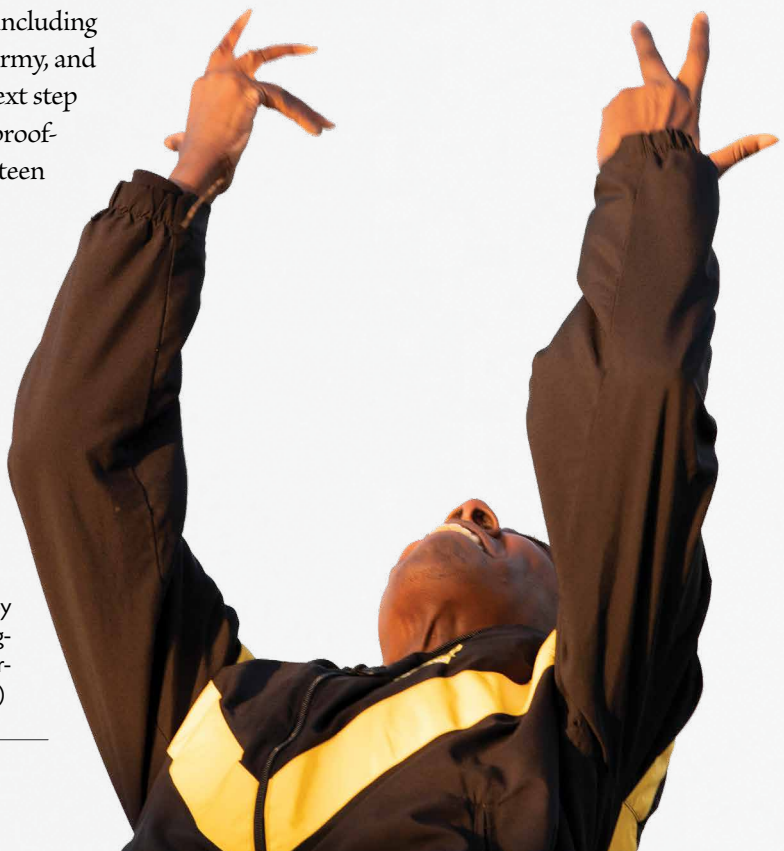
As a result of the new holistic approach to monitoring multiple health domains and the envelopment of several programs and installation-level resources into the H2F system, many Army proponents will have to update dozens of affected regulations, field manuals, and training circulars. Army Regulation (AR) 40-501, *Standards of Medical Fitness*, and AR 350-1, *Army Training and Leader Development*, are two such publications, but no doctrine will undergo more revision than FM 7-22, which the Army will rebrand as *Holistic Health and Fitness*. H2F planners provided final briefs to senior leaders including the Army chief of staff, sergeant major of the Army, and commander of USACIMT in February. The next step of the transition to H2F potentially includes a proof-of-concept at one installation for twelve to eighteen months before service-wide implementation.[16]

The new Army Field Manual 7-22. The new manual that governs the Army's approach to holistic health and fitness will include five sections and align more closely with the total force fitness framework's eight domains of individual fitness.[17] The intent is for the updated version to outline "the basics of human anatomy and performance physiology that are the foundation for program design."[18] According to Bigelman,

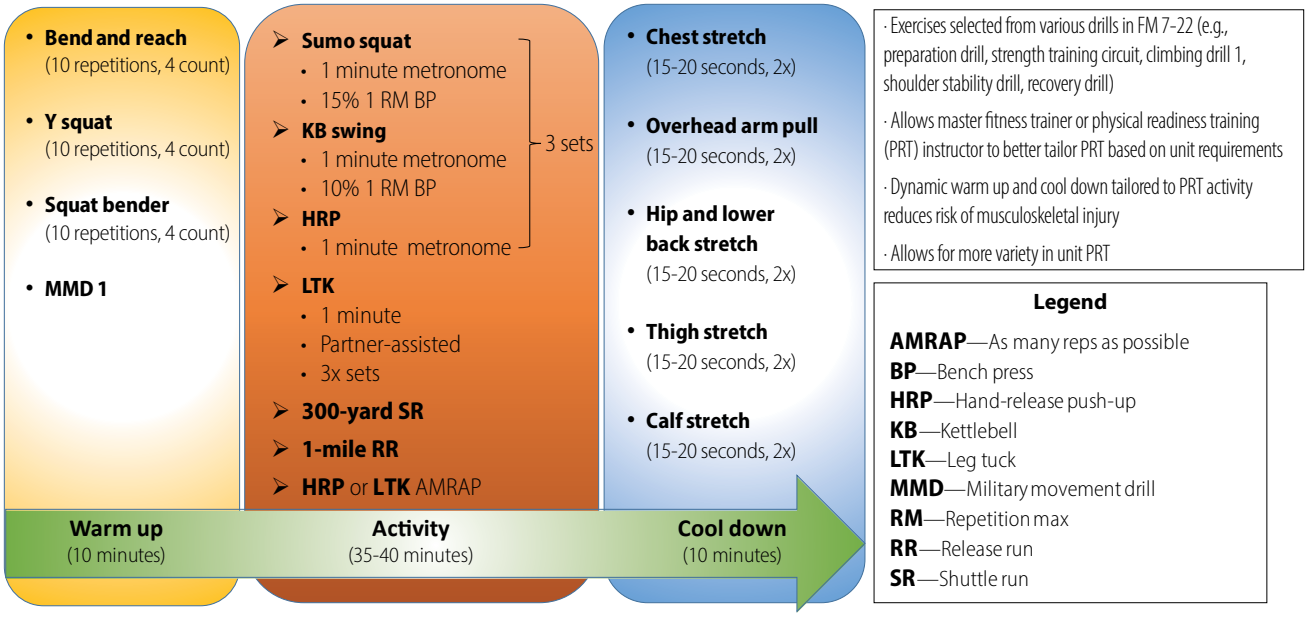
> Part I [of FM 7-22] will cover the H2F System overview and planning. Part II is the design, which covers each of the components: physical, mental, sleep readiness. Part III is the build, which covers program design specifics. Part IV is how it's delivered, which covers H2F schedules. Part V is how we assess.[19]

The assessment section of FM 7-22 will provide guidance on the purpose and execution of the ACFT. Subsequent appendices will address special populations and programs such as spiritual fitness, postpartum pregnancy physical training (PPPT), and unit-level reconditioning programs (RP).

Postpartum pregnancy physical training and reconditioning programs. The goal of PPPT is to prevent muscular atrophy and physical fitness degradation during



Maj. Malika Rodriguez tests her physical abilities by throwing a ten-pound ball 6 March 2020 during a diagnostic Army Combat Fitness Test at Fort Bragg, North Carolina. (Photo by Sgt. Alexandra Shea, U.S. Army Reserve)



(Figure by author)

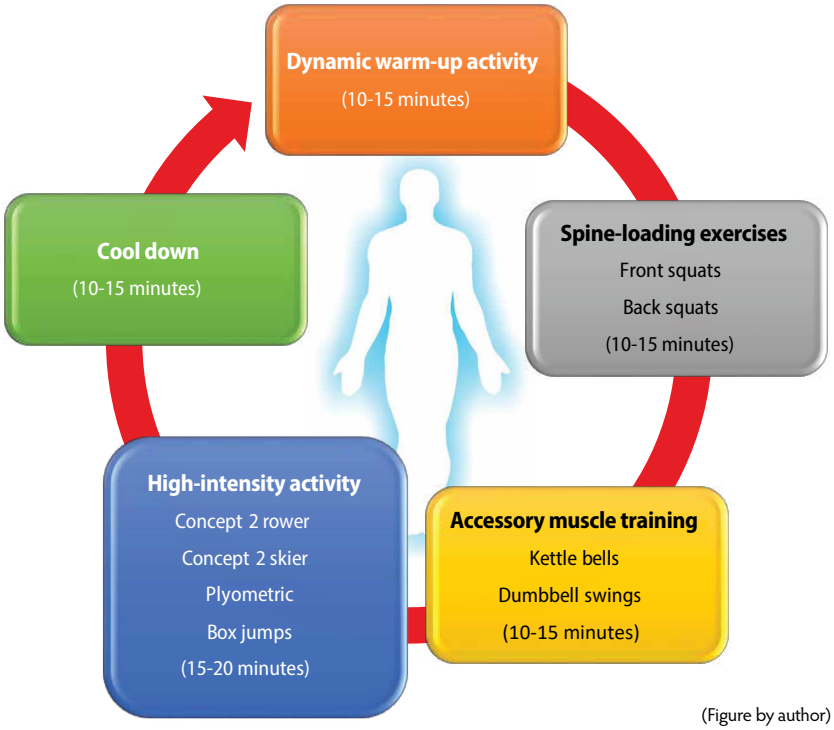
Figure 1. Sample Session with Select Exercises from Field Manual 7-22, *Army Physical Readiness Training*

pregnancy and expediently return soldiers to acceptable fitness levels following their pregnancies.[20] Certified exercise leaders supervise and instruct educational classes and prescribe fitness regimens designed to accommodate soldiers in every trimester of pregnancy and postdelivery. Even though AR 350-1 mandates participation, the program's success varies across brigades, divisions, and installations based on the degree of emphasis placed on PPPT by senior commanders and their command sergeants major.

Reconditioning programs, which share goals and training philosophies akin to PPPT, target soldiers who are physically limited due to injury or surgery and unable to participate in unit PRT sessions.[21] Many units do not have RPs due to a lack of resources, lack of understanding the program's potential impact on unit and individual readiness, or an unwillingness to comply with established training guidance for this special population. In order to eliminate the lack of nonparticipation with these programs, the Army should require each installation's senior mission commander to mandate compliance with PPPT and RPs in accordance with AR 350-1, FM 7-22, and Technical Guide Series 255A-E, *U.S. Army Pregnancy Post-Partum Physical Training Program*.

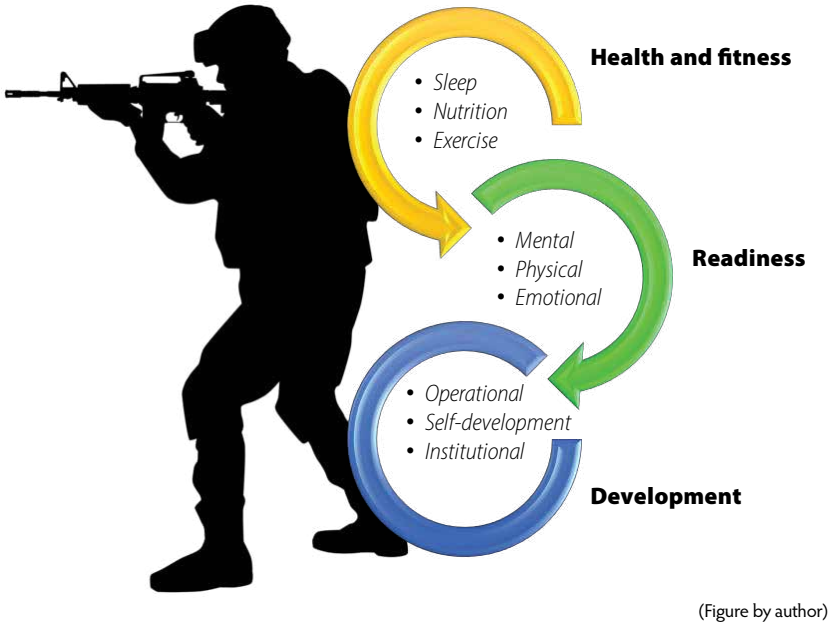
Army Combat Fitness Test. Presently, the hot-button topic related to the H2F system is the launch of the ACFT. In 2017, the Department of the Army announced that it would replace its forty-year-old, three-event Army Physical Fitness Test with the ACFT. The ACFT is an age- and gender-neutral, six-event test that gauges a soldier's aptitude and suitability for combat-related duties. While many have scrutinized the test's potential as a gender-based discriminant for assignments and an inaccurate reflection of MOS requirements, the Army could mitigate this problem by coding all duty positions in its force management system website to reflect the ACFT category required for each job.

USACIMT's research and analysis directorate used the *Baseline Soldier Physical Readiness Requirements Study* to evaluate soldiers using a simulated test of common and critical warrior tasks and battle drills, the Army Physical Fitness Test, and twenty three additional physical fitness events.[22] The ACFT will be the Army's test of record beginning in fiscal year 2021, and USACIMT will outline ACFT instructions in part V of the pending update to FM 7-22. Commanders will need to adopt innovative and creative physical readiness training plans to optimize unit performance on the ACFT. By consulting with master



(Figure by author)

Figure 2. Sample Soldier Physical Readiness Center's Physical Readiness Training Session with Exercise Examples



(Figure by author)

Figure 3. Correlation between Health and Fitness, Readiness, and Development

fitness trainers and cognitive enhancement teams, commanders and PRT leaders can identify select exercises and drills that simultaneously prepare units to accomplish their mission essential tasks by training for the ACFT (see figure 1, page 71). Since the proposal of the ACFT, commanders and leaders have decried the lack of resources necessary to train their soldiers for it.[23] The Army plans to provide the necessary physical resources but that does not substantiate the need for hexagonal barbells and medicine balls to prepare for the ACFT.

Provide Necessary Physical Resources

While the Army maintains a plan to field enough ACFT equipment to all battalions based on authorized strength, USACIMT also intends to provide the force with other tangible assets to enhance soldiers' physical readiness training.[24] One such resource is the soldier physical readiness centers (SPRC). According to USACIMT's functional concept for H2F, the Army intends for SPRCs to be dedicated space for units to train an array of physical readiness activities.[25]

USACIMT envisions SPRCs as brigade-level facilities with approximately forty-four thousand square feet of usable space for company-size units and their HPTs to train effectively.[26] The complex will include a wide range of free weights, strength and endurance training machines, and outdoor space for conducting PRT and ACFTs. HPTs and master fitness trainers can assist in the facilitation of mission essential tasks-driven training emblematic of training regimens for professional sports teams (see figure 2).[27] In order to maximize SPRC usage, commanders should restrict SPRC

use to individual training, fitness-related classes, unit PRT, PPPT, and RPs.

Conclusion

There is a direct correlation between a soldier's health and fitness, individual readiness, and professional development (see figure 3, page 72). If individuals are not exercising enough, properly fueling their bodies, or receiving adequate sleep and time for recovery, then the result is diminished cognitive performance. Knowledgeable H2F leaders recognize the potential link between suboptimal performance and insufficient sleep, dieting, or exercise habits. Poor cognitive performance may visibly manifest itself in a soldier's lack of mental agility, Army Physical Fitness Test failure, or an inability to maintain positive work and family relationships.[28] Over the length of a career, unhealthy habits inhibit a soldier's development across the operational, self-development, and institutional domains of the Army's leader development strategy.[29]

While the force anticipates the full-scale implementation of the ACFT with mixed reviews of enthusiasm and doubt, senior leaders must remain steadfast in their determination to change the Army's approach to readiness through fitness. This long-term plan requires a keen understanding and blend of programs that optimize the domains of exercise, nutrition, sleep, mental cognition, spirituality, and resilience. Successful implementation of the H2F system will take a total effort by the entire Army, more so from leaders at every echelon. The Army's senior leaders will provide the necessary talent, resources, and doctrine updates to institute the H2F system, but it is incumbent upon direct and organizational leaders across the force to comprehend modern principles of health science and lead the change to holistic health and fitness. ■

Notes

1. "The U.S. Army Holistic Health and Fitness Operating Concept: The U.S. Army's System for Enhancing Soldier Readiness and Lethality in the 21st Century" (Fort Eustis, VA: U.S. Army Center for Initial Military Training [USACIMT]: November 2019), 6.

2. Joseph Lacdan, "Army Launches Holistic Health and Fitness Initiative," Army.mil, 27 July 2017, accessed 19 August 2020, http://www.army.mil/article/191402/?st.

3. Chad Garland, "The Navy has Fattest Members of the Military—But Obesity Rates Are up Across All Services," *Stars and Stripes* (website), 3 September 2019, accessed 19 August 2020, http://www.stripes.com/news/the-navy-has-fattest-members-of-the-military-but-obesity-rates-are-up-across-all-services-1.597064.

4. USACIMT, "Holistic Health and Fitness," 7.

5. Bruce A. Ruscio et al., "Department of Defense Injury Prevention Priorities Working Group: Leading Injuries, Causes and Mitigation Recommendations" (Washington, DC: Office of the Secretary of Defense, Health Affairs, 1 February 2006), ii, accessed 19 August 2020, http://apps.dtic.mil/dtic/tr/fulltext/u2/a458257.pdf.

6. Ibid.

7. U.S. Army G-3/5/7, "Holistic Health & Fitness (H2F) v3" (PowerPoint, Department of Defense, Washington, DC, 26 June 2018).

8. Kevin A. Bigelman (Holistic Health and Fitness Chief for the Army Center of Initial Military Training), in discussion with the author, transcript and recording, 6 December 2019.

9. "May 2018 National Occupational Employment and Wage Estimates United States," U.S. Bureau of Labor Statistics, 2 April 2019, accessed 19 August 2020, http://www.bls.gov/oes/current/oes_nat.htm.

10. Bigelman, discussion, 3.

11. Ruscio et al., "Department of Defense Injury Prevention Priorities Working Group."

12. Field Manual (FM) 7-22, *Army Physical Readiness Training* (Washington, DC: U.S. Government Printing Office, 2012 [obsolete]), 26, accessed 20 August 2020, https://armypubs.army.mil/epubs/DR_pubs/DR_a/pdf/web/ARN7938_FM%207-22%20INC%20C1%20Final.pdf.

13. Army Talent Management Task Force, "Army Announces New Battalion Commander Selection Program," Army.mil, 6 November 2019, accessed 20 August 2020, https://www.army.mil/article/229500/army_announces_new_battalion_commander_selection_program.

14. Bigelman, discussion, 8.

15. Ibid.

16. Ibid., 5.

17. Chairman of the Joint Chiefs of Staff Instruction 3405.01, *Chairman's Total Force Fitness Framework* (Washington, DC: Joint Chiefs of Staff, 1 September 2011), accessed 20 August 2020, https://www.jcs.mil/Portals/36/Documents/Library/Instructions/3405_01.pdf?ver=2016-02-05-175032-517.

18. Whitfield B. East, David DeGroot, and Stephanie Muraca-Grabowski, "Baseline Soldier Physical Readiness Requirements Study," *Journal of Science and Medicine in Sport* 20, no. 2 (November 2017): 10.

19. Bigelman, discussion, 7.

20. Army Regulation 350-1, *Army Training and Leader Development* (Washington, DC: U.S. Government Publishing Office [GPO], 10 December 2017), accessed 27 August 2020, https://armypubs.army.mil/epubs/DR_pubs/DR_a/pdf/web/ARN18487_R350_1_Admin_FINAL.pdf.

21. FM 7-22, *Army Physical Readiness Training*, 2-3.

22. East et al., "Baseline Soldier Physical Readiness Requirements Study," 11.

23. Kelly Buckner, "What the Critics Miss: The Army Combat Fitness Test is Going to Make Us a More Combat-Ready Force," Modern War Institute at West Point, 9 October 2019, accessed 20 August 2020, http://mwi.usma.edu/critics-miss-army-combat-fitness-test-going-make-us-combat-ready-force/.

24. Michael A. Grinston, Timothy A. Guden, and Edward W. Mitchell, "Army Combat Fitness Test Q&A" (Washington, DC: Department of Defense, September 2019).

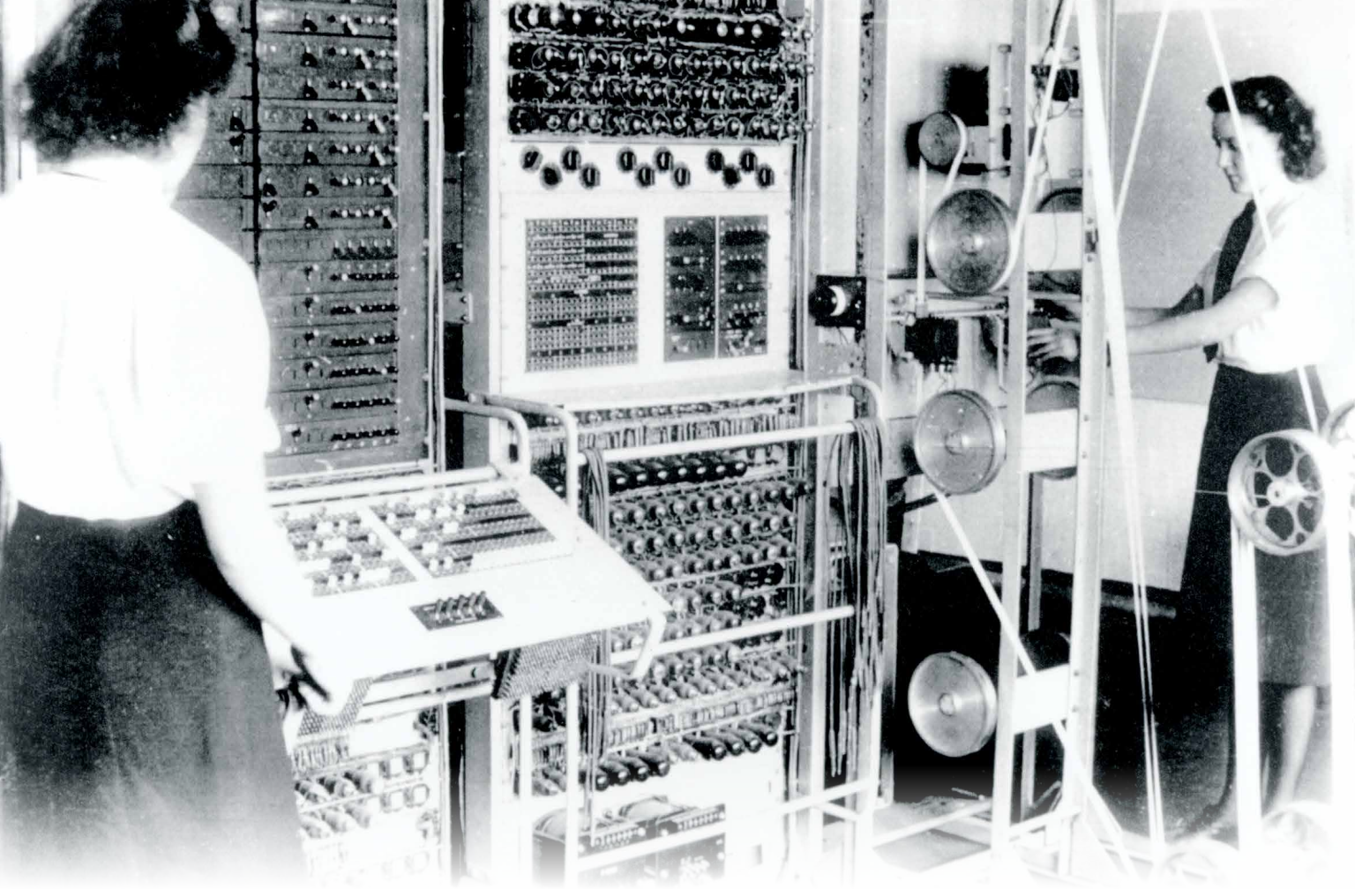
25. USACIMT, "Holistic Health and Fitness," 18.

26. Ibid.

27. Bigelman, discussion, 4.

28. Ibid., 6–7.

29. Army Doctrine Publication 6-22, *Army Leadership and the Profession* (Washington, DC: U.S. GPO, July 2019), accessed 20 August 2020, https://armypubs.army.mil/epubs/DR_pubs/DR_a/pdf/web/ARN20039_ADP%206-22%20C1%20FINAL%20WEB.pdf.



A Colossus Mark 2 codebreaking computer being operated by Dorothy Du Boisson (*left*) and Elsie Booker in 1943 at Bletchley Park, Buckinghamshire, England. (Photo courtesy of the United Kingdom National Archives) **Next page:** U.S. Cyber Corps insignia

Older Than You Realize

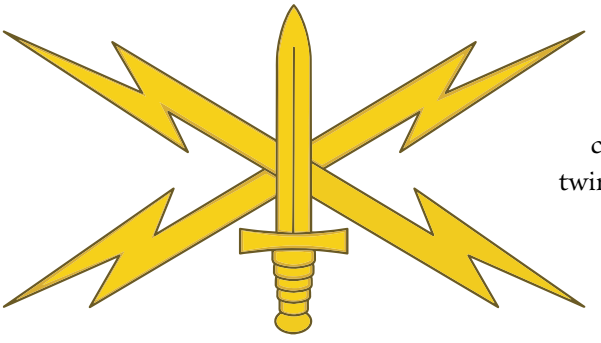
Teaching Branch History to Army Cyberwarriors

Scott Anderson

"So you are the Cyber Branch historian? That's cool, but I guess you don't have that much history to keep up with then."

I often hear similar comments when I explain my job title to people. To be fair, the U.S. Army Cyber School and Cyber Branch are just over six years old—mere embryos compared to the likes

of the infantry or cavalry. What bears explanation to skeptics is that while the Army's Cyber Branch is very young, the Department of Defense (DOD) effort to both protect networks and penetrate those of our adversaries goes back several decades. While the joint chiefs of staff may not have described cyberspace as a domain until 2004, the Soviets were paying hackers to steal U.S. military secrets as far back as 1986.[1] The birth of the Army's Cyber Branch in 2014 was merely a natural evolution in the need for the Army to codify the training standards and create a professional career path for its burgeoning corps of cyberwarriors who had until then been operating under the auspices of military intelligence (MI) units for some time.



The Cyber Branch Historian

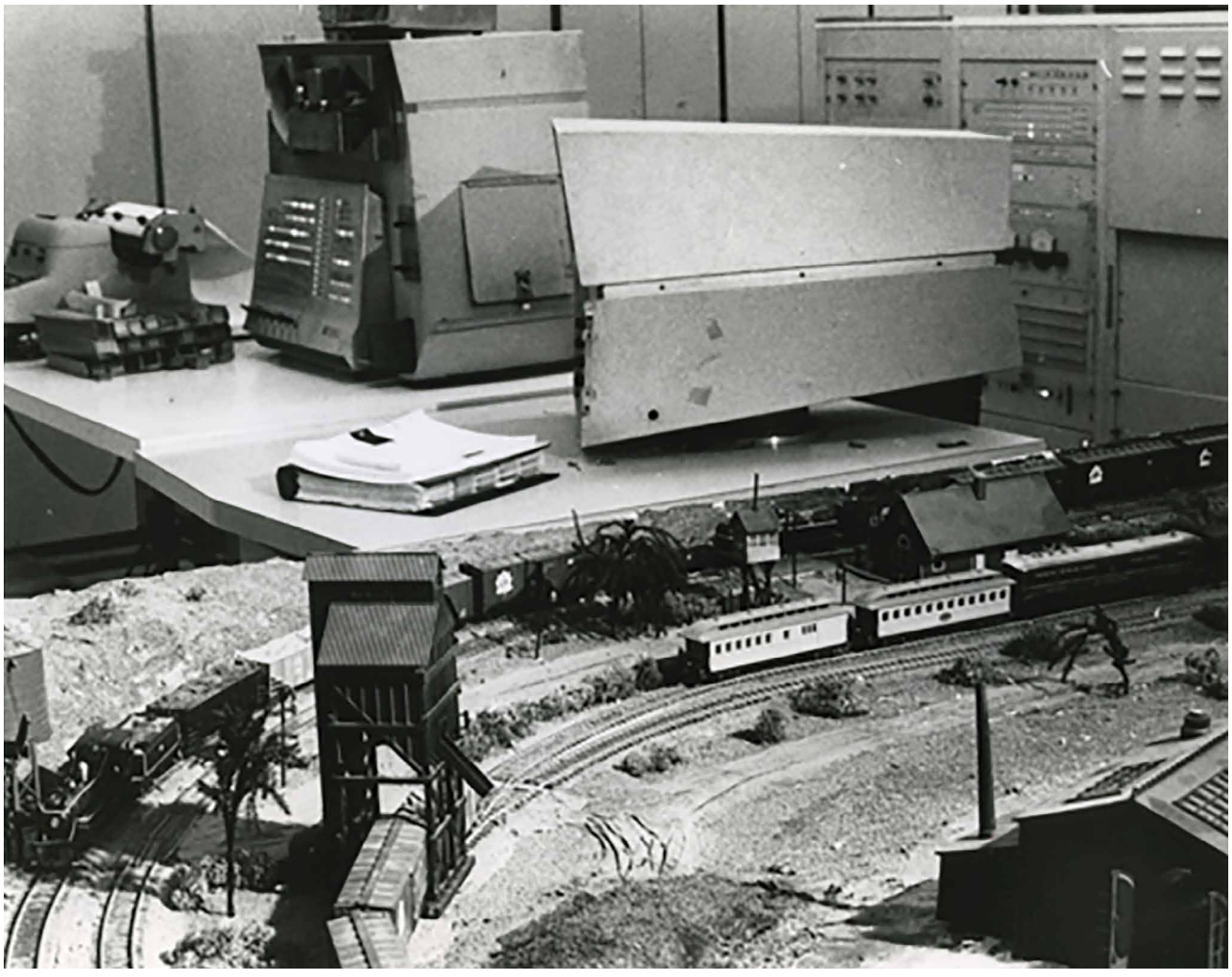
The U.S. Army Training and Doctrine Command's (TRADOC) Military History and Heritage Program oversees the requirements for Army branch historians. Every basic branch within the Army should have a historian working at its associated TRADOC school or center of excellence, and the young Cyber Branch is no exception. The Army Cyber School is located at Fort Gordon, Georgia, and nested within the Cyber Center of Excellence, which also operates the Army Signal School. The Cyber School, which officially opened in August 2014, had a historian on its staff by December 2015. Branch historians look to guidelines such as Army Regulation 870-5, *Military History: Responsibilities, Policies, and Procedures*; TRADOC Regulation 870-1, *United States Army Training and Doctrine Command Military History and Heritage Program*; and TRADOC Regulation 350-13, *Instruction in Military History*, for direction in their roles and responsibilities, with this latter regulation stipulating the categories of history instruction required for each type of professional military education class (e.g., Advanced Individual Training, Basic Officer Leaders Course, Warrant Officer Basic Course). Relevant branch history is among the required blocks for several of these classes, and it is here that I received my mandate to provide Cyber Branch history.

Creation of the Cyber Briefing

I developed a briefing for the officers, warrant officers, and enlisted soldiers at the U.S. Army Cyber School that would create an understanding of why their jobs exist and how many contemporary cyber events are not as new as they might think. This brief would be short if it only covered Army-related events, but as is the case with many aspects of the DOD's cyber mission, the milestones are of a joint nature. One of the unique things about cyber is that its history is intertwined with private-sector events and runs parallel in many instances with "hacking history." This hacking history, both in the military and the private sector, forms the basis for the briefing. What follows is a discourse on the content of the current cyber brief with an attempt to explain how past events in cyberspace (both military and private) have affected where we are today and why the U.S. Army has called cyberwarriors into service.

World War I

Cyber history begins here with World War I. The modern Cyber Branch of the U.S. Army originated from several of the duties and responsibilities formerly assigned to the Military Intelligence Corps and the Signal Corps. Gathering intelligence had always been a necessary component of warfare, but it was during World War I when the scale of information gathering reached unprecedented levels. From opening the citizenry's private mail to intercepting telegraph cables in order to gather secrets—or the inverse, cutting enemy cables to block communication—the origins of what we call "information warfare" were spawned during World War I. The predecessor of the National Security Agency (NSA), the ultrasecret Cipher Bureau headed by Herbert O. Yardley, came about in 1917. With the advent of radio and the ability to listen to an



A model railroad train set is in the foreground with a DEC PDP-1 console and monitor sitting on a table in the background in the Tech Model Railroad Club during the 1950s. (Photo courtesy of the Computer History Museum)

adversary's communications, the foundation of modern signals intelligence was also established.[2]

After the war, Yardley's Cipher Bureau, also known as "Black Chamber," set up a clandestine government cryptanalytic unit in a New York City building disguised as a commercial entity called the Code Compiling Company. Despite the chamber's success, the State Department shut it down in 1929 for several reasons, most famously after Secretary of State Henry L. Stimson stated, "Gentlemen do not read each other's mail." Disgruntled Yardley, out of a job, authored *The American Black Chamber* in 1931. The shocking exposé revealed the primary mission of the unit—the decryption of diplomatic communications of both friend and foe.[3]

World War II

Communications encryption became important in the early twentieth century, and with World War II came the advent of mechanized codebreaking. This codebreaking process was the focus at Bletchley Park, a nineteenth-century mansion and estate near London and the top secret headquarters of the British Government Code and Cypher School.[4] Among the scholars and academics turned codebreakers working in numbered huts at Bletchley, Alan Turing became the most known for his part in helping break the German Enigma code. Turing and his colleagues were depicted as breaking the Enigma by utilizing a "bombe" machine in the 2014 film *The Imitation Game*.[5]

The bombes were technically not computers but electromechanical devices that did not carry out calculations. However, another important machine developed at Bletchley Park is generally considered the first programmable electronic computer ever devised. With it, British cryptographer Tommy Flowers cracked an even more complex cipher machine known as the Lorenz, which carried communications of the German High Command—including Adolf Hitler. Flowers and his team dubbed their creation "Colossus," a project that remained a secret until the mid-1970s. Colossus was the first to utilize the modern binary system of ones and zeros that form the basis of modern computing.[6] Gen. Dwight Eisenhower reportedly gained confidence to launch the D-Day invasion on the Normandy beaches based on Colossus-intercepted messages confirming the Germans thought the invasion would be at Calais rather than Normandy.[7] William Friedman, perhaps America's most famous cryptologist and considered by many to be the father of modern cryptography, stated in 1942, "Actual physical warfare is intermittent, but mental, that is cryptanalytic warfare is continuous."[8]

> From opening the citizenry's private mail to intercepting telegraph cables in order to gather secrets—or the inverse, cutting enemy cables to block communication—the origins of what we call "information warfare" were spawned during World War I.

Postwar Developments

Early cryptography and mechanized codebreaking laid the foundation for the rapid postwar development of computers. The Army, in partnership with the University of Pennsylvania, built the first general purpose electronic computer. The previously mentioned Colossus had a specific task—codebreaking—while the new Electronic Numerical Integrator and Computer (ENIAC) handled a variety of tasks.[9] The ENIAC became operational in late 1945; its initial task was to calculate artillery firing tables for the U.S. Army's Ballistic Research Laboratory with a goal to both reduce calculation times and remove human error.[10]

"Cyber" entered the vernacular during the early postwar years via the concept of "cybernetics." This was the term coined by Massachusetts Institute of Technology (MIT) mathematician Norbert Weiner, whose interest in the new world of computing led to a new scientific discipline of sorts. Weiner took the Greek verb "kybernan," which means to steer, navigate, or govern, and attached his theory of cybernetics, promoting the idea that the most promising path for computer science was to devise machines that would work well with human minds rather than try to replace them.[11] While use of the word "cyber" as we use it today laid predominantly dormant until several decades later, Weiner's concepts serve as a conduit from the postwar rise of computers to modern day.

Turing theorized as far back as the 1930s about machine learning, but the 1950s are when artificial intelligence (AI) research began in earnest. During this decade, Turing developed his eponymously named "Turing Test," which evaluates a machine's ability to exhibit intelligent behavior equivalent to or indistinguishable from that of a human.[12] Dr. John McCarthy coined the term "artificial intelligence" in 1956, and along with Marvin Minsky, began the first coordinated AI research at MIT in 1959.[13]

Besides the aforementioned AI research program, MIT's Tech Model Railroad Club (TMRC) figures prominently in the early phase of cyber history. Founded in 1946, this club had two factions by the mid-1950s: those interested in the layout and painting of model trains and the "Signals and Power Subcommittee." The members of this latter group in many ways formed the nucleus of what became a recognized hacker culture within the United States. Members of the TMRC Signals and Power Subcommittee began applying the term "hacks" as early as 1955 to all manner of technology-based practical jokes and in the context of hacking the electrical system of their model railroads. In Steven Levy's thorough treatment of the TMRC in

Hackers: Heroes of the Computer Revolution, he explains that to qualify as a hack, the members felt that the feat must be innovative, stylish, and infused with technical virtuosity.[14] The members of the Signals and Power Subcommittee graduated in a sense from working on model train components to the early computers acquired by MIT. Their urge to learn coding and programming became so insatiable that they often forewent class attendance for precious time on the shared computer. One such member, Steve "Slug" Russell, even programmed the first computer video game in 1962 when he used MIT's PDP-1 computer to create *Spacewar!*[15] According to Levy, Russell and his fellow hackers also developed a silently agreed upon "hacker ethic."[16] These early computer enthusiasts called themselves hackers, but their "hacking" came mostly in the form of teaching themselves how to program these bulky computers to do things they were not intended to do, such as creating the aforementioned video game.

The first known public use of the term hacker in the modern vernacular came in the 20 November 1963 issue of MIT's newspaper, *The Tech*. The article described a criminal trespass, with hackers connecting the PDP-1 computer to the telephone system and launching a brute force attack, tying up all the phone lines between MIT and Harvard. In another act of ingenuity, the article explains that the hackers made long distance calls but charged them to a local radar installation.[17] This segues into an explanation of "phone phreaking" in the late 1960s and early 1970s, where crafty protohackers like John "Captain Crunch" Draper figured out how to replicate the precise 2,600 Hz tone needed to fool the Bell telephone system and make free calls around the world at a time when long-distance charges were at a premium and cell phones were nonexistent. In fact, whether using a computer, a "blue box," or even a toy whistle pulled from a Cap'n Crunch cereal box, making free long-distance phone calls became a rite of passage for many early hackers.[18]

Scott Anderson is the Army Cyber School and Cyber Branch historian at the Cyber Center of Excellence, Fort Gordon, Georgia. He holds an MA in public history from Middle Tennessee State University. His previous assignments include researching cases of World War II missing-in-action personnel for the U.S. military accounting mission and working for the U.S. Naval History and Heritage Command.

The Cold War

A concept now enters the discussion that really is at the heart of cyber—the development of networked computers. In many ways, the massive early warning radar system known as the Semi-Automatic Ground Environment, or SAGE, provided the foundation for linking many computer systems. Developed in the early years of the Cold War to warn of Soviet nuclear bombers entering North American airspace, SAGE consisted of hundreds of radar systems connected to large computer centers using an early modem capable of converting analog radar signals into digital code via telephone lines.[19] By the late 1960s, more and more organizations were linking their computer systems together via networks.

The DOD was no exception to this new practice that made for faster file sharing and collaboration within organizations. Willis Ware, an engineer for the RAND Corporation, could be considered the first computer security whistleblower. Ware delivered a paper at an academic conference in 1967 titled, "Security and Privacy in Computer Systems," which highlighted concerns with networked computers.[20] After Ware's warning, the DOD concerned itself with this new threat, even assembling a task force (with Ware as chairman) to recommend appropriate computer security safeguards. The task force report, published in February 1970, showed how corrupt insiders and spies could actively penetrate computers and steal or copy classified information.[21]

During the period that Ware and his team worked on their report, something truly monumental occurred that set the stage for practically everything that follows in the cyber chronology—the Advanced Research Projects Agency Network (ARPANET) established its first permanent link. The ARPANET, which was the precursor to our modern internet, was a computer network connecting American universities with defense research programs and the Pentagon. On 21 November 1969, this first permanent link was established between the University of California at Los Angeles (UCLA) and Stanford Research Institute (SRI) in Menlo Park, California, 367 miles apart. The network used packet switching, a new communications protocol that bundled a packet of data with its destination address. Every node on the network

An image of Cape Cod, Massachusetts, is displayed on screen in a Semi-Automatic Ground Environment (SAGE) control room during the Cold War. SAGE provided the foundation for linking many computer systems. (Photo courtesy of the U.S. Air Force)

passed on each packet until it reached its destination. This kept information flowing, with packets from one message filling in spaces between those of other messages so that each line could be used close to capacity. By 31 December 1969, ARPANET had expanded to four nodes: UCLA, SRI, the University of California at Santa Barbara, and the University of Utah.[22] By 1972, the "@" symbol was used to show that electronic messages were coming from a particular network, and by the following year, ARPANET users in the United States were corresponding with British researchers in real time over the Atlantic.[23]

Personal Computing

Since their development in the 1940s, computers steadily decreased in size from the mammoth ENIAC, which took up one thousand square feet of floor space, to the more compact but still refrigerator-size "minicomputers." The evolution from vacuum tubes to the transistor in 1948 and then to the microchip a decade later allowed the size of these machines to shrink while simultaneously increasing their speed and power. However, it was not until Intel's development of the microprocessor in 1971 that computers began transitioning to the compact sizes that we recognize as the personal computer.[24]

The cover story in the January 1975 issue of *Popular Electronics* magazine featured the "Altair 8800" and told how this simple looking small box with lights and switches rivaled the power of much larger commercial computers. Boyhood friends Bill Gates and Paul Allen later entered into a partnership with the Altair's makers to write the BASIC programming language, which in turn led to the formation of Microsoft.[25] Another famous duo in the development of personal computers, Steven Jobs and Stephen Wozniak, came out with the Apple I in 1976.[26] The 1970s witnessed several other firsts, including the first IRS computer embezzlement and the first hack into a government computer. And in 1979, a fifteen-year-old child became the first hacker to be arrested and charged with felony vandalism for disrupting a university's computer programs.

The 1980s

In 1983, the hit movie *WarGames* was released. If the previous decade had dabbled with the notion of teenagers getting smart on the new world of interconnected computer networks, this film amped up the theme to

the next level. *WarGames* stars Matthew Broderick as the typical hacker who nearly starts Armageddon from his bedroom when he begins playing what appears to be a new computer game called *Global Thermonuclear War*. However, he has unwittingly connected to an artificially intelligent computer with control over NORAD's nuclear arsenal. Interestingly, the film's writers consulted with the previously mentioned Willis Ware, who explained how the military's computers were at risk, giving them the confidence to move forward with their script.[27] While there are seemingly far-fetched aspects of this movie, it provides a case of pop culture influencing national policy. President Ronald Reagan watched *WarGames* shortly after its release and began asking whether something like what was depicted in the movie could really happen. Fifteen months later, his administration published National Security Decision Directive 145, *National Policy on Telecommunications and Automated Information Systems Security*.[28]

That same year, a group of real teenage hackers from Milwaukee calling themselves "The 414s" broke into several computer systems including the one in the Los Alamos National Laboratory. The FBI eventually caught up with them; foolishly, the group named themselves after their local area code.[29]

Solidifying 1983 as the year of the teenager hacker, CBS premiered *Whiz Kids* that fall, portraying a group of kids who routinely use hacking skills to assist the police in bringing criminals to justice.[30] Finally, to close out this monumental year, a graduate student named Fred Cohen created the first computer virus in November. Upon his proof-of-concept code taking over a mainframe within minutes at a computer security seminar, Cohen's academic advisor likened the self-replicating program to a "virus."[31]

The cyber milestones continued in the mid-1980s. The first large-scale data breach occurred in 1984 when hackers stole a file password from TRW, a large credit reporting agency that handled the confidential credit histories of over ninety million Sears customers on the West Coast. Utilizing a favorite communication medium of the early hacking age, the criminals posted the password on an electronic bulletin board providing like-minded individuals access to the exposed personal data.[32]

In 1986, the Soviets became involved in cyber espionage, but their participation was uncovered by American astronomer turned computer administrator Cliff Stoll. Well before our modern convenience of almost universal internet connection on a personal level, Stoll's employer, Lawrence Berkeley National Laboratory, received user fees from ARPANET patrons needing a network access point. Instead of ignoring a $0.75 billing discrepancy connected to one of these patrons, Stoll decided to dig. He connected the payment issue with a user moving through the network, suspiciously accessing several sites including the Army's unclassified portion of the ARPANET aptly named Military Network, or MILNET. Stoll employed many innovative tricks in an attempt to trace the hacker including setting up his pager to send alerts when the hacker logged in. Stoll eventually began sleeping at the lab for quicker response times, but his nemesis never stayed on the network long enough to get an accurate trace. Finally, Stoll concocted a plan that solidified his legacy. He planted juicy, albeit fake, documents in his network that the hacker could not resist, thus keeping him online long enough for an accurate trace. Known as a "honeypot," the technique is still part of the cyber toolkit today. In the end, Stoll's determination and innovation led to the capture of a West German hacker ring whose members sold stolen documents from U.S. military sites to the KGB. Stoll's 1989 book, *The Cuckoo's Egg*, chronicled these events, describing Russia's initial foray into cyber espionage. While the West Germans were caught and one member served prison time, the Russians were implicated in a type of spy craft they would eventually master.[33]

In the wake of Stoll's baptism by fire into this new world of cybersecurity, he became involved in helping solve other problems. He did not have to wait long for the next major incident: the "Morris Worm," which is considered the first large-scale malware attack in history.[34] On 2 November 1988, Robert T. Morris Jr., a Cornell University computer science graduate student, unleashed a self-replicating "worm" that did not destroy data but temporarily disabled about 10 percent of the internet, or about six thousand computers. One of the first people Stoll contacted upon learning of the problem was Robert H. Morris, who was not only the chief scientist at NSA's National Computer Security Center, but in an ironic twist, also happened to be the culprit's father! The younger Morris realized he was in trouble and confessed to his father, who could not help but feel a bit proud of his son's creation. Securing a lawyer, father and son went to the FBI. Morris's alleged goal was benign, to estimate the size of the internet, but a design error in his program

caused it to replicate out of control. Morris holds the distinction of being the first person found guilty by jury and convicted under the 1986 Computer Fraud and Abuse Act. He received three years' probation, four hundred hours of community service, and a $10,000 fine. A silver lining to this incident was the DOD's creation of the first computer emergency response team (CERT) at Carnegie Mellon University. Today, almost every country has a CERT, but in 1988, this important organization served as an around-the-clock cybersecurity response unit and raised public awareness about the vulnerabilities of connecting to the internet.[35]

It is safe to say that 2019 was the year of ransomware. That year saw an unprecedented number of attacks on state and municipal governments and agencies, healthcare providers, and educational establishments at a cost of over $7 billion.[36] However, the first case of ransomware occurred more than thirty years ago in a bizarre effort to boost AIDS research funding. During the second week in December 1989, Dr. Joseph Popp, a biologist working as a World Health Organization consultant in Africa, mailed over twenty thousand computer discs to business and government agencies in Europe, Africa, and Asia (none to the United States) under the guise of the "PC Cyborg Corporation." The recipients only saw a questionnaire about HIV when they popped in the discs, but after rebooting their computers ninety times, a hidden virus activated a file encryption program. Users then received a ransom note, promptly demanding a "licensing fee" of $189 for one year or $378 for lifetime access to their own files. Fortunately for the victims, most IT professionals easily bypassed the encryption, which meant Popp did not raise any research money. Popp was arrested and extradited to Great Britain but was deemed not mentally competent to stand trial.[37]

Impact of the World Wide Web

If 2019 marked the thirtieth anniversary of Popp's devious scheme, it also was the thirtieth anniversary of a more productive element within cyber history—the development of hypertext, the impetus for the creation of the World Wide Web. In March 1989, British computer scientist Timothy Berners-Lee submitted a proposal explaining his creation of hypertext to his bosses at the European

"President Ronald Reagan watched *WarGames* shortly after its release and began asking whether something like what was depicted in the movie could really happen. Fifteen months later, his administration published National Security Decision Directive 145, *National Policy on Telecommunications and Automated Information Systems Security*."

Cover art for *WarGames* courtesy of Metro-Goldwyn-Mayer

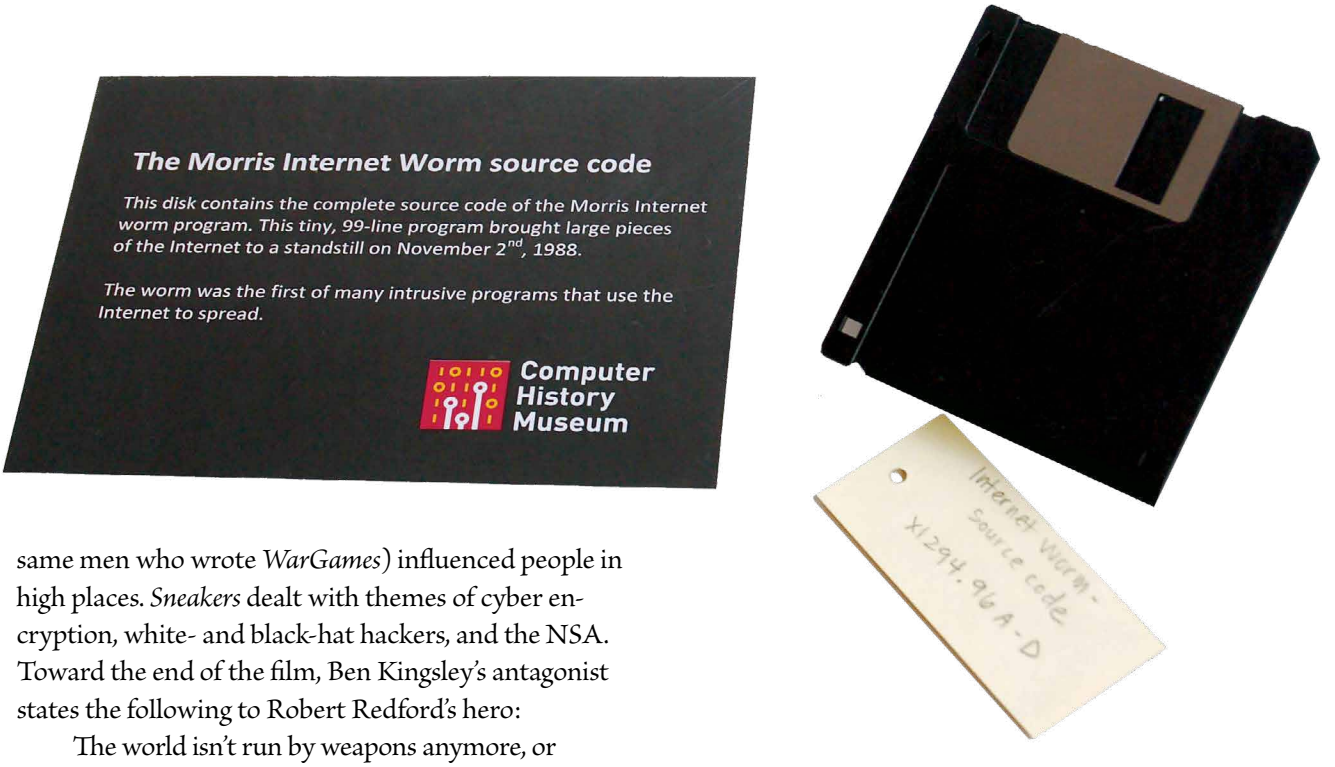
Council for Nuclear Research (CERN) in France. His idea for hypertext was to create words or phrases that were coded so that when clicked, the reader would be sent to another document or piece of content. When writing his initial proposal, the only name he had for it was "mesh," but soon after, he decided on "World Wide Web." He also created the term "uniform resource locator," more commonly known as URL, and a suite of tools that included "hypertext transfer protocol" (HTTP) and "hypertext markup language" (HTML), standard tools still in use today. The first website on the World Wide Web, a CERN page, went online two years later on 6 August 1991.[38]

With an increasing number of computer novices dialing into the World Wide Web in the early nineties, the average citizen became aware of issues related to privacy, identity theft, and hacking as they lived more of their lives "online." Hollywood followed suit with a slate of films such as *Hackers* and *The Net*, reflecting this new connected world. Reminiscent to the effect *WarGames* had on Reagan, the 1992 film *Sneakers* (cowritten by the same men who wrote *WarGames*) influenced people in high places. *Sneakers* dealt with themes of cyber encryption, white- and black-hat hackers, and the NSA. Toward the end of the film, Ben Kingsley's antagonist states the following to Robert Redford's hero:

> The world isn't run by weapons anymore, or energy, or money, it's run by little ones and zeroes, little bits of data. It's all just electrons … There's a war out there, old friend. A world war. And it's not about who's got the most bullets. It's about who controls the information. What we see and hear, how we work, what we think … it's all about the information![39]

The NSA director at the time, Rear Adm. John Michael McConnell, saw the movie and was apparently convinced that the mission of the NSA needed to follow the key theme from the film, that "There's a war out there … It's all about who controls the information." Shortly thereafter, McConnell hired a director of information warfare within the NSA.[40]

The first large-scale DOD cyberattack exercise was orchestrated by the NSA—an event known as "Eligible Receiver." From 9 to 13 June 1997, NSA Red Team experts equipped with only off-the-shelf, publicly available computer equipment, began a systematic cyberattack against unsuspecting targets.[41] They targeted the electric grid first, and without flipping the switch, proved they could do so if they desired. Next came the Pentagon itself, which the testers thoroughly penetrated in four days. The Red Team compromised the U.S. military's command and control to the point that officials shut



A computer disk containing the Morris Internet Worm source code now found at the Computer History Museum in Mountain View, California. The worm was released 2 November 1988 and is considered the first large-scale malware attack in history. (Photo courtesy of the Intel Free Press via Flickr)

down Eligible Receiver early. The exercise proved there was much work to be done in cyberdefense.[42]

Government officials were still reviewing lessons learned from Eligible Receiver when the U.S. government faced major back-to-back cyberattacks in early 1998. In February, the Pentagon underwent the most organized and systematic attack on its unclassified computer systems to date. After the first week of attacks, DOD leaders took the unprecedented step to mobilize a special crisis cell on the joint staff under Operation Solar Sunrise to deal with the intrusions. In the end, the perpetrators were two California sixteen-year-old teenagers working with an eighteen-year-old Israeli.[43]

U.S. officials might have dodged a bullet with Solar Sunrise being the work of teenage pranksters, but no sooner had this event ended when administrators detected a more troubling intrusion that became known as Moonlight Maze. This new incursion was alarming enough that Deputy Secretary of Defense John Hamre briefed a congressional committee that "we're in the middle of a cyberwar."[44] Victims included the Pentagon, NASA, and the Department of Energy, just to name a few. The attacks persisted for several years, and most information is still classified, but in a somewhat odd metric provided, Moonlight Maze operators supposedly stole enough information that if printed on paper, the pile would stand three times higher than the Washington Monument.[45] Most evidence pointed to Russia; however, Moscow denied it, and the incident brought the problem of attribution to the forefront. The attack reinforced the reality that we were no longer just dealing with teenage hackers but state-sponsored attacks.[46]

In a signal that DOD officials had simply seen too much with the trifecta of cyber vulnerabilities revealed by Exercise Eligible Receiver, Solar Sunrise, and Moonlight Maze, they created Joint Task Force-Computer Network Defense (JTF-CND) in 1998, which reported to the secretary of defense and planted the seeds of an eventual national cyber command. This joint task force became the first organization with direct authority over operations on individual military service and DOD networks.[47] In June 1998, Company B, 742nd MI Battalion, 704th MI Brigade, was tasked to develop a computer network operations force.[48] This Fort Meade-based unit became the first Army unit dedicated to conducting cyber operations.

Twenty-First Century Cyber

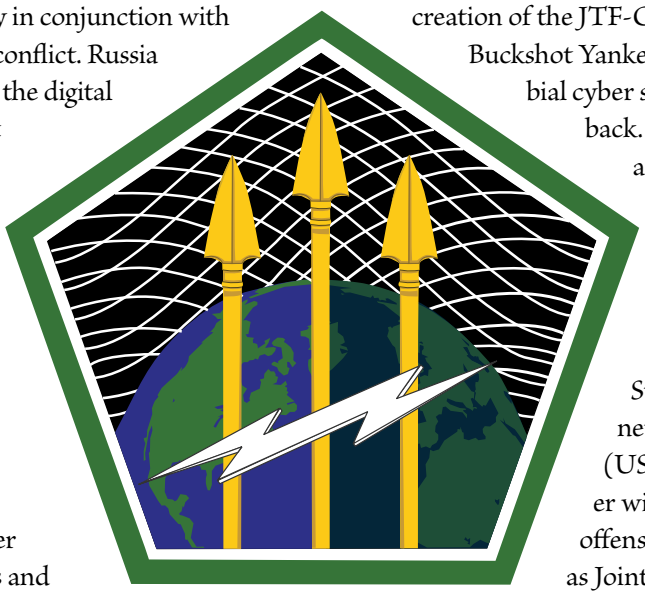
As the cyber chronology breached the twenty-first century, we saw the first real examination of hacking by the People's Liberation Army of China. Chinese patriotic hackers had struck U.S. websites, including the White House site, as early as 1999 in response to the accidental U.S. bombing of the Chinese embassy in Belgrade, Serbia, during the Kosovo conflict.[49] However, by 2003, the DOD was concerned with the first significant case of persistent Chinese cyberespionage. The U.S. codename for these intrusions was initially Titan Rain, with perhaps the most well-known target of these attacks being the Chinese theft of terabytes of data on the Joint Strike Fighter (F-35 Lightning II), which has suspiciously led to China's own development of similar stealthy fighters.[50] While Titan Rain was the first significant case of Chinese cyberespionage, it certainly was not the last.

The next major cyber milestone was triggered in 2007, oddly enough by a World War II-era statue located in the capital city of Tallinn, Estonia—a former Soviet republic. As Estonian leaders debated about the possible removal and relocation of the monument to the Liberators of Tallinn, which many viewed as a symbol of former Soviet repression, the Russian government warned that removing the statue would be "disastrous for Estonians."[51] Within hours after the statue's relocation from Tallinn's city square to a nearby military cemetery on 27 April, a widespread series of distributed denial of service attacks commenced against Estonia's computer networks. Lasting about three weeks, the attacks crippled much of Estonia's online infrastructure, including government services, online banking, and news media services. While the Russian government denied involvement, Vladimir Putin had fiercely criticized the statue decision. In the end, only one ethnic Russian Estonian was charged in relation to the attack. Before the incident, many considered Estonia the most "wired" country in Europe, but when the digital smoke cleared in the aftermath of what some nicknamed "Web War I," it was clear that this technologically progressive nation had not invested enough in cyberdefense.[52]

About fifteen months after the Estonia attacks, the world watched Russia become embroiled in another conflict with one of its former republics. The Russo-Georgian War lasted from 7 to 12 August 2008 over disputes in the Abkhazia and South Ossetia regions of Georgia. The

distributed denial of service attacks against Georgia had a whiff of familiarity to the Estonia attacks as Georgian online infrastructure such as government, news, and banking websites were hit. However, the incident quickly escalated to a shooting war as well, and it is considered by many to be the first time in history that cyber effects were used against an adversary in conjunction with conventional forces in armed conflict. Russia easily dominated both in both the digital and terrestrial battlespace, but another important aspect of the conflict is how Russia controlled the prevailing narrative available to the Georgians. The hacking became so pervasive that Russian propaganda allowed Moscow's version of events to dominate—a classic case of information warfare.[53]

Up to this point in the cyber narrative, the myriad breaches and hacks on U.S. government systems took place in the unclassified realm, never straying beyond (to our knowledge) the U.S. military's Nonclassified Internet Protocol Router Network, widely known as NIPRNet. However, in the fall of 2008, the DOD received a major wake-up call when a virus known as Agent.btz successfully penetrated not only NIPRNet but also the DOD's secret (SIPRNet) and top secret (Joint Worldwide Intelligence Communications System, or JWICS) systems. The standard unclassified version of the narrative involves curious DOD personnel stationed in the Middle East discovering an infected USB flash drive and inadvertently introducing the malware onto the network. While popping an unknown flash drive into a DOD computer was not acceptable in 2008, it is also likely that additional bad cyber hygiene promulgated the virus past the unclassified network. The virus was identified when the malware beaconed location information back to its creator, and the DOD responded with Operation Buckshot Yankee to fend off the attack. The United States never formally declared attribution to a specific nation, but there were several connections to Russia. As a result of this major incident, the DOD put new security procedures in place, including the banning of portable flash drives. Ultimately, Buckshot Yankee became the inspiration for centralizing the nation's cyber forces in a major new organization.[54]



U.S. Army Cyber Command Insignia

U.S. Cyber Command

As the milestone events Eligible Receiver, Solar Sunrise, and Moonlight Maze had prompted the creation of the JTF-CND a decade earlier, Buckshot Yankee seemed to be the proverbial cyber straw that broke the camel's back. Between November 2008 and June 2009, Secretary of Defense Robert Gates ordered directives connected to the creation of a new subunified command to operate under U.S. Strategic Command. The new U.S. Cyber Command (USCYBERCOM) came together with the merger of the existing offensive cyber organization known as Joint Functional Component Command–Network Warfare and the defensive Joint Task Force–Global Network Operations. On the day that Gen. Keith Alexander received his fourth star, the "dual-hat" arrangement between the NSA and USCYBERCOM was born, with Alexander leading both organizations at Fort Meade, Maryland. On 4 May 2018, USCYBERCOM became the Nation's tenth unified combatant command, no longer subordinate to U.S. Strategic Command.[55]

USCYBERCOM needed subordinate cyber units from all the service branches, and accordingly, the Army chief of staff approved the creation of a new separate command in early 2010. Headquartered at Fort Belvoir, Virginia, the new U.S. Army Cyber Command (ARCYBER) officially activated on 1 October 2010 with Lt. Gen. Rhett Hernandez as its first commanding general.[56] Two months later, the Army approved the establishment of its first dedicated cyber brigade, the 780th MI Brigade at Fort Meade.[57] The 780th falls administratively under the Intelligence and Security Command but operationally answers to ARCYBER.

ARCYBER announced in December 2013 that its base of operations would move to Fort Gordon, Georgia, and in September 2014, the Cyber Protection Brigade, which is ARCYBER's defensive cyberspace

operations unit, was activated at Fort Gordon.[58] Ground was eventually broken for the new ARCYBER headquarters in November 2016, and the official move took place in July 2020.[59]

One of the most analyzed cyber events in history is the Operation Olympic Games, better known as Stuxnet. While Pentagon officials have never officially taken credit or admitted any involvement in the creation of this virus that substantially set the Iranian nuclear program back, numerous articles and books contend that Stuxnet was an American/Israeli joint venture.[60] Regardless, the designers successfully infected Iran's Natanz uranium enrichment facility computer systems with a virus called the Stuxnet worm. During 2009 and 2010, the malware destroyed more than one thousand of the six-and-a-half-foot-tall aluminum centrifuges by causing them to spin out of control and be rendered useless. After Stuxnet accidentally spread beyond the Natanz facility due to a programming error, those studying the worm marveled at the sophistication of its design. Stuxnet is considered to be the first computer virus to go after industrial systems and cause actual damage to physical equipment. Stuxnet was a game changer, a point of no return that ushered in a new era in which warfare would never be the same.[61]

Chinese and Russian Attacks

Circling back to China and its hacking activities since the 2003 discovery of the aforementioned Titan Rain, that nation's hacking became synonymous with cyber espionage and the theft of both U.S. defense and private corporation secrets. Another cyber first occurred in May 2014 when the United States handed out the first-ever state-actor cyber espionage indictments against five Chinese People's Liberation Army officers for stealing data from six American commercial targets. U.S. authorities labeled the five officers as members of Unit 61398, also known as Advanced Persistent Threat 1, which is believed to be linked to the initial Titan Rain attacks.[62] Alexander believes China's estimated gains from economic espionage cost the U.S. hundreds of billions each year, calling it "the greatest transfer of wealth in history."[63]

In 2015, the U.S. Office of Personnel Management delivered the news that during the previous year, unknown but believed to be Chinese nationals hacked the Office of Personnel Management network, making off with the personal information of over twenty-one million Americans. The majority of victims were U.S. military and government employees who had applied for security clearances. Anyone who has ever filled out one of those forms knows the level of deeply personal background information required. Not only was China stealing defense and economic secrets, but now it also owned the most personally identifiable information of millions of Americans, which could be used for data mining or social engineering on a scale heretofore never seen.[64]

While the last five years have witnessed several major cyber events around the world, the last significant hacking event discussed in detail here is how Russia successfully flipped off the power switch in two areas of Ukraine during what some refer to as the Russo-Ukrainian War. After its annexation of Crimea in 2014, the Russian government launched a series of cyberattacks against the former Soviet republic including two significant wintertime power outages. On 23 December 2015, hackers shut down a significant part of Ukraine's electrical grid in the Ivano-Frankivsk region of western Ukraine, gaining access to thirty electricity substations. Over two hundred thousand people were left without electricity for a period of one to six hours during this first confirmed hack to take down a power grid.[65] Nearly a year later, just before midnight on 17 December 2016, another cyberattack shut down the power grid for part of the Ukrainian capital of Kyiv. Instead of gaining access to the Ukrainian utilities' networks and manually switching

off power to electrical substations, as hackers did in 2015, the 2016 attack was fully automated. It was programmed to include the ability to communicate directly to grid equipment, sending commands in the obscure protocols those controls use to switch the flow of power on and off. This power cut amounted to a loss of about one-fifth of Kyiv's power consumption at that time of night, and it lasted about an hour. As with the first attack, Russian hackers were suspected to be behind the attack, demonstrating their penchant for treating Ukraine as a cyber test lab.[66]

(Photo courtesy of the U.S. Army Cyber School)

Cyber School and Cyber Branch

On 20 February 2013, TRADOC commander Gen. Robert Cone gave an important briefing at the Association of the U.S. Army Symposium in Fort Lauderdale, Florida. In his briefing, he called for the formal creation of a cyber school and career field within the U.S. Army. He stated the Army needed to "start developing career paths for cyberwarriors as we move to the future."[67] On 25 June 2013, Army Chief of Staff Gen. Raymond Odierno approved the establishment of a consolidated Army Cyber School at Fort Gordon. The purpose of the Cyber School would be to unify and integrate training for the new cyber career field.[68]

The Army released executive order 057-14 on 24 January 2014, which officially changed the Signal Center of Excellence to the Cyber Center of Excellence and established the U.S. Army Cyber School at Fort Gordon. The Cyber Center of Excellence force modernization proponent included "cyberspace operations, offensive and defensive cyber operations, signal/communications networks and information services, and electronic warfare." The Cyber School mission was to "conduct analysis for the required training needed to develop a highly skilled cyber force, trained to joint standards and ready to meet combatant commanders' current and future force requirements."[69]

On 4 August 2014, Lt. Gen. Robert Brown, commanding general of the U.S. Army Combined Arms Center, which oversees the various Army centers of excellence, presided over a multifaceted transfer of

authority ceremony on Fort Gordon. During the ceremony, Col. Jennifer G. Buckner became the first chief of cyber and first permanent commandant for the new U.S. Army Cyber School. Later the same day, Buckner, a career MI officer, unveiled the Cyber School sign and cut the ribbon leading into the headquarters building.[70] However, the fanfare only lasted one day as the small staff immediately set to work planning the course maps for the school. Official branch creation came next, and when staff members handed Odierno the routing form with the draft orders on 31 August 2014, he initialed approval and added in bold letters: "Important and Historic!" The Army officially established the Cyber Branch as a basic branch of the Army the next day with the release of Department of Army General Orders 2014-63, signed by Secretary of the Army John McHugh.[71] Now branch officials could proceed with creating the 17-series career fields for officers (17A), warrant officers (170A), and enlisted soldiers (17C). In October 2014, the Army announced a Cyber Voluntary Transfer Incentive Program for active duty officers, second lieutenant through colonel, and by June 2015, the Army outlined guidance for warrant officers and enlisted soldiers desiring a transfer to the Cyber Branch.[72]

The Cyber Branch has a historical connection to the MI and Signal branches, and certain duties, functions, and positions associated with Army cyber operations were derived from career fields within the Signal and Military Intelligence Corps. A basic connection we can make when discussing these parent branches is that offensive cyberspace operations is a child of MI, and defensive cyberspace operations is the offspring of Signal.

On 26 May 2016, the lieutenants from the first Cyber Basic Officer Leadership Course class became the first to ever graduate a Cyber School course.[73] The first warrant officers graduated from Cyber Warrant Officer Advanced Course in August 2016, and October 2016 saw the activation of the Cyber Training Battalion, which manages the students while they are attached to the school.[74]

Army leadership then decided the electronic warfare functional area now belonged in the cyber realm as the Army resurrected it from the ashes of post-Cold War atrophy to what became a vital sphere in the era of remote-controlled improvised explosive devices during the Global War on Terrorism. All electronic warfare officers, warrant officers, and noncommissioned officers officially became members of the Cyber Branch on 1 October 2018.[75] In February 2017, top-secret-level course content became a reality with the opening of the Cyber Training Facility, and in early August 2017, the first 17C Advanced Individual Training class graduated.[76]

Another huge milestone occurred in October 2017 when the acting secretary of the Army approved a pilot program for direct commissioning of civilians with the right skills as officers in the Cyber Branch.[77] The first two direct commissioned officers were sworn in on 9 May 2018, breaking the centuries old Army tradition of only directly commissioning officers into the medical, legal, and religious fields during peacetime. Over two years into what was originally a pilot, the Army continues this program for cyber. While members of the Army Cyber Corps are in many ways still figuring out their identity and traditions, they can be proud of all that the branch has accomplished in such a brief period of time. ■

Notes

1. *The National Military Strategy of the United States of America: A Strategy for Today: A Vision for Tomorrow* (Washington, DC: Joint Chiefs of Staff, 2004), 1, accessed 25 August 2020, https://history.defense.gov/Historical-Sources/National-Military-Strategy/.

2. Gordon Corera, *Cyberspies: The Secret History of Surveillance, Hacking, and Digital Espionage* (New York: Pegasus Books, 2016), 10; John Finnegan, *Military Intelligence* (Washington, DC: U.S. Government Printing Office, 1997), 29.

3. Corera, *Cyberspies*, 40; Finnegan, *Military Intelligence*, 47–48; James Gilbert and John Finnegan, eds., *U.S. Army Signals Intelligence in World War II: A Documentary History* (Washington, DC: U.S. Government Printing Office, 1993), 26. In reality, the peacetime signals intelligence activities of the U.S. government did not stop. In 1929, the Signal Intelligence Service (SIS) was created to control all Army cryptology and absorbed the covert intelligence-gathering activities formerly conducted by the Black Chamber. The new unit, led by William Friedman, was set up within the Signal Corps rather than the Military Intelligence Division to reduce its visibility and better meet the technical requirements of signals intelligence. In Friedman's own words, the intercept activities of the SIS were technically illegal, so they stressed the idea that any intelligence was a byproduct of "training" in cryptanalysis.

4. "Cottage Industry," Bletchley Park, accessed 25 August 2020, https://bletchleypark.org.uk/our-story/why-it-matters/cottage-industry.

5. *The Imitation Game*, directed by Morten Tyldum, screenplay by Graham Moore (Santa Monica, CA: Black Bear Pictures, 2014).

6. Corera, *Cyberspies*, 26.

7. Ibid., 30–34.

8. Gilbert and Finnegan, *U.S. Army Signals Intelligence in World War II*, 26.

9. Walter Isaacson, *The Innovators: How a Group of Hackers, Geniuses, and Geeks, Created the Digital Revolution* (New York: Simon & Schuster, 2014), 79.

10. Ibid., 73.

11. Ibid., 222; Thomas Rid, *Rise of the Machines: A Cybernetic History* (New York: W. W. Norton, 2016), 3.

12. Isaacson, *The Innovators*, 124.

13. Ibid., 202; Martin Childs, "John McCarthy: Computer Scientist Known as the Father of AI," Independent, 1 November 2011, accessed 26 August 2020, https://www.independent.co.uk/news/obituaries/john-mccarthy-computer-scientist-known-as-the-father-of-ai-6255307.html.

14. Steven Levy, *Hackers: Heroes of the Computer Revolution*, 3rd ed. (Sebastopol, CA: O'Reilly Media, 2010), 10.

15. Ibid., 49–56.

16. Ibid., 27–31. Elements of this hacker ethic include (1) access to computers should be unlimited and total; (2) all information should be free; (3) mistrust authority; (4) hackers should be judged by their hacking, not bogus criteria such as degrees, age, race, or position; (5) you can create art and beauty on a computer; and (6) computers can change your life for the better.

17. Henry Lichstein, "Telephone Hackers Active," *The Tech*, 20 November 1963, 1, accessed 26 August 2020, http://tech.mit.edu/V83/PDF/V83-N24.pdf.

18. For an exhaustive study on phone phreaking, see Phil Lapsley, *Exploding the Phone: The Untold Story of the Teenagers and Outlaws Who Hacked Ma Bell* (New York: Grove Press, 2013).

19. "SAGE: Semi-Automatic Ground Environment Air Defense System," Lincoln Laboratory, Massachusetts Institute of Technology, accessed 27 August 2020, https://www.ll.mit.edu/about/history/sage-semi-automatic-ground-environment-air-defense-system; Isaacson, The Innovators, 225–26.

20. Willis H. Ware, "Security and Privacy in Computer Systems" (lecture, Spring Joint Computer Conference, Atlantic City, NJ, 17–19 April 1967), accessed 27 August 2020, https://www.rand.org/pubs/papers/P3544.html.

21. *Security Controls for Computer Systems: Report of Defense Science Board Task Force on Computer Security* (Washington, DC: RAND Corporation, 11 February 1970), accessed 27 August 2020, https://csrc.nist.gov/csrc/media/publications/conference-paper/1998/10/08/proceedings-of-the-21st-nissc-1998/documents/early-cs-papers/ware70.pdf.

22. Carl Stieren, "ARPANET, Forerunner of the Internet, Becomes Permanent," It Happened in the 60s, 20 November 2012, accessed 27 August 2020, http://www.ithappenedinthe60s.com/posts/november-21-1969/#:~:text=By%20Dec.,and%20the%20University%20of%20Utah.

23. Corera, *Cyberspies*, 81.

24. Isaacson, *The Innovators*, 197–99.

25. H. Edward Roberts and William Yates, "ALTAIR 8800: The Most Powerful Minicomputer Project Ever Presented-Can Be Built for Under $400," *Popular Electronics* 7, no. 1 (January 1975): 33–38, accessed 27 August 2020, http://www.computermuseum.20m.com/popelectronics.htm; Isaacson, *The Innovators*, 337.

26. Levy, "Woz," chap. 12.

27. Fred Kaplan, *Dark Territory: The Secret History of Cyber War* (New York: Simon & Schuster, 2016), 1, 9–10.

28. Ibid., 1–2.

29. Timothy Winslow, "I Hacked into a Nuclear Facility in the '80s. You're Welcome," CNN, 3 May 2016, accessed 27 August 2020, https://www.cnn.com/2015/03/11/tech/computer-hacker-essay-414s/index.html.

30. Sally Bedell Smith, "CBS is Revising Show on Computer Tampering," *New York Times* (website), 1 September 1983, accessed 27 August 2020, https://www.nytimes.com/1983/09/01/arts/cbs-is-revising-show-on-computer-tampering.html.

31. Kim Zetter, "Nov. 10, 1983: Computer 'Virus' is Born," *Wired* (website), 10 November 2009, accessed 27 August 2020, https://www.wired.com/2009/11/1110fred-cohen-first-computer-virus/.

32. Stuart Diamond, "Credit File Password is Stolen," *New York Times* (website), 22 June 1984, accessed 27 August 2020, https://www.nytimes.com/1984/06/22/business/credit-file-password-is-stolen.html.

33. For more details on Stoll's persistent investigation into the hacker, see Clifford Stoll, *The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage* (New York: Doubleday, 1989); or the shorter article, Clifford Stoll, "Cuckoo's Egg: Stalking the Wily Hacker," in *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*, ed. Jason Healey (Vienna, VA: Cyber Conflict Studies Association, 2013), 89–106.

34. Stoll described his investigation into the "Morris Worm" incident in the epilogue of Stoll, *The Cuckoo's Egg*, 308–23.

35. Robert T. Morris eventually became a tenured professor in the Electrical Engineering and Computer Science Department at the Massachusetts Institute of Technology. For more details on the "Morris Worm" incident, see Corera, *Cyberspies*, 131–45.

36. "The State of Ransomware in the US: Report and Statistics 2019," EMISOFT Blog, 12 December 2019, accessed 27 August 2020, https://blog.emsisoft.com/en/34822/the-state-of-ransomware-in-the-us-report-and-statistics-2019/.

37. Kaveh Waddell, "The Computer Virus that Haunted Early AIDS Researchers: The First-Ever Ransomware Attack was Delivered on a Floppy Disk," *The Atlantic* (website), 10 May 2016, accessed 27 August 2020, https://www.theatlantic.com/technology/archive/2016/05/the-computer-virus-that-haunted-early-aids-researchers/481965/.

38. Isaacson, *The Innovators*, 410–14.

39. *Sneakers*, directed by Phil Alden Robinson (Los Angeles: Universal Studios, 1992).

40. Kaplan, *Dark Territory*, 31–32.

41. Joint Publication 2-0, *Joint Intelligence* (Washington, DC: U.S. Government Printing Office, 22 October 2013), GL-11. Red teaming is defined as "an organizational element comprised of trained and educated members that provide an independent capability to fully explore alternatives in plans and operations in the context of the operational environment and from the perspective of adversaries and others."

42. Kaplan, *Dark Territory*, 68–70; Corera, *Cyberspies*, 171–72.

43. Tim Maurer, "SOLAR SUNRISE: Cyber Attack from Iraq?," in Healey, *A Fierce Domain*, 121–35.

44. Newsweek Staff, "We're in the Middle of a Cyberwar," *Newsweek* (website), 19 September 1999, accessed 28 August 2020, https://www.newsweek.com/were-middle-cyerwar-166196.

45. "Moonlight Maze Lives On? Researchers Find 20-Year-Old Link to Current APT," Secure World, 3 April 2017, accessed 28 August 2020, https://www.secureworldexpo.com/industry-news/moonlight-maze-lives-on-researchers-find-link-to-current-apt.

46. Adam Elkus, "Moonlight Maze," in Healey, *A Fierce Domain*, 152–63.

47. Healey, *A Fierce Domain*, 44–47; "U.S. Cyber Command History," U.S. Cyber Command (USCYBERCOM), accessed 28 August 2020, https://www.cybercom.mil/About/History/.

48. "History," 780th Military Intelligence (MI) Brigade, accessed 28 August 2020, https://www.inscom.army.mil/msc/780mib/history.html.

49. Healey, *A Fierce Domain*, 51.

50. Corera, *Cyberspies*, 189; "After Copying F-35's Stealth, China's J-20 Duplicating its Non-Stealth Features," DefenseWorld.net, 4 June 2020, accessed 28 August 2020, https://www.defenseworld.net/news/27131/After_Copying_F_35_s_Stealth__China_s_J_20_Duplicating_its_Non_Stealth_Features.

51. Joshua Davis, "Hackers Take down the Most Wired Country in Europe," *Wired* (website), 21 August 2007, accessed 28 August 2020, https://www.wired.com/2007/08/ff-estonia/.

52. Andreas Schmidt, "The Estonian Cyberattacks," in Healey, *A Fierce Domain*, 174–77.

53. Kaplan, *Dark Territory*, 164-65.

54. Karl Grindal, "Operation BUCKSHOT YANKEE," in Healey, *A Fierce Domain*, 205–11.

55. USCYBERCOM, "U.S. Cyber Command History."

56. "History," U.S. Army Cyber Command, accessed 28 August 2020, https://www.arcyber.army.mil/Organization/History/.

57. 780th MI Brigade, "History."

58. Subordinate units of the 780th MI Brigade are the 781st MI Battalion at Fort Meade and the 782nd MI Battalion at Fort Gordon; Neil Guillebeau, "Army Cyber Brigade Activates at Fort Gordon," Army.mil, 12 September 2014, accessed 28 August 2020, https://www.army.mil/article/133614/army_cyber_protection_brigade_activates_at_fort_gordon.

59. Wesley Brown, "Army Cyber Command Announces Fort Gordon as New Headquarters," *Augusta Chronicle* (website), 19 December 2013, accessed 31 August 2020, https://www.augustachronicle.com/article/20131219/NEWS/312199907; "Groundbreaking Marks 'Leap Forward' for Army Cyberspace Operations," Army.mil, 1 December 2016, accessed 28 August 2020, https://www.army.mil/article/178917/groundbreaking_marks_leap_forward_for_army_cyberspace_operations; "Army Cyber Command Ceremony Heralds Its Arrival at New Headquarters at Fort Gordon," Army.mil, 24 July 2020, accessed 28 August 2020, https://www.army.mil/article/237570/army_cyber_command_ceremony.

60. One example is David Sanger, *The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age* (New York: Crown, 2018), 9.

61. For more reading on Stuxnet, see Kim Zetter, *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon* (New York: Crown, 2014); Kim Zetter and Huib Modderkolk, "Revealed: How a Secret Dutch Mole Aided the U.S.-Israeli Stuxnet Cyberattack on Iran," Yahoo! News, 2 September 2019, accessed 28 August 2020, https://news.yahoo.com/revealed-how-a-secret-dutch-mole-aided-the-us-israeli-stuxnet-cyber-attack-on-iran-160026018.html.

62. Sanger, *The Perfect Weapon*, 119–20; "What Is an Advanced Persistent Threat (APT)?," Kaspersky, accessed 3 September 2020, https://www.kaspersky.com/resource-center/definitions/advanced-persistent-threats. According to Kaspersky, an APT is an "advanced persistent attack using clandestine, and sophisticated hacking techniques to gain access to a system and remain inside for a prolonged period of time, with potentially destructive consequences."

63. Adam Segal, "From TITAN RAIN to BYZANTINE HADES: Chinese Cyber Espionage," in Healey, *A Fierce Domain*, 173.

64. Sanger, *The Perfect Weapon*, 111–17.

65. Kim Zetter, "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid," *Wired* (website), 3 March 2016, accessed 28 August 2020, https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/.

66. Andy Greenberg, "How an Entire Nation Became Russia's Test Lab for Cyberwar," *Wired* (website), 20 June 2017, accessed 28 August 2020, https://www.wired.com/story/russian-hackers-attack-ukraine/.

67. "Army Leaders See Much Cyber Work to Do," Taktik(z), 24 February 2013, accessed 16 February 2017, http://taktikz.com/2013/02/24/army-leaders-see-much-cyber-work-to-do/.

68. "New Center, School to Bring Signals, Cyber, EW Together," *Military Times* (website), 25 June 2013, accessed 28 August 2020, https://www.militarytimes.com/2013/06/25/new-center-school-to-bring-signals-cyber-ew-together/.

69. Headquarters Department of the Army Executive Order 057-14, "Cyber Center of Excellence (COE) Establishment," 24 January 2014.

70. Meg Mirshak, "Fort Gordon Unveils U.S. Army Cyber School Headquarters," *Augusta Chronicle* (website), 4 August 2014, accessed 8 January 2016, https://www.augustachronicle.com/article/20140804/NEWS/308049896.

71. John M. McHugh, Department of the Army General Orders (DAGO) 2014-63, "Establishment of the United States Army Cyber Branch," 21 August 2014.

72. Officer - Military Personnel (MILPER) Message 14-298, 8 October 2014; Enlisted - MILPER Message 15-164, 2 June 2014; Warrant Officer - MILPER Message 15-166, 4 June 2015.

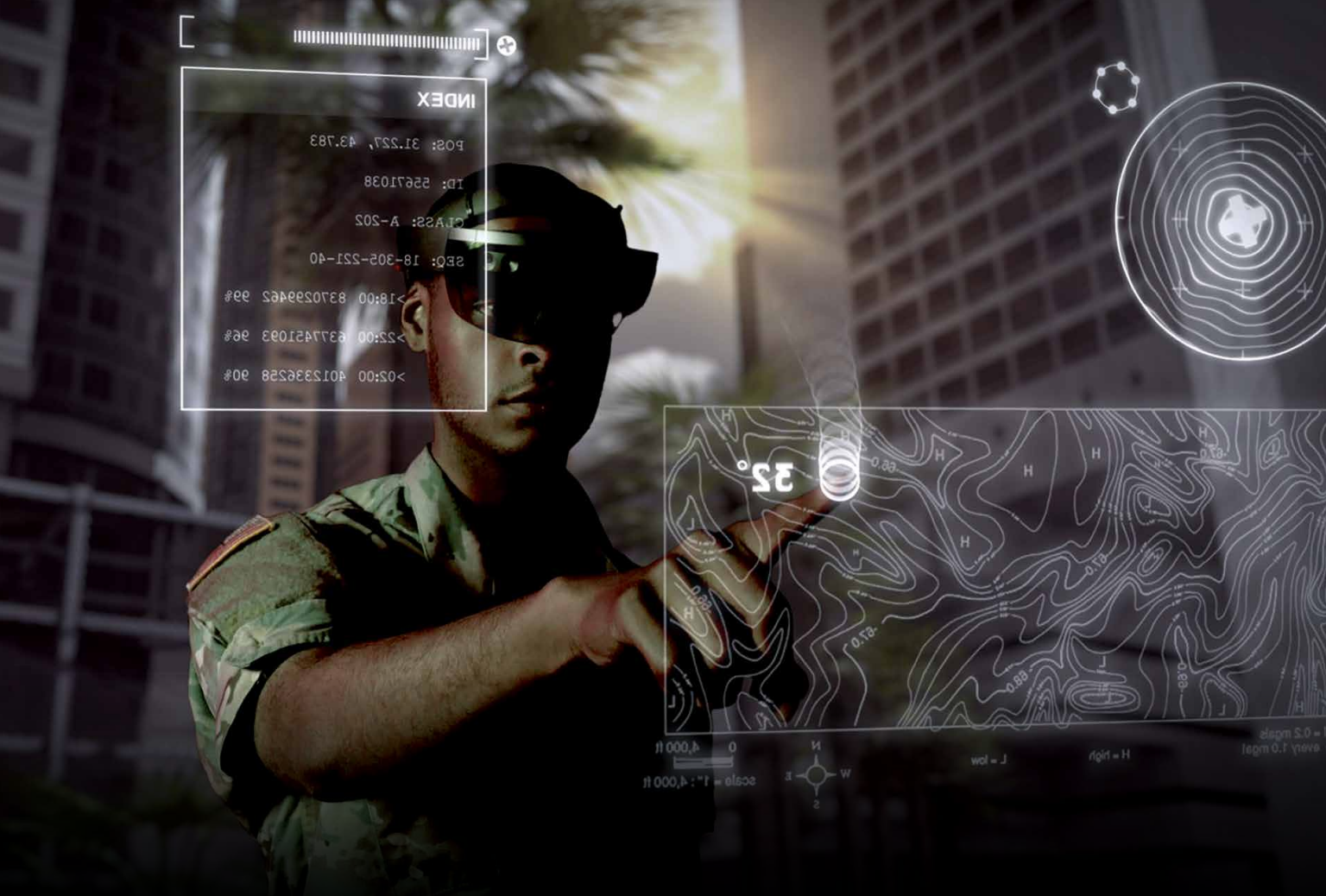
73. Laura Levering, "Army Cyber School Marks Major Milestone," Army.mil, 17 August 2015, accessed 28 August 2020, https://www.army.mil/article/154001/Army_Cyber_School_marks_major_milestone/.

74. Danielle S. Covington, "Cyber Training Battalion Activates," *Fort Gordon Globe* (website), 14 October 2016, accessed 31 August 2020, https://www.fortgordonnews.com/articles/cyber-growth-2/.

75. Nick Spinelli, "Cyber Celebrates 4 Years, Welcomes New Branch," *Fort Gordon Globe* (website), 5 October 2018, accessed 31 August 2020, https://www.fortgordonnews.com/articles/cyber-celebrates-4-years-welcomes-new-branch/.

76. Nefeteria Brewster, "Fort Gordon Graduates First Class for Cyber School," *Augusta Chronicle* (website), 8 August 2017, accessed 9 September 2020, https://www.augustachronicle.com/news/2017-08-08/fort-gordon-graduates-first-class-cyber-school.

77. Ryan D. McCarthy, Memorandum for Principal Officials of Headquarters, Department of the Army, "Army Directive 2017-26 (Pilot Program for Direct Commission to Cyber Positions)," 27 October 2017 (superseded).



Human experience-driven mixed reality research is shaping how soldiers will operate and train. (Graphic courtesy of the U.S. Army Combat Capabilities Development Command Soldier Center)

The Fourth Domain

Lt. Col. Brian R. Hildebrand, Texas Army National Guard

Today the U.S. Army is in the midst of a digital disruption. The Army's senior leaders are fully aware of this.[1] With the establishment of the Army Futures Command in 2018 and the publication of the "Army Modernization Strategy" (AMS) in 2019, senior leaders believe shifting from an industrial age mindset to an information age mindset will help the Army get past the systemic shock of technology-induced turbulence and prepare it for multi-domain operations by 2035.[2] According to the World Economic Forum, digital technologies are contributing to a near complete overhaul of how the world operates, running the gamut from transportation and finance to communication and leadership.[3]

The broad range and scope of technology across society has had a significant impact on the Army's leader development strategy. Addressing the current state of affairs for technology, how innovation and technology are insinuated into the current leader development domains, and how a technological domain develops leaders and

what that looks like will lead to an examination on why the Army's culture needs a technological domain.

Technology in the Now

Over the last three years, the Army has consistently defined the new strategic environment as a great-power competition among geopolitical superpowers. Whereas during the wars in Afghanistan and Iraq, the U.S. Army focused mainly on violent extremist organizations, today the Army's senior leaders have shifted the focus to the peer threats of Russia and China.[4] The AMS further delineates focus areas in which Russia and China have outpaced the United States in terms of technological capabilities and establishes Army research priorities in order to make up ground.[5]

Hanging in the balance is technology's role in the Army's modernization strategy. Army leaders have a difficult task of striking the equilibrium between embracing technology as a simple solution to complex problems and applying technology as a tool.[6] Leaders intent on using technology can be lured into rushing its use with reckless abandon. How do they avoid technology's siren call?[7]

There is no question that the Army is in desperate need of modernization and that emerging technology is a central tenet in its strategy to modernize. As the Army modernizes "who we are," technology and innovation play a dominant role in leader development and education.[8] The Army needs more critical and creative leaders capable of systems thinking and who are able to streamline emerging technologies into the business of leadership and command and control of the battlefield.

Updating the Framework

The recently published Army Doctrine Publication (ADP) 6-22, *Army Leadership and the Profession,* manifests this growth.[9] It is a good mix of updates for Army leader development and a continuity of legacy concepts. The dynamics of leadership require leaders to understand in context themselves, those who they lead, and the situation.[10] Furthermore, the "Army Leader Development Strategy" is still heavily vested in the institutional Army, the operational Army, and the individual.[11] This framework enables three lines of effort of training, education, and experience.[12] Within these updates and framework, where do dynamically astute leaders sort out the most critical inputs and application of technology to leader development?

Ultimately the goal of the "Army Leader Development Strategy" is to create adaptive leaders who can exercise mission command to prevail in a complex and contested multi-domain operational environment.[13] Competence is part of the Army leadership foundation, which leads to proficiency, expertise, and mastery. ADP 6-22 defines three core leadership competencies: lead, develop, and achieve.[14] Each of these are further broken down into more competencies, ultimately making ten competencies total for Army leaders.[15] Through training, education, and experience, the Army affords leaders opportunities to develop these competencies into proficiencies.[16] These opportunities come in the form of challenging experiences.[17] Whether in the institutional, operational, or self-development domain, the challenges are laden with technology.

Institutional domain. Technology infuses training, education, and experience in the institutional domain to build a foundation for leadership capabilities. Technology enhances learning outcomes to keep apace of the emerging requirements of the multi-domain operations (MDO) environment. It does this through a variety of means: faster access to information; greater opportunity for higher levels of education through online venues; increased responsiveness through artificial intelligence; and enhanced knowledge retention, analytic reasoning, and satisfaction through virtual training simulators.[18] Ultimately, technology creates institutional agility and soldier adaptability, allows greater synergy between the various primary military education institutions and academia, and supports the fluency of technology required for implementing the "Army People Strategy."[19]

Operational domain. In the operational domain, where concepts and lessons from the institutional domain are improved upon and refined, technology is a key enabler.[20] The recursive nature of training, education, and experience in the

Lt. Col. Brian R. Hildebrand, Texas Army National Guard, is serving on a Title 10 tour with the Army Futures Command, Human Capital Directorate. He holds a BA from the University of Saint Thomas and an MS from Norwich University. His previous assignments include J7 (Joint Professional Development, Leadership, and Education) director for the Texas Military Department Joint Forces Headquarters, G5 (chief of plans) for the 36th Infantry Division, and commander of 3rd Battalion, 133rd Field Artillery Regiment.

Soldiers with the 730th Area Support Medical Company of the South Dakota Army National Guard conduct virtual convoy operations training 14 June 2018 during Exercise Golden Coyote at Camp Rapid, South Dakota. (Photo by Spc. Jeffery Harris, U.S. Army)

operational domain makes technology fluency a must. As leaders teach others, they learn, and they are heavily dependent on technology to do this. Training complexity runs the gamut from the simple to the complex. Sometimes it is a laptop with PowerPoint for completing Army Regulation 350-1, *Army Training and Leader Development*, training requirements; sometimes it is using Adobe Connect to host an online unit professional development program; and sometimes it is using technology to do terrain walks on virtual battlefields for reviewing case studies in tactics. In any case, technology is the main conduit for Army learning and education in the operational domain.[21]

Perhaps the best example of technology enabling, not replacing, leaders in the operational domain is the application of mission command.[22] Leaders use mission command to command and control forces both at home station and while deployed. In garrison, technology's visage takes the form of the Integrated Personnel and Pay System–Army, the Defense Readiness Reporting System–Strategic, the Defense Training Management System, and the Director's Personnel Readiness Overview. These systems of record, and myriad other semiautonomous reporting systems, give leaders at every echelon situational understanding of important key readiness indicators and help to inform decisions from the tactical to the strategic. While deployed, there are multiple technology systems used to exercise mission command. These technologies, like Force XXI Battle Command Brigade and Below and the Advanced Field Artillery Tactical Data System, are used to facilitate a common operating picture, increase situational understanding, and enhance decision-making. As the force grows and technology becomes more capable, these systems will augment more of the leader's decision-making, not taking the human element out of it but rather shaping processes and activities so that the interaction with the system is a mental, social, and physical extension of the self.[23]

Self-development domain. Where leaders encounter technology unencumbered and use it with incredible fluency is in the self-development domain. The ubiquity

of online degree programs, the emergence of handheld portable devices such as smartphones and tablets, and the ever-increasing availability of shared ideas through social media is fundamentally changing how everyone thinks, processes information, and ultimately learns.[24] Leaders across the Army have incredible access to opportunities for self-development and self-awareness. Technology helps these leaders fulfill their commitment to stay on the cutting edge of the profession.[25]

First, it increases the outlets for reading and learning. Many senior leaders in the Army publish reading lists for diverse audiences in order to encourage leaders to self-develop. Audiobooks and podcasts are another example. Those who do not like reading or lack the time and industry can learn through listening.

Next, technology cultivates the ability to conduct research through information immediacy. The internet not only allows leaders to dig deeper into the subjects they learn about through reading and experience, but it also connects them to subject-matter experts on a range of relevant topics. Technology also spurs on the capacity for continuous writing through social media platforms such as blogs, online forums, and digital media. Leaders can submit original work for publication, post ideas on a blog, and participate in professional discussion through Twitter, Facebook, or Instagram.[26]

Lastly, technology facilitates self-awareness. Online surveys and personal assessments, such as the Multisource Assessment and Feedback program, the Commander 360 program, and myriad other personal assessments, increase self-awareness for Army leaders through candid comments from subordinates, peers, and superiors. Self-awareness is further enhanced in leaders through the practices of mindfulness and meditation.[27] There are multitudes of smartphone apps for guided meditation and mindfulness, which can reposition the leader into a better posture of self-awareness.

Basically, for the self-development domain, technology translates challenges for improvement into opportunities for growth and self-awareness. The human element is not diminished by technology. Leaders still must aspire to improve and develop self-awareness; it does make satisfying these aspirations and achieving self-awareness easier.

Technology: The Fourth Domain

While technology infuses training, education, and experience in all three leader development domains, its impact is so great on the profession that it deserves consideration as a separate leadership domain with its own necessary training, education, and experiences.

> Advances in professionalism seem to be positively correlated with advances in technology and the increasing specialization they require. As technology improves, war fighting becomes more complex. With each iteration of technology—from catapults to artillery, horse-mounted cavalry to armored vehicles, sails to steam, hot air balloons to fixed-wing flight—militaries developed new core competencies. Driven by technology, these new core competencies required an equal development of technical understanding within the professional force that fields them.[28]

Making a fourth leadership development domain, specifically a technological domain, allows for the requisite development in technical understanding required of today's leaders.

What does the technological domain look like? As with the other leadership domains, it is both a reflection of society and the means by which the Army develops effective leaders for the future.[29] The ultimate goal of the technological domain is the technologically fluent leader. Taking these in short order, how does the technological domain reflect society? How does the Army use the technological domain to develop leaders? What does it look like? And what is technology fluency?

How the Fourth Domain Reflects Society

The Army has a shared identity with the society that it has sworn to protect.[30] Even though the technological domain fosters learning outcomes, developmental assignments, and self-awareness, it reflects many of the same structural changes currently underway in society. As technology redefines our current way of life, society and the Army (1) become more dependent on rapid and far-reaching technology, (2) capitalize on the globalization of information, (3) prioritize knowledge over physical attributes, and (4) flatten hierarchies.[31]

Rapid and far-reaching technology. In many ways, the Army's dependency on rapid and far-reaching technology is manifested in the way that it delivers battlefield results. The technological domain accounts for the imperative within each branch to understand the

impact of breakthrough technologies. Take, for example, the emerging tank technology of the interwar period. Two prescient and well-known Army leaders, Dwight D. Eisenhower and George S. Patton, took on the institution to bring about the tactics and techniques for armor on the battlefield. They learned a lot from their time as instructors at tank schools during World War I, presented their ideas in scholarly work during the interwar period, and then ultimately tested their theories during the series of Army maneuvers leading up to World War II.[32] Eisenhower and Patton understood the Army's dependency on new technology, and fortunately, they possessed the requisite knowledge and vision to use this technology effectively enough to prove it to the rest of the Army. This same trend is visible in today's Army senior leaders. With the publication of the AMS and the Army priority research areas, the Army at least knows what it needs to learn.[33] This is an important first step. The remainder of the equation is lining up the emerging technology leaders (ETL) to carry this technology to the battlefield. Although this remains to be seen, the global advance of technology is propelling this initiative evermore.

> "Technology … deserves consideration as a separate leadership domain with its own necessary training, education, and experiences."

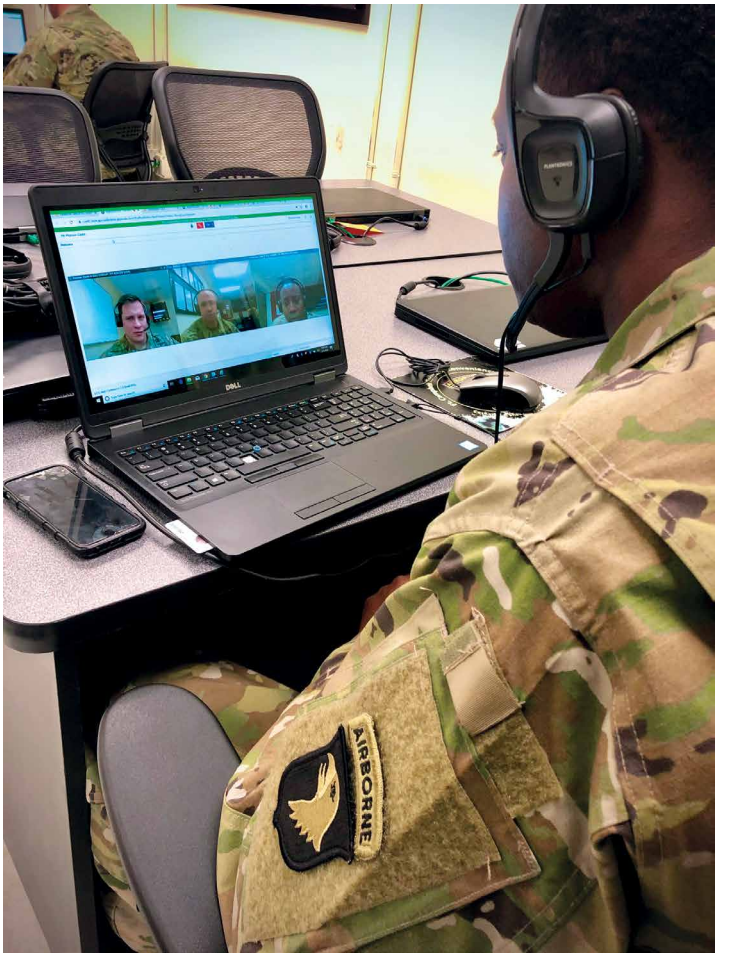
Globalization of information. Technology is not the only thing moving at breakneck speed across the world. Globalization and the Internet has created an information superhighway with multiple ingresses and egresses for users everywhere. As globalization and the dynamic spread of information change how society communicates, shares ideas, and creates meaning, the technological domain accounts for the essential operational requirement within the Army to exploit information into understanding, and ultimately, action.[34] The Army has done this before but not in an all-encompassing leader development strategy such as is articulated with the fourth domain. Rather, the Army proved the importance of intelligence dominance and the ubiquity of information available during operations in Iraq and Afghanistan with Task Force (TF) 714.[35] Gen. Stanley McChrystal and his crew, including Adm. William McCraven and Lt. Gen. Michael Flynn, flipped the script on the enemy. Instead of focusing on destroying targets—people, places, and equipment—TF 714 focused on exploiting intelligence. This was a complete paradigm shift. These leaders perceived information to be the greatest common divisor on the battlefield. This drove McChrystal's decisions and allowed him to get the best possible result from the most efficient intelligence work, resulting in what Gen. Raymond Odierno called the "irreducible minimum."[36] The Army's appreciation of intelligence dominance continues even now. In today's globally connected and networked society, information looms large in every military operation. Securing the primacy of educating, training, and experiencing successful exploitation of information globalization is one of the main thrusts behind standing up the technological domain.

Primacy of knowledge over physical attributes. The discussion about the ubiquity of information segues perfectly into the conversation about the digital world, virtual world, and cyberspace. There is no denying the assertion that millions of users plug into a virtual world each day in order to be someone more or other than themselves. As society continues to shift from the physical to the virtual, the Army does the same. The implications for this transition are staggering. The Army, which is built for land warfare, may need to commit multiple resources to operate in the cyber domain. In other words, a virtual battle in cyberspace could potentially carry the same significance as a physical battle on the ground (primarily because in an MDO environment, crossover between domains is imperative for success). In this sense, the enemy is more an organism in a virtual-physical ecosystem as opposed to an organization of people and equipment. This means the Army must learn to attack not just people and machines but processes.[37] The technological domain accounts for the imperative to develop technology such as machine learning, artificial intelligence, and algorithms in order to combat these multi-domain threats.

The technological domain not only creates opportunities within each branch for leaders to learn the cutting-edge research required for this type of mission success, but it also provides the training and experience necessary for judging the operational relevance of this technology.[38]

Flattened hierarchies. A digital or networked society is a nonhierarchal, decentralized, flattened society.[39] Prima facie, this is the one area where the Army does not mirror the shift in society, as the Army is perceptibly the quintessential American hierarchy. The Army's tenacity for mission command and recent operations, such as Defender-Europe 20, suggest otherwise. The essential key to success for Allied partners participating in Defender-Europe 20 was interoperability, which is the principle of "fungibility or interchangeability of force elements and units … [and] … the mechanics of system technical capabilities and interfaces between organizations and systems."[40] In other words, despite the cultural and language differences of partners, they come together from diverse locations to achieve a mission because they share a common goal. The Army's use of mission command supports interoperability. Even though communication and information technologies improve situational understanding, the autonomy of the leader on the battlefield to accomplish the mission is the main thrust of decentralized operations and a mission command imperative. The more decentralized the organization, the better able the leader is to handle the "on demand" requirements and stay ahead of emerging threats.

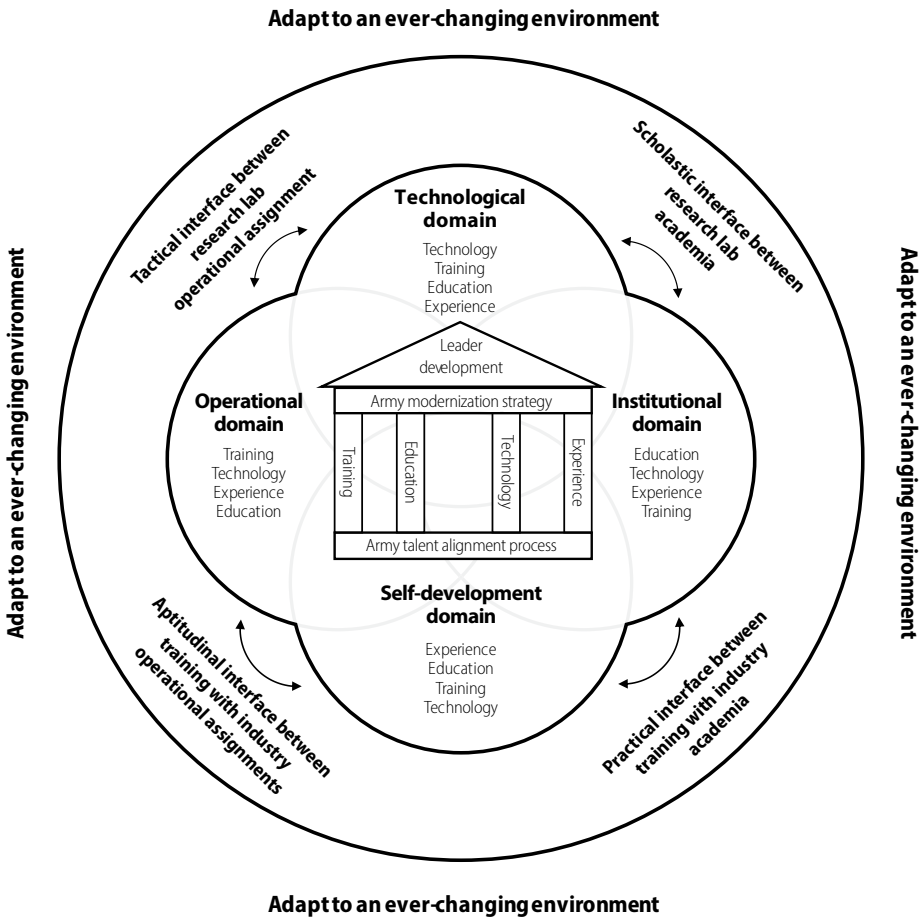
In today's world, a hierarchical organization that cannot effectively transition part of its systems to horizontal models fails because it is too slow and bureaucratic and cannot respond appropriately to the constantly changing environment. The Army flattens itself through mission command and finds the sweet spot between hierarchy and autonomy by using technology.[41] The technological domain accounts for the adaptability and nimbleness required to cope with the speed, volatility, complexity and ambiguity of an MDO environment. It does through developing leaders who can bring together all of the assets onto the battlefield despite physical locations, reduce knowledge silos and information stovepipes, and connect subordinates to resources for decentralized decision-making in the midst of high-intensity operations.



Sgt. 1st Class Jerry Dickerson, a facilitator assigned to the 101st NCO Academy at Fort Campbell, Kentucky, uses the Defense Collaboration Services website to meet with other facilitators 31 March 2020 in preparation for the daily face-to-face time between the facilitators and Basic Leader Course students at Fort Bliss, Texas. (Photo by Sgt. 1st Class Jedhel Somera, U.S. Army)

How the Technological Domain Develops Leaders

Participating in the digital and networked society not only sustains the Army's pace with social forces, ideologies, and institutions dominant within society, it also allows the Army to meet the demands of the twenty-first-century security environment.[42] The Army will do this primarily through its people and



(Figure adapted by author based on the Army Leader Development Model, *Army Leader Development Strategy 2013*)

Figure. The Fourth Domain

through its technology. The key bridge between the two is the technological domain.[43]

The Army and technology are inseparable. "The Army has been and will continue to become increasingly dependent on technology as a combat multiplier."[44] As with the other leader development domains, the technological domain develops leaders through a composite of training, education, and experience, but it does this through the lens of technology (see figure). Thus, the technological domain also develops leaders through innovation, modernization, and transformation initiatives.

Innovation. The Army has a long and storied history with innovation.[45] The defining character of successful innovations in the past has been the presence of a champion, a senior leader with a strong will and persistent personality.[46] This reinforces the core belief in the Army that its people are its greatest asset and affirms the nexus between developing leaders and innovation. The aptitude for innovation within leaders is in the bailiwick of the fourth domain. In other words, the technological domain is where leaders learn how to be agents of organizational change that helps to accomplish missions, is unique in character or application, and is underwritten by the Army at large.[47]

Modernization. Modernization builds on innovation. Focused on "how we fight, what we fight with, and who we are," the Army Modernization Framework shows how the Army will be ready for the MDO fight by 2035 despite competing priorities and reduced spending power.[48] In this sense, modernization describes ongoing processes aimed at overcoming the bureaucracies that suffocate innovation. The competitive advantage in cutting through the red tape is innovative and adaptive leaders.[49] The technological domain is the place where Army leaders learn to visualize, describe, direct, lead, and assess new ways of fighting with emerging technology and advanced equipment.

Transformation. Ultimately, innovation and modernization lead to transformation. Transformation is not a novel concept. In the last fifty years, the Army has undergone multiple transformations; one of the most important is the result of the Goldwaters-Nichols Act of 1986.[50] The Army is in the midst of another transformation. The Army is not "trying to fight the last fight better. We're focused on winning the next

Soldiers don the Integrated Visual Augmentation System (IVAS) Capability Set 2 Heads-Up Display 20 November 2019 during Soldier Touchpoint 2 testing at Fort Pickett, Virginia. The test is designed to provide feedback to Program Executive Office Soldiers so that IVAS can be further enhanced before two hundred thousand headsets begin to be fielded in 2021. (Photo by Courtney Bacon)

fight. To do that, we recognize the need for transformational change."[51] Transformation ensures that the Army moves from its current state of limited technology to a future state of unbridled innovation. Transformation also defines the ends, ways, and means for reaching this future state. The primary means for Army transformation is its people.[52] The technological domain is where innovative leaders embrace the philosophy of "people first" and where the attitude of "winning matters" meets the future operating and environment concepts and technology development required to build the Army that will fight for the next forty years.[53]

A Look inside the Technological Domain

Technical, academic research, and laboratory assignments would make up the preponderance of focus areas in the fourth domain and offer multiple ways for achieving transformational change. Leaders are ideally assigned to technological positions, upon completion of an advanced science, technology, engineering, or mathematics (STEM) degree from the civilian education system and after gaining the operational experience from a variety of challenging assignments.

Technological assignments prepare officers to integrate emerging technologies on the battlefield and better position them to advise the commander and other senior leaders in the field as to the requirements, implementation, advantages, and disadvantages of emerging technologies. Technical leaders introduce emerging technology to the unit and establish technology development programs in order to increase the knowledge of that emerging technology and its efficacy on the battlefield.

Assignment to academic research positions throughout the career time line provides technical leaders with an educational opportunity to further development or hone technical competencies through research, writing, publishing, and involvement with professional education, curriculum development, and academic instruction. Similarly, periodic assignment to laboratory positions throughout the career time line provides technical leaders with exposure to a different analytical environment.

The laboratory presents them with opportunities to work complex STEM problems and cutting-edge research. Ultimately, laboratories are where the Army grows strategic, adaptive, and innovative technical leaders

with expert capabilities in Army priority research areas: disruptive energetics, radio frequency electronic materials, quantum, hypersonic flight, artificial intelligence, autonomy synthetic biology, material by design, and science of additive manufacturing.

Fluency of Technology

While the Army envisions multiple ends for this transformational change, an investment in the Army's people is its greatest aspiration. The bottom line is that the technological domain creates leaders who are fluent in technology. To do this, the Army must expand its discourse community to include a technical vernacular. "A discourse community is a group of individuals who share a common language, common knowledge base, common thinking habits, and common intellectual assumptions."[54] True, the Army needs leaders who are fluent in technology. Even more true, however, is that the Army needs leaders who are literate in technology. The difference between technology fluency and technology literacy is mastery. Borrowing from educational technologist Clint Lalonde's idea of digital literacy and digital fluency, technological literacy is an understanding of how to use the new technologies or tools, such as any one of the emerging technologies promoted through the AMS.[55] Technology fluency is the ability to create a new process, procedure, or tactic using emerging technology. Eisenhower and Patton did this with tanks.[56] Fluency also includes "being able to move nimbly and confidently from one technology to another."[57] Thus, when the "Army People Strategy" speaks of the fluency of technology, it does so on a continuum or by degrees of mastery. At the very least, all Army leaders must be literate in technology, with the idea that they ultimately move along the continuum of proficiency to fluency.

Army Culture and the Fourth Domain

The Army is built on a culture of trust that rests on the Army values of loyalty, duty, respect, selfless service, honor, integrity, and personal courage.[58] In order for the Army to develop adaptive leaders who can compete in an MDO environment, it has to update its culture to include innovation and technology.[59] The best way to do this is through the technological domain. Here are a couple reasons why.

The technological domain connects the recent modernization initiatives like the AMS, the Army Talent Management Task Force, and the "Army People Strategy" to the core enterprise of leader development. The Army has taken an important first step in the right direction with the collaboration of the Army Talent Management Task Force to create a career field for an ETL.[60] In the past, similar programs such as the Uniformed Army Scientist and Engineer Program failed because they were too different from the mainstream Army. The Uniformed Army Scientist and Engineer Program's focus was too narrow, its skillset too unique, and its career path too divergent.[61] Additionally, it is hard for the rest of the Army to learn new techniques, tactics, and procedures or benefit from the capabilities of such a relatively small and loosely structured group of people who research and develop avant-garde projects. Small groups lack the resources to take their innovative ideas and processes enterprise wide. Having a technological domain would create the required culture necessary to sustain the career paths of the ETL, share the successes of their capabilities with the rest of the Army, scale their innovations, and really educate the force on MDO.[62]

Having a technological domain also diminishes the effects of organizational bureaucracy on innovation. The Army creates bureaucracy as a byproduct of organizational behavior and institutional processes. This happens in two ways. First, each level of the Army has its own unique bureaucracy because each level has its own understanding of how things are done and what things mean. Bureaucracy also arises during succession in senior leaders, who do not always agree on the same vision and future for the organization. As a result, desynchronization between levels of bureaucracy and succession of senior leaders typically results in frustration and innovation failure.[63] Having a technological domain, however, provides a clearinghouse for understanding the principles and practices of innovation and technology.

Technology is not a panacea. It does not supersede the primacy of mission command and human decision-making on the battlefield, and it cannot replace boots on ground during combat.[64] The technological domain puts technology in its proper place where leaders can learn how to use it to augment tactics, techniques, and procedures. The true value of technology is in how it is used, not what it can do. Having a technological domain ensures this.

Conclusion

The Army and technology have an undeniable nexus. Throughout history, technology has fueled military innovation, and it will continue to do so into the future. The Army senior leaders have the right logic. Their attempt to build a sustainable career path for the ETL signals the importance of embracing technology for the future MDO fight and sets the Army on a new trajectory. Will the career path for the ETL be sustainable? While this remains to be seen, the argument for the technological domain presents a fundamentally different approach for preparing the Army for the future MDO fight. This approach recognizes the potency of technology in leader development, engineers the framework to match skills to opportunities, and fosters an Army culture necessary to sustain the importance of technical understanding into the future. If the Army adopts a technological domain as part of the leader development strategy, it is not abandoning its old model. Rather, it is building on its existing strengths. Ultimately, adding the technological domain assimilates the core leader competencies into a consistent approach that prepares the Army for the MDO fight of the next forty years. ■

Notes

1. Ryan D. McCarthy, "Note from the Secretary of the Army to the Chief of Staff of the Army" (Washington, DC: Department of Defense [DOD] 5 November 2019), accessed 25 August 2020, https://www.milsuite.mil/book/docs/DOC-823453.

2. Ryan D. McCarthy, James C. McConville, and Michael A. Grinston, "2019 Army Modernization Strategy: Investing in the Future" (Washington, DC: DOD, 2019), 3, accessed 19 August 2020, https://www.army.mil/e2/downloads/rv7/2019_army_modernization_strategy_final.pdf; Daniel A. Skog, Henrik Wimelius, and Johan Sandberg, "Digital Disruption," *Business & Information Systems Engineering* 60 (July 2018): 432, https://doi.org/10.1007/s12599-018-0550-4.

3. Artur Kluz and Mikolaj Firlej, "How to Be a Leader in the Digital Age," World Economic Forum, 10 May 2016, accessed 16 July 2020, https://www.weforum.org/agenda/2016/05/how-to-be-a-leader-in-the-digital-age/.

4. Office of the Secretary of Defense, *Summary of the 2018 National Defense Strategy of the United States of America: Sharpening the American Military's Competitive Edge* (Washington, DC: DOD, 2018), accessed 16 July 2020, https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf.

5. McCarthy, McConville, and Grinston, "2019 Army Modernization Strategy," 9–10. Figure 4 of the "Army Modernization Strategy" lists nine Army priority research areas that will support modernization efforts: "(1) Disruptive Energetics: greater than 2x energetic energy over smaller footprints; (2) RF Electronic Materials: taking advantage of optical and thermal properties of diamond materials for directed energy; (3) Quantum: optimized information transfer, sensing, and communication with unparalleled security; (4) Hypersonic Flight: aerodynamics, materials, and processes; (5) Artificial Intelligence: increasing speed and agility with which we respond to emerging threats; (6) Autonomy: maneuverability and off-road mobility of platforms; (7) Synthetic Biology: reactive and responsive skins/spectrally selective materials/antimateriel properties; (8) Material by Design: protection overmatch against future threats; and (9) Science of Additive Manufacturing: for next generation munitions for increased range and lethality."

6. Robert H. Scales Jr. and Paul K. Van Riper, "Preparing for War in the 21st Century," in *Future Warfare Anthology*, ed. Robert Scales Jr., rev. ed. (Carlisle, PA: U.S. Army War College, 2000), 23–40, accessed 16 July 2020, https://publications.armywarcollege.edu/pubs/1531.pdf.

7. Ibid.

8. McCarthy, McConville, and Grinston, "2019 Army Modernization Strategy," 8.

9. Army Doctrine Publication (ADP) 6-22, *Army Leadership and the Profession* (Washington DC: U.S. Government Publishing Office [GPO], July 2019).

10. Ibid., 1–17.

11. John M. McHugh, Raymond T. Odierno, and Raymond F. Chandler, "Army Leader Development Strategy" (Washington, DC: U.S. GPO, 2013).

12. Ibid.

13. Ibid.

14. ADP 6-22, *Army Leadership and the Profession*, 9–5.

15. Ibid., 1–16. ADP 6-22 provides details about the Army core competencies.

16. Ibid.

17. U.S. Army Maneuver Center of Excellence, "Leader Development," Maneuver Self Study Program, last modified 18 December 2018, accessed 16 April 2020, https://www.benning.army.mil/mssp/Leader%20 Developement/.

18. Ron Schmelzer, "AI Applications in Education," *Forbes* (website), 12 July 2019, accessed 11 August 2020, https://www.forbes.com/sites/cognitiveworld/2019/07/12/ai-applications-in-education/#65a50f2462a3.

19. Ryan D. McCarthy, James C. McConville, and Michael A. Grinston, "The Army People Strategy" (Washington, DC: U.S. GPO, October 2019), 7, accessed 19 August 2020, https://people.army.mil/wordpress/wp-content/uploads/2019/10/The-2020-Army-People-Strategy-Final.pdf.

20. Christian Jarrett, "Learning by Teaching Others is Extremely Effective—A New Study Tested a Key Reason Why," Research Digest, 4 May 2018, accessed 12 August 2020, https://digest.bps.org.uk/2018/05/04/learning-by-teaching-others-is-extremely-effective-a-new-study-tested-a-key-reason-why/.

21. U.S. Army Training and Doctrine Command (TRADOC) Pamphlet 525-8-2, *The U.S. Army Learning Concept for Training and Education 2020-2040* (Fort Eustis, VA: TRADOC, April 2017).

22. H. R. McMaster, foreword to Eitan Shamir, *Transforming Command: Pursuit of Mission Command* (Stanford, CA: Stanford University Press, 2011), xii.

23. McCarthy, McConville, and Grinston, "2019 Army Modernization Strategy," 8; Sari R. R. Nijssen, Gabi Schaap, and Geert P. Verheijen, "Has Your Smartphone Replaced Your Brain? Construction and Validation of the Extended Mind Questionnaire (XMQ)," *PLoS One* 13, no. 8 (31 August 2018), https://doi.org/10.1371/journal.pone.0202188.

24. Nijssen, Schaap, and Verheijen, "Has Your Smartphone Replaced Your Brain?"

25. Dean A. Nowowiejski, "The Importance of a Long-Term Self-Development Concept to Army Officers," *Military Review* 97, no. 2 (March-April 2017): 62–69.

26. Christopher G. Ingram, foreword to *Why We Write: Craft Essays on Writing War*, ed. Rand Brown and Steve Leonard (Johnston, IA: Middle West Press, 31 January 2020), 1–6.

27. Walt Piatt, "Finding a Mindful Balance," interview by Anne Alexander, Mindful, 31 October 2019, accessed 11 August 2020, https://www.mindful.org/finding-a-mindful-balance/.

28. Nathan K. Finney and Tyrell O. Mayfield, eds., "The Modern Military Profession," in *Redefining the Modern Military: The Intersection of Profession and Ethics* (Annapolis, MD: Naval Institute Press, 2018), 223.

29. Samuel P. Huntington, *The Soldier and the State: The Theory and Politics of Civil-Military Relations* (Cambridge, MA: Harvard University Press, 1957), 2.

30. Leonard Wong and Stephen J. Gerras, "Protecting, Not Just Reflecting, Society," *Military Review* (Online Exclusive, May 2018).

31. Kluz and Firlej, "How to Be a Leader in the Digital Age."

32. Lisa Alley, "U.S. Army Observes 75th Anniversary of Armored Force: Part 1 of 2," *Armor* (July-September 2015), accessed 12 August 2020, https://www.benning.army.mil/armor/eARMOR/content/issues/2015/JUL_SEP/ARMOR_July-September2015_edition.pdf; Thomas Morgan, "The Making of a General: Ike, the Tank, and the Interwar Years," Armyhistory.org, accessed 12 August 2020, https://armyhistory.org/the-making-of-a-general-ike-the-tank-and-the-interwar-years/.

33. See Army priority research areas as laid out in the "Army Modernization Strategy."

34. Kluz and Firlej, "How to Be a Leader in the Digital Age."

35. Richard Shultz, *Military Innovation in War: It Takes a Learning Organization: A Case Study of Task Force 714 in Iraq*, Joint Special Operations University [JSOU] Report 16-6 (MacDill Air Force Base, FL: JSOU Press, 2016), 37.

36. Ibid., 63–71.

37. Ori Brafman, *The Starfish and the Spider: The Unstoppable Power of Leaderless Organizations* (New York: Penguin, 2006), 29–56.

38. Karl F. "Fred" Meyer, "Uniformed Army Technical Leader White Paper," draft version 5 (2 August 2019), 2, accessed 25 August 2020, https://www.milsuite.mil/book/docs/DOC-745550.

39. Kluz and Firlej, "How to Be a Leader in the Digital Age."

40. Myron Hura et al., *Interoperability: A Continuing Challenge in Coalition Air Operations* (Santa Monica, CA: RAND Corporation, 2000), 7–15, accessed 12 August 2020, https://www.rand.org/pubs/monograph_reports/MR1235.html.

41. Brafman, *The Starfish and the Spider*, 179–96.

42. Huntington, *The Soldier and the State*, 2; Meyer, "Uniformed Army Technical Leader White Paper," 1.

43. Meyer, "Uniformed Army Technical Leader White Paper," 1.

44. Ibid.

45. Jon T. Hoffman, ed., *A History of Innovation: U.S. Army Adaptation in War and Peace* (Washington, DC: Center of Military History, 2009), 1–3.

46. Jeffrey J. Clarke, foreward to Hoffman, *A History of Innovation*, v.

47. Hoffman, *A History of Innovation*, 2.

48. McCarthy, McConville, and Grinston, "2019 Army Modernization Strategy," 2–3.

49. Raymond T. Odierno, "Leader Development and Talent Management: The Army Competitive Advantage," *Military Review* 95, no. 4 (July-August 2015): 9.

50. David Jerome, "Army Transformation: What Does It Mean?" (PhD diss., University of Arkansas, Fayetteville, AR, December 2011), accessed 12 August 2020, http://scholarworks.uark.edu/etd/176.

51. Devon L. Suits, "CSA: 'Transformational Change' Necessary to Fight, Win Future Conflicts," Army News Service, 22 January 2020, accessed 12 August 2020, https://www.army.mil/article/231878/csa_transformational_change_necessary_to_fight_win_future_conflicts.

52. McCarthy, McConville, and Grinston, "The Army People Strategy," 1–2.

53. Suits, "CSA: 'Transformational Change' Necessary"; McCarthy, McConville, and Grinston, "The Army People Strategy," 1.

54. Ruth Ann McKinney, *Reading Like a Lawyer: Time Saving Strategies for Reading Like a Law Expert*, 2nd ed. (Durham, NC: Carolina Academic Press, 2012), 11–14.

55. Clint Lalonde, "Digital Fluency vs Digital Literacy," EdTech, 22 February 2019, accessed 12 August 2020, https://edtechfactotum.com/digital-fluency-vs-digital-literacy/.

56. Ibid.

57. Ibid.

58. McCarthy, McConville, and Grinston, "The Army People Strategy," 11.

59. McCarthy, McConville, and Grinston, "The Army Modernization Strategy," 7.

60. Meyer, "Uniformed Army Technical Leader White Paper," 1.

61. Ibid.

62. McCarthy, McConville, and Grinston, "2019 Army Modernization Strategy," 8.

63. Jerome, "Army Transformation," 8.

64. Scales and Van Riper, "Preparing for War in the 21st Century," 23–40.

BRICS leaders (*from left to right*) Vladimir Putin, Narendra Modi, Dilma Rousseff, Xi Jinping, and Jacob Zuma holding hands in unity 15 November 2014 at the G20 summit in Brisbane, Australia. The BRICS acronym stands for the five major emerging national economies of Brazil, Russia, India, China, and South Africa. (Photo by Roberto Stuckert Filho, Agência Brasil)

Chinese Soft Power

Creating Anti-Access Challenges in the Indo-Pacific

Maj. Robert F. Gold, U.S. Army

In 1949, scores of Chinese Nationalist troops and civilian refugees under the leadership of Chiang Kai-shek fled to Taiwan to escape the onslaught of Chinese communist forces in mainland China. Major combat in the bloody Chinese Civil War ended; however, the lack of an armistice or a peace treaty meant that the conflict remains politically undecided. Since 1949, the Chinese Communist Party (CCP) has sought to annex Taiwan and bring the Chinese Nationalists under control of the CCP. The passing of time has not waned Chinese

A Chinese propaganda poster from 1958 that translates to "We Must Liberate Taiwan." (Graphic courtesy of Wikimedia Commons)

interest in this endeavor. This threat to Taiwan has proved to be an enduring geopolitical issue for the region.

Taiwan sits approximately 180 kilometers off the east coast of China, separated by what is called the Taiwan Strait. The island nation is also bordered by the East China Sea, the South China Sea, and the Philippine Sea. These waters play an important role in the global economy. About 80 percent of global trade by volume moves by sea, with about one-third of that traffic moving through the South China Sea alone.[1] This amount of trade in the South China Sea was estimated to be US$3.37 trillion in 2016.[2] In addition to interstate trade, the region is also rich with natural resources such as hydrocarbons that fuel the region's economies. Taiwan sits strategically along both trade routes and energy resources. This puts it in competition with China, which looks to secure the trade and resources necessary to secure hegemonic status in the region, if not globally.

The amount of trade that transits Asian waters and the region's resources are not only of interest to China, but the region is also of great interest to the United States for economic and security reasons. The United States depends heavily on trade across Asia. For instance, goods and services trade with the other twenty member states of the Asia-Pacific Economic Cooperation forum in 2018 totaled US$3.2 trillion.[3] To keep the flow of goods and services, the United States is interested in the overall security of the region. However, the U.S. presence in the region is viewed as disruptive by the Chinese government and conflicts with its interests.

There has been much discussion in the past few years about Chinese anti-access/area denial capabilities in the Indo-Pacific region. These discussions tend to center around the growing Chinese military capabilities. Buoyed by economic growth, China has spent years reforming its military and investing in various military technologies. Maps of the Indo-Pacific region typically show red fans indicating the weapon engagement zones for Chinese antiship and antiaircraft missiles. However, despite the threat these weapons may pose, military power is only one component of China's national power used to deny the United States access to the region, especially if it sought to defend strategically important Taiwan.

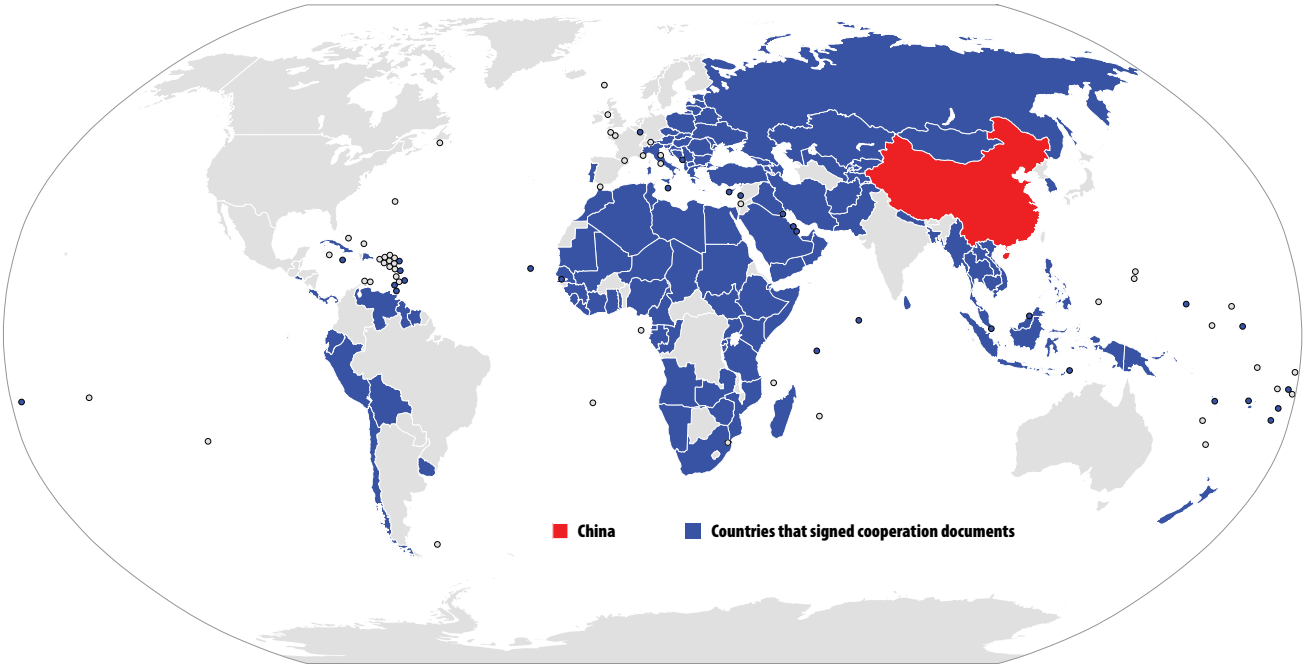
China has spent years using diplomacy, information operations, and economic investment to shape the global environment and influence its neighbors. However, despite its global outlook, China still looks across the Taiwan Strait and wishes to complete its long-term aim of annexing Taiwan. Chinese diplomatic, informational, and economic efforts are setting the stage to allow China to seize Taiwan in the future by isolating it. Additionally, these nonmilitary means of national power are working to separate the United States from its regional allies and to deny prompt access to potential crisis spots. For the U.S. military, overcoming Chinese antiship and antiaircraft missiles is only one problem in gaining access to the region. Potentially, the U.S. military may someday face a reality where access to Indo-Pacific seaports and airports is not only hampered by long-range missiles but also through Chinese political maneuvering and foreign investment. This reality will require the U.S. military, especially the Army, to be prepared to conduct an array of amphibious operations across the region's littoral areas. This will be vital to protecting U.S. interests and allies within the region.

Chinese Diplomacy in the Strategic Environment

Politically, China is very engaged globally because of its Belt and Road Initiative (BRI). The BRI was announced by Chinese President Xi Jinping during a trip to Kazakhstan in 2013 and is a global development strategy that spans dozens of countries.[4] The purpose of this strategy for China is to create new trade corridors and opportunities across the globe through land and maritime routes. Additionally, increased economic interaction with other countries allows China to increase its cultural interactions with them as well. China hopes to complete this initiative by 2049 to coincide with the one hundredth anniversary of the CCP coming into power in China. To achieve this goal, China remains politically engaged through several forms. Part of the Chinese strategy is to remain a participant in international organizations to showcase its ability to be a regional and global leader. Through these international forums, China engages in diplomatic campaigns to further its interests and delegitimize the claims of others through "lawfare," or legal engagement.

Chinese land-based trade corridors across Asia and Europe greatly benefit from the country's membership in the Shanghai Cooperation Organization (SCO), of which it is a founding member. The SCO is an intergovernmental organization that was originally founded to play a role in the regional security of Central Asia. However, its role has expanded to increase political and economic ties between member states. Original members of the alliance included China, Russia, Kyrgyzstan, Kazakhstan, and Tajikistan, but it has now grown to include India, Pakistan, and Uzbekistan. Several states hold observer status in the SCO and the organization is in dialogue with Turkey, Cambodia, Sri Lanka, Armenia, Azerbaijan, and Nepal. Political engagement by China through its participation in the SCO that has allowed China to secure its land routes for the BRI.

The SCO is only one example of Chinese participation in intergovernmental institutions. China also actively plays a part in the United Nations (UN) by holding a permanent seat on the UN Security Council and participating in UN-affiliated organizations such as the International Monetary Fund, the World Bank, and the International Criminal Court. Additionally, China also regularly deploys troops as part of UN's peacekeeping operations. Active membership in international institutions



(Figure by Owennson via Wikimedia Commons)

Belt and Road Initiative Participants as of 27 April 2019

and the global community writ large allows China to further its diplomatic engagements and show itself as a leader on important international issues. Additionally, this allows China to shape the strategic and operational environments in the Indo-Pacific by attempting to sway U.S. allies into the Chinese sphere of influence and limit American opportunities for engagement in the region.

The CCP also uses its diplomatic platform to delegitimize competitors in the Indo-Pacific as it furthers its own interests. China does this through lawfare. China claims several small islands and reefs in the Pacific, using the language of the UN Convention on the Law of the Sea (UNCLOS), placing it at odds with countries such as Japan and the Philippines. The UNCLOS establishes international law to govern the use of the world's oceans and its resources.[5] The UNCLOS grants states ability to claim sovereign rights of an exclusive economic zone that extends two hundred nautical miles from the shore, to include use of the seabed.[6] Additionally, states can claim territorial seas that may not exceed twelve nautical miles from the shore line.[7] However, according to the UNCLOS, areas that have no ability to sustain human habitation have no economic zone.[8]

China makes the claim that, historically, the Diaoyu Islands (Senkaku Islands in Japanese), a small uninhabited area near important shipping lanes in the South China Sea, belong to the country. This area offers potential oil and natural gas fields as well as abundant fishing areas.[9] Additionally, China is at odds with the Philippines over the Spratly Islands and Scarborough Shoal. These areas, like the Diaoyu Islands, are potential sources of natural resources to fuel the Chinese economy. China has used its claims to these areas as justification to occupy and build up the areas with several man-made islands. Attempting to use the language of the UNCLOS, China claims its territorial waters extend twelve miles from the shores of these artificial islands.

This claim by the Chinese government has been disputed in international court. A ruling by an international tribunal at The Hague in 2016 sided with the Philippines and determined that the Chinese government cannot claim territorial waters of areas that are primarily submerged and are within the exclusive economic zones of other states.[10] However, despite this ruling, the Chinese continue to challenge freedom of navigation operations by the U.S. Navy in the South China Sea.

China also uses lawfare to improve its strategic positioning by enforcing contract law. As part of the BRI, China, through state-owned enterprises, has invested

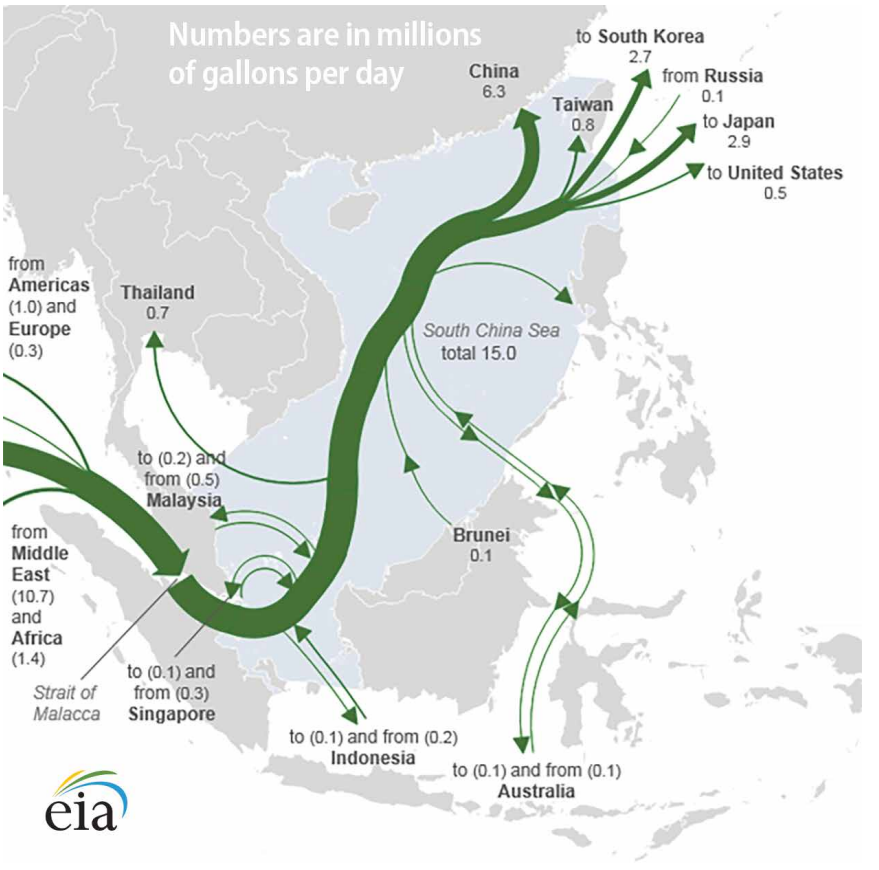
(Figure courtesy of Jackopoid, Wikimedia Commons)

Disputed Senkaku Island Chain in the East China Sea

in infrastructure or partnered with other nations on infrastructure projects. These projects include seaports, airports, and energy infrastructure. Chinese loans to poorer states in the Indo-Pacific have the potential for setting up a debt-trap if the state defaults on its loan. Sri Lanka had such an experience with the construction of the port at Hambantota, which was contracted to the China Harbor Engineering Company.[11] However, the port did not generate enough revenue to allow Sri Lanka to pay off the Chinese loans that paid for the port's construction. This was because the Sri Lankan Port

Authority had struck a deal with the Chinese to withhold container traffic at Hambantota for a time to not undermine container traffic at the Sri Lankan port of Colombo.[12] Sri Lanka ended up owing the Chinese the equivalent of US$1.3 billion with no ability to pay back Chinese-backed loans.[13] China exercised the terms of its contract with Sri Lanka and ordered that a China Merchants Group take over a majority equity holding in the port. Additionally, Sri Lanka was forced to lease fifteen thousand acres of land to the Chinese around the port for a period of ninety-nine years.[14] These actions enabled the Chinese to gain control of a seaport on the Indian Ocean.

The example of Hambantota is only one example of Chinese enforcement of its contracts with other governments. While Chinese loan behavior is not necessarily predatory by nature, China, through its state-owned enterprises, has engaged throughout the Indo-Pacific on many projects with states that are economically underdeveloped. This sets the conditions for China to have at least a minority stake (if not a majority) in infrastructure the United States might need to project forces and build combat power should China threaten Taiwan. These conditions provide the Chinese with political leverage over host nations that it can apply to deny critical locations such as seaports, airfields, and other key facilities for use by U.S. forces. Additionally, the presence of Chinese enterprises and their workers in these locations creates an operational security concern for U.S. forces staging in an area. Finally, control of infrastructure by Chinese companies would potentially limit the amount of contract support the U.S. military might be able to rely upon.



(Figure courtesy of the U.S. Energy Information Administration)

Major Crude Oil Trade Flows in the South China Sea (2016)

Chinese Influencing Activities

In addition to its diplomatic efforts, China also uses information operations to manipulate the strategic environment to degrade security partnerships with the United States in the Indo-Pacific region. China also focuses much of its activities internally as part of a carefully planned information strategy. As an authoritarian regime, the CCP tightly controls the internet and other media forms within China to carefully craft its image to the rest of the world. This has resulted in social engineering of the Chinese people and pushes a nationalist message to make its citizens more patriotic and supportive of Chinese strategic interests. For example, China makes itself appear as a victim regarding the international court ruling on its claims to islands in the South China Sea. Playing the role of victim, China claims that the U.S. Navy's freedom of navigation operations are a direct challenge to Chinese sovereignty. This has caused Chinese citizens to express outrage over social media with some calling for war.[15]

As mentioned, China's influencing activities are not limited to its own people. China also uses propaganda and social media to interfere in politics within other countries and promote Chinese cultural values.[16] China has targeted its influencing activities toward Chinese citizens in countries like Australia and New Zealand as well as others in the Indo-Pacific. Through political donorship linked to Beijing and the silencing of foreign critics, China is able to influence domestic debate in foreign countries to reexamine those countries' views on China's policies. Through these proxies, China advocates against the recognition of Taiwan, for the recognition of the Chinese economic development model, and for furthering friendly relations with China. Additionally, China also funds Confucius Institutes across the globe on university and secondary school campuses. These institutes have the goal of sharing Chinese language and culture with students and educators. However, Confucius Institutes teach a nuanced view of Chinese culture that discourages critical discourse on Chinese policies.

These influencing activities serve to isolate Taiwan from the international community and ensure it is more vulnerable to Chinese aims for reunification. In 2018, according to the U.S. Department of Defense, Taiwan lost three diplomatic partners, leaving only seventeen countries around the world to grant diplomatic recognition to Taiwan.[17] Additionally, Taiwan is still refused formal recognition by many international institutions such as the UN. Chinese efforts to influence opinion has also had the consequence of swaying some Taiwanese citizens to call for reunification with China.[18] The consequence would create a dynamic and complex operating environment if the United States were to come to the aid of Taiwan in case of a hostile annexation attempt by China.

Most importantly for the United States, Chinese influencing activities act as a wedge between the United States and its allies in the Indo-Pacific. While it undermines U.S. security partnerships, China itself does not necessarily want to become the security partner of choice in the Indo-Pacific.[19] Instead, China wants to degrade U.S. influence while China seeks its own objectives such as the annexation of Taiwan. The vast distances of the Pacific and geography make the United States reliant on security cooperation with countries throughout the region to secure American interests. The degradation of diplomatic and security relationships with long-term U.S. allies would make it harder for the United States to project power and achieve a basing strategy to balance Chinese power.

Using Economics to Shape the Environment

The growth of the Chinese economy has been remarkable since economic reform became a priority for the Chinese government in the late 1970s. As a communist country, the Chinese economy was centrally planned for decades with Chinese leadership placing emphasis on autarky, or economic self-sufficiency. The Chinese economy was agriculturally based and did not interact much with the global economy. However, through the implementation of policies aimed at economic reform, the Chinese have been able to move to a more market-based economy. But it is important to recognize that the Chinese economy, while a market economy, is still socialist.

A major difference between the Chinese economy and capitalist markets is the level of government participation in the market. The presence of state-owned enterprises within China allow the CCP to maintain a degree of control of the marketplace. State-owned enterprises only make up 3 percent of the businesses that operate in China, but these companies account for 40 percent of the business capital within China.[20] This limitation on private control of capital assets by China is different than a capitalist market economy where private control is encouraged over government intervention. However, Chinese control of the market through governmental action allows it to more directly influence the course of its own economy.

The benefit for China in loosening economic restrictions is that it has encouraged individuals and other business enterprises to partake more fully in the global marketplace.[21] China seeks to capitalize on this through the BRI, as previously mentioned. To support the BRI, China has also stood up the Asian Infrastructure Investment

Maj. Robert F. Gold, U.S. Army, is a student at the U.S. Army Command and General Staff College at Fort Leavenworth, Kansas. His most recent assignment was as an advisor team leader with the 5th Battalion, 2nd Security Force Assistance Brigade at Fort Bragg, North Carolina. He holds a master's degree in international relations from Troy University and a bachelor's degree in business management from Widener University.

Bank. This bank is a lending institution that China uses to support its infrastructure investment projects in not just the Indo-Pacific region but also in the rest of Asia, Africa, South America, and Europe. It is believed that the Chinese government is involved in the construction or operation of at least forty-two ports in thirty-four countries globally.[22] Additionally, in 2015, it was reported that the Civil Aviation Administration of China had fifty-one ongoing projects at airports tied to the BRI.[23]

China has also increased its investment in amphibious ships and force structure. The People's Liberation Army Navy maintains five Type-071 Amphibious Transport Docks with three more under construction as of 2018.[25] Also, in 2019, it was reported that the People's Liberation Army Navy had plans to construct three Type-075 Landing Helicopter Dock vessels. The CCP has also grown the oddly named People's Liberation Army Navy Marine Corps from just two brigades to seven brigades.[26]

> "Increased Chinese wealth has allowed it to invest in infrastructure projects that have increased China's sphere of influence and enabled it to posture itself around the globe."

Chinese economic reform has led to an increase in gross domestic product and net wealth that has allowed nearly one billion Chinese to be lifted out of poverty. However, despite a rise in relative wealth, China is still a large source of inexpensive labor. This has attracted foreign direct investment to China as manufacturers look to take advantage of a cheaper labor force to lower their manufacturing costs and increase their bottom line.

China has benefited greatly from its increasing wealth, which it uses to fund reform of its military and expand its sphere of influence through targeted investment. Chinese military reforms have been ongoing for many years. The purpose of these reforms is to allow the Chinese military to compete more effectively with the United States and Japan. Also, a stronger military allows China to secure its interests abroad through its own force projection.

As part of its reforms, the People's Liberation Army reduced three hundred thousand personnel from its ranks and it condensed its seven military districts to five in recent years.[24] This not only allows for more efficient command and control of Chinese forces, but it also frees up a significant portion of the Chinese military budget for procurement. Increased Chinese wealth has allowed the acquisition of newer missiles (e.g., the DF-21 "carrier killer"), fifth-generation aircraft, and ships. China now maintains two aircraft carriers, one of which it purchased from Russia (the *Liaoning*) and another it has built domestically (the *Shandong*). These aircraft carriers signal Chinese intent to extend its influence outside of Chinese territorial waters. Additionally, two divisions from the People's Liberation Army Ground Forces are reported to have been restructured as combined arms mechanized amphibious brigades.[27] Like China's aircraft carriers, an increase in amphibious capability allows China to project power abroad and indicates that it wishes to fight in an expeditionary manner like the United States.

Chinese economic reform has allowed it to do several things. Increased Chinese wealth has allowed it to invest in infrastructure projects that have increased China's sphere of influence and enabled it to posture itself around the globe. Chinese infrastructure projects at civilian seaports and airports offer potential locations for the Chinese government to project and build its own combat power in response to Chinese interests around the globe. Additionally, China has used its wealth to leverage other states in pursuit of its political objectives. One result of this is the ever-increasing isolation of the Taiwanese government as fewer states recognize it diplomatically. Rising Chinese affluence has also supported massive military reform spending by the Chinese government. This increased military spending enables the People's Liberation Army to be more competitive with the United States and serves to create a hard power instrument that can coerce Taiwan into reunification.

What This Means for the United States

Despite Chinese efforts to shape the Indo-Pacific region, it is important to note that the Chinese have not

blocked American access to the region; they have only made it more complicated. For years, the United States has postured itself to defend its interests away from the U.S. mainland. This has included forward deployed troops, as well as pre-positioned stocks of equipment. The United States is still very capable of engaging its adversaries across the globe. However, a vulnerability of the U.S. military is its reliance on existing infrastructure to support the logistical requirement of building combat power and fighting abroad.

Over the last two decades, the United States has especially been reliant upon airports and seaports to receive large quantities of personnel and equipment for reception, staging, onward movement, and integration into a theater of operations. Additionally, the U.S. military has grown more reliant on contractor support to meet its operational logistics needs. However, operations in the Indo-Pacific may require a different approach in the future that is less reliant on existent facilities and contract support. The U.S. military should be prepared for a nonpermissive environment where it does not have access to the infrastructure it needs for large combat operations. In this type of environment, the joint force may need to conduct distributed amphibious assault operations, open or construct seaports, construct aircraft landing strips, and conduct joint-logistics-over-the-shore operations to sustain operations. In the future, the United States may have to gain access to a part of the Indo-Pacific by fighting its way ashore to seize or construct the facilities it needs to fight and win.

However, while China builds its amphibious capability, the capability to conduct amphibious operations has been steadily declining in the U.S. military since the end of World War II.[28] The U.S. Navy maintains thirty-two amphibious warships, which is short of the fifty amphibious support ships needed by some estimates. Still, of these amphibious warships, only sixteen are capable of supporting operations at any one time.[29] Additionally, the U.S. Marine Corps is undergoing review of its force design to move away from large-scale amphibious assaults and sustained land combat. Instead, the Marine Corps is moving toward a force design that would allow it to operate in smaller formations and seize expeditionary advanced bases from where precision fires could be employed against an adversary.

The U.S. Army has an important role to contribute as part of a joint force in the Indo-Pacific region. It has the combat formations, precision fires, and logistics capabilities to seize terrain and conduct sustained operations. Even though amphibious capability in the Army is deficient, it is a capability that will be necessary to overcome Chinese access challenges in the Indo-Pacific region. The Army does maintain a small watercraft fleet that is manned by the Transportation Corps. This allows the operational movement and maneuver of soldiers and equipment in littoral environments. However, this fleet of vessels is too small and is more suited for use in permissive environments. Additionally, the small number of personnel who operate these craft are the only subject-matter experts on amphibious operations in the Army today. There is a significant gap in institutional knowledge to fully integrate Army forces into joint planning to conduct amphibious operations.

The Army has not always been averse to conducting amphibious operations, however. During World War II, the Army took part in fifty-eight of sixty-one amphibious operations.[30] The Army also took part in six major assault operations and supported seven other amphibious operations along with the Navy and Marine Corps. Amphibious Army engineer units also proved their worth during the Korean War by enabling UN forces to conduct shore-to-shore maneuvers in the littoral regions of the Korean peninsula. However, after the Korean War, the management of amphibious craft was transferred to the Army Transportation Corps.[31] By the mid-1960s, the last Army amphibious units were deactivated as the Army focused on fighting large Soviet tank formations in Europe. With these last units went the institutional knowledge to plan and conduct Army-led amphibious operations.

One way to restore amphibious capability in the U.S. Army would be to create a multifunctional brigade of engineers and logisticians called the Engineer Amphibious Support Brigade (EASB).[32] This brigade would combine some of the Army's watercraft fleet with engineer troops who could help establish the base camps necessary to support the joint force in the Indo-Pacific. Additionally, this type of formation would be helpful in the opening or clearing of seaports, or even in the construction of temporary port facilities, if necessary. The EASB would be capable of conducting construction and combat engineering operations to sustain and support large-scale combat.[33] In a nonpermissive environment like the one China is shaping in the Indo-Pacific, the EASB would contribute

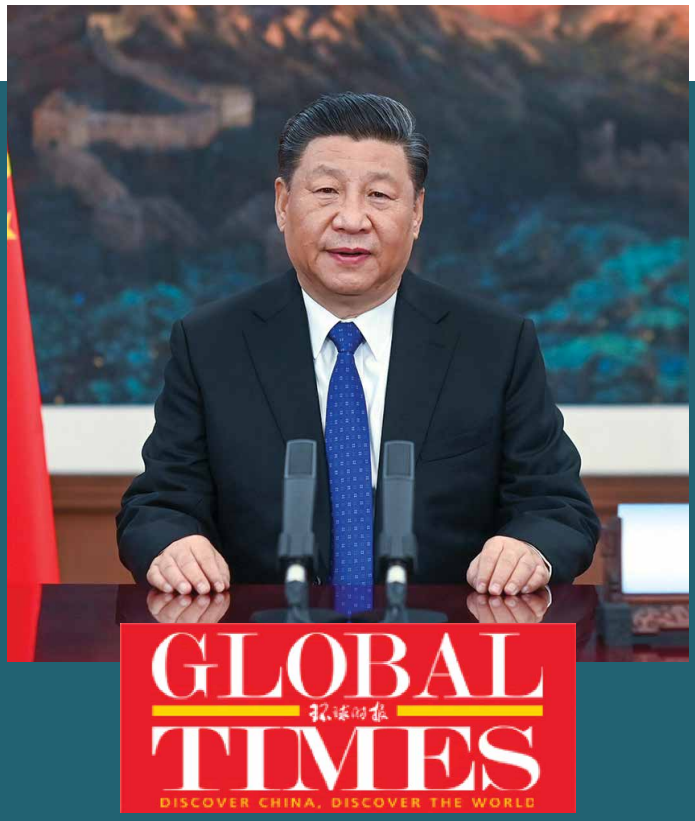
to gaining U.S. forces access to the region in the event of a crisis, such as a war between Taiwan and China.

For the Army, forming a new type of organization to improve its ability to conduct amphibious operations is just one step. Training and education would be necessary to better prepare Army personnel to conduct amphibious operations in the world's littoral regions. To accomplish this the Army should coordinate with the U.S. Navy and U.S. Marine Corps to conduct amphibious joint training and exercises. This would allow the sharing of lessons learned, build the institutional knowledge for soldiers regarding the planning and conduct of amphibious operations, and streamline integration of the Army into future joint amphibious operations.[34] Additionally, the Army could work with the Navy and Marine Corps to invest in new ship-to-shore connectors to allow forces to be better protected in nonpermissive environments.

Conclusion

China has been adept at using its instruments of national power to manipulate the strategic environment in the Indo-Pacific, especially regarding Taiwan. Chinese diplomatic, informational, and economic efforts have allowed it to increasingly isolate Taiwan from the rest of the international community. Chinese efforts have been aimed at swaying allies away from the United States and preventing U.S. access to key infrastructure in the region. This would hamper a U.S. response to a crisis in the region such as a Chinese invasion of Taiwan. China has also used its increasing wealth to fund military reform and modernization efforts. A more modern and efficient People's Liberation Army allows the Chinese to back up their soft power gains with coercive hard power. It has also better enabled the Chinese to invade and annex Taiwan.

To overcome these challenges, the United States will need to be prepared to conduct amphibious operations and open critical infrastructure needed to sustain operations in the Indo-Pacific region. Being comfortable operating in littoral regions will allow the U.S. military to move and maneuver large numbers of troops and equipment, whether from ship-to-shore, or shore-to-shore. While the United States already has robust amphibious capability compared to most nations, it is also a capability that



"China has a huge array of multimedia tools to carry out 'Information Operations.' It leverages online operations, audio visual productions, and of course the traditional media of newspapers and television news channels. It reportedly controls more than three thousand public television channels in the world, over one hundred and fifty pay TV channels, around twenty-five hundred radio stations, about two thousand newspapers and ten thousand magazines, and more than three million internet sites. The biggest and by far the most important asset in this propaganda machinery is the *Global Times*. It is a tabloid that has been appropriated by the Chinese Communist Party (CCP) and now attempts to pass off as a daily newspaper. Earlier it came out only in the Chinese language for internal consumption; in 2009 it started publication in English to cater for 'international readership.'"

Snippet of article courtesy of "The Global Times: Obnoxious Headquarter of Chinese Information Warfare," by Col. (Retired) Jaibans Singh, *NewsBharati*, 23 September 2020, https://www.newsbharati.com/Encyc/2020/9/23/Information-Global-Times-.html.

Photo: Chinese President Xi Jinping delivers a speech 18 May 2020 during the 73rd World Health Assembly in Beijing. (Photo by Li Xueren, Xinhua News Agency)

has been declining for several years. For the Army, the capability is almost nonexistent.

It will be necessary for the Army to invest resources into growing its ability to conduct amphibious operations. While they are very capable organizations, the Navy and Marine Corps cannot shoulder the burden of operations in the Indo-Pacific alone. The Army brings significant capability to the joint force in the Indo-Pacific, but it must get its forces there first. One step the Army can take is to look at creating specific organizations, such as the EASB. This would enable the Army to create the basing and infrastructure the joint force needs to sustain combat operations in the region. Additionally, the Army should work with the Navy and Marine Corps to build the institutional knowledge to conduct complex amphibious operations. These actions would allow the Army to better integrate with the joint force to overcome Chinese efforts to deny the United States access to the Indo-Pacific. ■

Notes

1. "How Much Trade Transits the South China Sea?," China Power, accessed 30 April 2020, https://chinapower.csis.org/much-trade-transits-south-china-sea/.
2. Ibid.
3. "U.S.-APEC Bilaterial Trade and Investment," Office of the United States Trade Representative, last updated 24 October 2019, accessed 30 April 2020, https://ustr.gov/countries-regions/japan-korea-apec/apec/us-apec-trade-facts.
4. Ankit Panda, "How Old Is China's Belt and Road Initiative Exactly?," The Diplomat, 11 February 2019, accessed 31 August 2020, https://thediplomat.com/2019/02/how-old-is-chinas-belt-and-road-initiative-exactly/.
5. "United Nations Convention on the Law of the Sea of 10 December 1982," United Nations Division for Ocean Affairs and the Law of the Sea, 11 February 2020, accessed 31 August 2020, https://www.un.org/Depts/los/convention_agreements/convention_overview_convention.htm.
6. Ibid.
7. Ibid.
8. Ibid.
9. "How Uninhabited Islands Soured China-Japan Ties," BBC, 10 November 2014, accessed 1 March 2020, https://www.bbc.com/news/world-asia-pacific-11341139.
10. Jane Perlez, "Tribunal Rejects Beijing's Claims in South China Sea," *New York Times* (website), 12 July 2016, accessed 31 August 2020, https://www.nytimes.com/2016/07/13/world/asia/south-china-sea-hague-ruling-philippines.html.
11. Hong Zhang, "Beyond 'Debt-Trap Diplomacy': The Dissemination of PRC State Capitalism," The Jamestown Foundation, 5 January 2019, accessed 31 August 2020, https://jamestown.org/program/beyond-debt-trap-diplomacy-the-dissemination-of-prc-state-capitalism/.
12. Ibid.
13. Ibid.
14. Ibid.
15. P. W. Singer and Emerson T. Brooking, *LikeWar: The Weaponization of Social Media* (New York: Houghton Mifflin Harcourt, 2018).
16. Amy E. Searight, *Chinese Influence Activities with U.S. Allies and Partners in Southeast Asia* (Washington, DC: Center for Strategic and International Studies, 6 April 2018), accessed 1 May 2020, https://www.csis.org/analysis/chinese-influence-activities-us-allies-and-partners-southeast-asia.
17. *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2019* (Washington, DC: Office of the Secretary of Defense, 2019), accessed 1 May 2020, https://media.defense.gov/2019/May/02/2002127082/-1/-1/1/2019_CHINA_MILITARY_POWER_REPORT.pdf.
18. Ibid.
19. Searight, *Chinese Influence Activities with U.S. Allies and Partners in Southeast Asia*.
20. Melanie Manion, "Politics in China," in *Comparative Politics Today: A World View*, ed. G. Bingham Powell et al., vol. 12 (New York: Pearson, 2018), 340–76.
21. Ibid.
22. Shaun Turton, "China's Belt and Road Ports Raise Red Flags over Military Plans," Nikkei Asian Review, 23 July 2019, accessed 2 May 2020, https://asia.nikkei.com/Spotlight/Asia-Insight/China-s-Belt-and-Road-ports-raise-red-flags-over-military-plans.
23. "China's Belt and Road Initiative and Aviation," Centre for Asia Pacific Aviation, 26 July 2018, accessed 2 May 2020, https://centreforaviation.com/analysis/airline-leader/chinas-belt-and-road-initiative-and-aviation-427350.
24. Joel Wuthnow and Phillip C. Saunders, "Chinese Military Reforms in the Age of Xi Jinping: Drivers, Challenges, and Implications," Chinese Strategic Perspectives No. 10 (Washington, DC: National Defense University Press, March 2017), accessed 18 August 2020, http://ndupress.ndu.edu/Portals/68/Documents/stratperspective/china/ChinaPerspectives-10.pdf?ver=2017-03-21-152018-430.
25. *Annual Report to Congress*.
26. Ibid., 35.
27. Ibid., 86.
28. Brett A. Friedman, "Ensuring Access in a Maritime World," *Proceedings* 145, no. 4/1394 (April 2019), accessed 2 May 2020, https://www.usni.org/magazines/proceedings/2019/april/ensuring-access-maritime-world.
29. Ibid.
30. Robert F. Gold, "The Engineer Amphibious Support Brigade: A Concept for Future Operations Rooted in the Past," *Engineer* 50 (January-April 2020): 30–33, accessed 2 May 2020, https://home.army.mil/wood/application/files/9415/8680/1624/EN_Jan-Apr_2020_reduced_size.pdf.
31. Ibid., 31.
32. Ibid.
33. Ibid.
34. Ibid., 33.

2021 General William E. DePuy

Special Topics Writing Competition

This year's theme: "Contiguous and noncontiguous operations: pivoting to U.S. Indo-Pacific Command—the Army's role in protecting interests against adversaries who can contest the U.S. joint force in all domains."

Articles will be comparatively judged by a panel of senior Army leaders on how well they have clearly identified issues requiring solutions relevant to the Army in general or to a significant portion of the Army; how effectively detailed and feasible the solutions to the identified problem are; and the level of writing excellence achieved. Writing must be logically developed and well organized, demonstrate professional-level grammar and usage, provide original insights, and be thoroughly researched as manifest in pertinent sources.

Contest opens 1 January 2021 and closes 12 July 2021

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, please visit https://www.armyupress.army.mil/DePuy-Writing-Competition/.

Sgt. Dylan Weiss and Spc. Anthony Roller observe a simulated enemy compound 15 September 2020 during Noble Partner 20 at Vaziani Training Area, Georgia. (Photo by Spc. Isaiah Matthews, U.S. Army)

Sgt. 1st Class Lisa Capocci, a U.S. Army Reserve drill sergeant from the 98th Training Division, explains something to a trainee 18 November 2019 during the Pick-Up Day process at Fort Jackson, South Carolina. (Photo by Maj. Michelle Lunato, U.S. Army Reserve)

Discipline as a Vital Tool to Maintain the Army Profession

Maj. Michael Petrusic, U.S. Army

During the past decade, discipline within the Armed Forces and the structures used to maintain that discipline have been scrutinized at a level not seen since the development of the modern Uniform Code of Military Justice following World War II.[1] From the criticism of the military's handling of sexual assault cases and senior leader misconduct to the high-profile courts-martial of Chelsea Manning and

Bowe Bergdahl and to the recent allegations of serious disciplinary lapses within the Navy's special operations community, service member misconduct and the manner in which the Armed Forces investigate and address that misconduct have been critically examined by Congress, the media, and the public.[2] The commander of the Naval Special Warfare Command recently echoed criticism of disciplinary lapses in his own organization, stating that the "root of our problem begins with members who fail to correct this behavior within their sphere of leadership," and such failure "erodes the foundation of trust we have earned with our leaders and the American people."[3]

Army leaders often rightly emphasize proper investigation and disposition of misconduct as critical to ensuring good order and discipline within the force. But the criticism noted above suggests a deeper purpose to getting discipline right: enforcing high ethical and behavioral standards is essential to maintain the public trust and to protect the Army's continued status as a profession and the tremendous deference that status provides. If Army leaders inadequately police misconduct within the force by failing to consider and exercise their range of disciplinary options when appropriate, they will create a perception that the Army is unable or unwilling to address misconduct within the ranks. That perception will both contribute to a culture of impunity regarding misconduct and erode the public's trust in the Army's disciplinary systems and its ability to self-police. This will inevitably result in the breakdown of the Army profession and the relative independence with which Army leaders have managed the institution for decades.

This article's discussion of the military disciplinary system's unique nature and examination into whether the full range of options in the system is underutilized in the Army will lead to an analysis of whether failure to police misconduct within Army ranks is a lapse of leadership that threatens the Army's standing as a profession. It will include an evaluation of the repercussions if the public loses faith in the Army's ability to self-police the force and argue that leaders must fully leverage the range of disciplinary options available to them while preserving the legitimacy of the system and respecting crucial soldier rights.

Discipline and Organizational Legitimacy

The very nature of the military disciplinary system is what makes it an indicator of the Army's legitimacy as a profession rather than just a commander's tool to maintain good order and discipline. The commanders' central role in all aspects of this system distinguishes the Army profession from any other government entity, corporation, or organization in the United States. In none of these other organizations does leadership have the sole discretion to exercise a full range of disciplinary processes in response to member misconduct. But Army commanders have a suite of options available to them in responding to soldier misconduct, ranging from taking no action on the low end to recommending or referring a case for court-martial on the high end.[4] In between these poles are a variety of administrative and nonjudicial options such as bars to reenlistment, administrative separations and officer eliminations, and nonjudicial punishment under Article 15 of the Uniform Code of Military Justice.[5] Although certain serious offenses must be elevated to higher levels of command for disposition and can only be adjudicated at specified types of courts-martial, commanders otherwise have significant freedom to exercise independent judgment and initiate action from across the range of disciplinary options.[6]

This high level of discretion, placed in the hands of select officers, inextricably links the Army's disciplinary system to the legitimacy of the command and the profession. Because Army commanders have exclusive control over the initiation of the disciplinary processes, issues of misconduct and the responses to them will inevitably reflect on the command. A corporation can take some actions in response to employee misconduct but is typically limited to, at the most, firing employees. And a mayor or governor can take some limited actions to punish bad actors in the governments they run but must rely on independent prosecutors and attorneys general to decide to prosecute individuals criminally. Leaders in these organizations therefore have

Maj. Michael Petrusic, U.S. Army, is a judge advocate for the 1st Special Forces Group (Airborne) at Joint Base Lewis-McChord, Washington. He holds a BA from the University of Virginia, a JD from the University of North Carolina School of Law, and a LLM from the Judge Advocate General's Legal Center and School. He has previously served in the 82d Airborne Division, 16th Military Police Brigade, and as an associate professor at the Judge Advocate General's Legal Center and School.

fairly limited discretion in disciplinary matters. But the people have entrusted the Army to police itself, and commanders have been empowered to exercise the full range of discipline when soldiers commit misconduct. Consequently, any failure to adhere to and enforce ethical and behavioral standards is seen as not just a failure of the soldier but reflects negatively on the legitimacy of the whole organization.

Are Commanders Underutilizing Their Disciplinary Options?

Considering the diverse range of disciplinary options available to commanders, and their sole discretion over those options, many would expect the answer to this question to be a clear "no." With military law's fundamental purposes "to promote justice, to assist in maintaining good order and discipline in the Armed Forces, [and] to promote efficiency and effectiveness in the military establishment," one would anticipate commanders would use these tools to their utmost potential.[7] But notwithstanding the range of options available and the critical purposes of maintaining discipline, the commander can experience significant tensions in fully utilizing the disciplinary system.

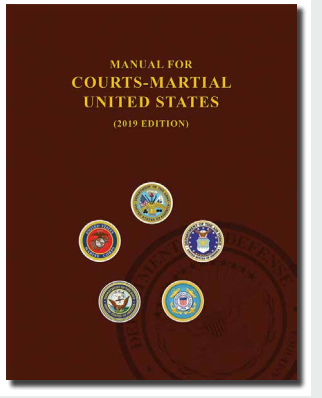
First, many commanders may determine that the Army's disciplinary system consumes too much time and too many unit resources to be fully exercised. Courts-martial, the most serious of the disposition options, can take a significant period of time to complete due to discovery and evidence production, motions and other pretrial practice, and scheduling conflicts among counsel and the military judge.[8] And throughout this time, the commander will be required to support the proceedings with bailiffs, escorts, panel members, witnesses, and funding.[9] Administrative separations, which require processing through various offices, notice periods, and boards for soldiers with six years of service, or where an other than honorable characterization of service upon discharge may result, can also be time and labor intensive.[10] These are significant time and resource commitments for units constantly asked to achieve more with less.

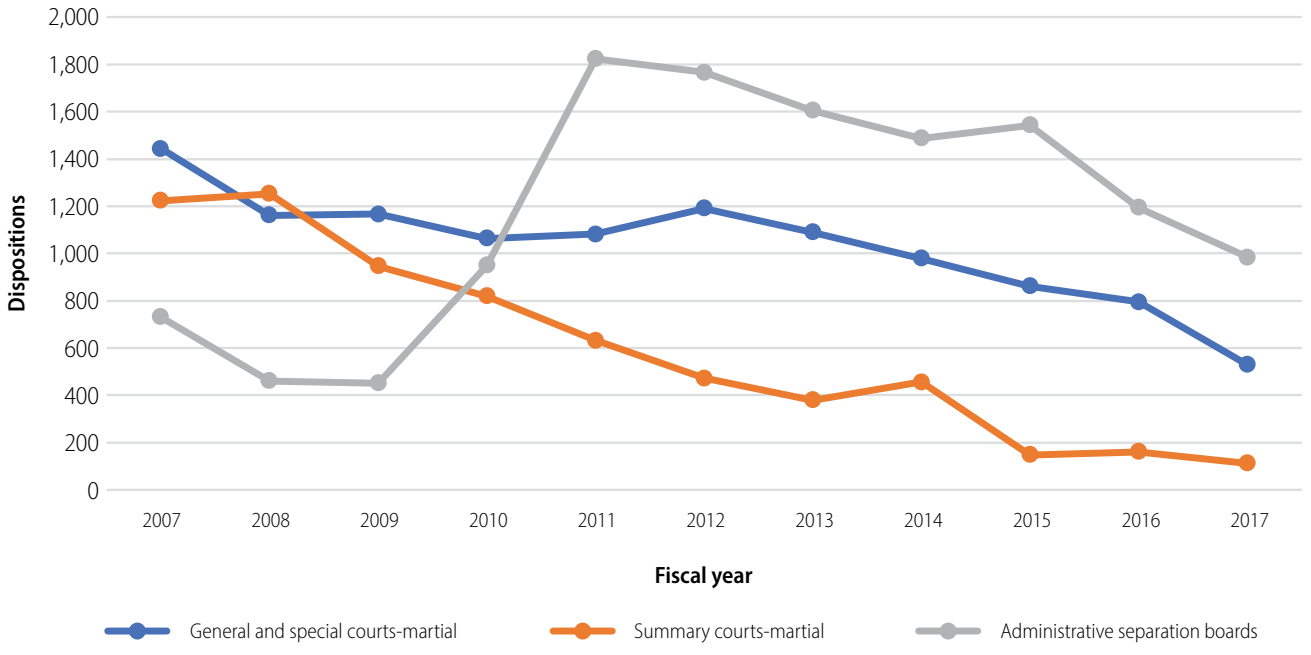
The drain on time and resources for these processes presents even greater challenges during periods of high operational tempo where commanders may need all hands available, or in the cases of soldiers with specialized skills highly valued by the organization. Commanders may simply have little patience for initiating burdensome disciplinary processes when there are more important real-world priorities or if they want to keep an "all-star" soldier. Maj. Gen. James Mingus, 82nd Airborne Division commander, cautioned against this dynamic during the 2019 Profession of Arms Forum at Fort Leavenworth, Kansas. He noted that leaders should not allow their desire for soldier competence and commitment to overtake the need to ensure soldier character, as doing so risks degrading the profession of arms.[11]

Beyond these practical challenges in initiating disciplinary proceedings, many commanders may also feel conflict between the need to address misconduct or ethical lapses within their formation and the Army's ethos of taking care of soldiers. Doctrine tells commanders that the "nation entrusts the Army leader with its most precious commodity, its sons and daughters," and cautions them to "keep the well-being of their subordinates and their families in mind" and "connect at a personal level with their subordinates."[12] This mandate to keep in mind the interests of soldiers and form deep connections with them puts commanders in a tough situation when they are called on to consider initiating proceedings that could result in a soldier's separation, loss of pay, or even imprisonment. This tension can be understandably difficult for many commanders to navigate.

So, with these tensions in mind, is the Army underutilizing its disciplinary toolkit? Former Secretary of Defense James Mattis certainly suspected this was

The law requires the president of the United States, acting as commander in chief of the Armed Forces, to write rules and regulations to implement military law. The president does so by issuing an executive order promulgating the *Manual for Courts-Martial (MCM) United States*. The *MCM* details rules and regulations for military courts-martial and provides information for each military offense listed in the punitive articles of the Uniform Code of Military Justice. The 2019 edition updates pertinent amendments and executive orders from 1984 to 2019. To view this manual, visit https://jsc.defense.gov/Portals/99/Documents/2019%20MCM%20(Final)%20(20190108).pdf?ver=2019-01-11-115724-610.





(Figure by author)

Figure 1. Offender Dispositions (Courts-Martial and Separations)

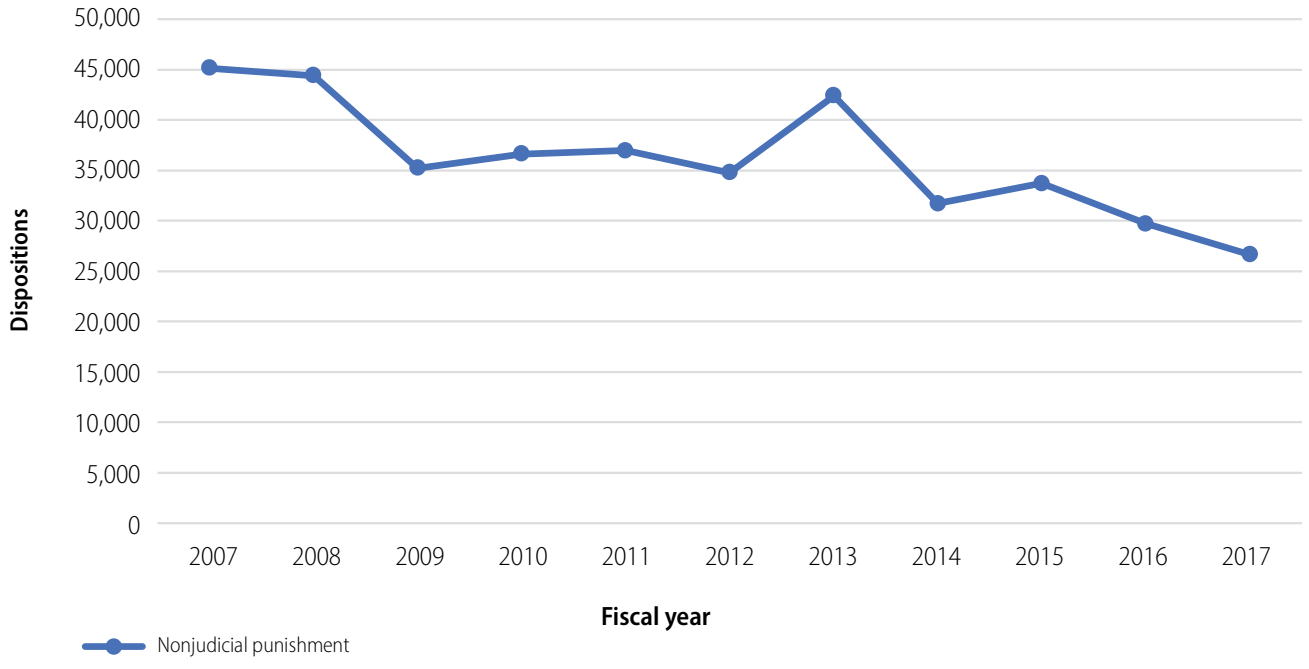
the case. In a 2018 memorandum to all service secretaries and chiefs and all combatant commanders, he stated that it "is a commander's duty to use [the military justice system]. ... Leaders must be willing to choose the harder right over the easier wrong. Administrative actions should not be the default method to address illicit conduct simply because it is less burdensome than the military justice system."[13] He further stated bluntly, "Time, inconvenience, or administrative burdens are no excuse for allowing substandard conduct to persist."[14]

Beyond the observations of Mattis, data on the utilization of various disciplinary actions over the past decade also indicate a significant decline in their use. Analyzing the numbers of courts-martial, administrative separation boards, and Article 15 proceedings in the Army from fiscal year (FY) 2007 to FY 2017, reveals a marked decline over time.[15]

Figures 1 and 2 (on page 116) indicate that other than administrative separations, the exercise of all of these disciplinary options within the Army decreased dramatically from FY 2007 to FY 2017. And although there were slightly more administrative separation boards in FY 2017 than there were in FY 2007, the 984 boards in FY 2017 were well below the 1,823 boards in FY 2011. The court-martial, the most time and resource-intensive option in the commander's disciplinary toolkit, saw the most dramatic decrease with the 2,667 total courts-martial of all types in FY 2007 plummeting to 641 courts-martial of all types in FY 2017.

Although these declines appear dramatic, getting a full context requires also considering offender rates in the Army for various types of offenses over the same period. That is, have the numbers of disciplinary dispositions in the Army fallen because commanders are using them less, or simply because the numbers of alleged offenders within the Army have also fallen? Figure 3 (on page 117) shows the trends in offender rates for various types of offenses over time and helps us paint a fuller picture.[16]

This figure shows that the number of alleged offenders for various categories of offenses has also fallen from FY 2007 to FY 2017. However, comparing the decline in types of offenses against the dispositions typically appropriate for those offenses shows the decrease in the exercise of disciplinary options has been significantly sharper than the decline in alleged offenders. For example, while the misdemeanor offender rate decreased 36.7 percent, the number of Article 15 proceedings executed in the Army over the same period



(Figure by author)

Figure 2. Offender Dispositions (Nonjudicial Punishment)

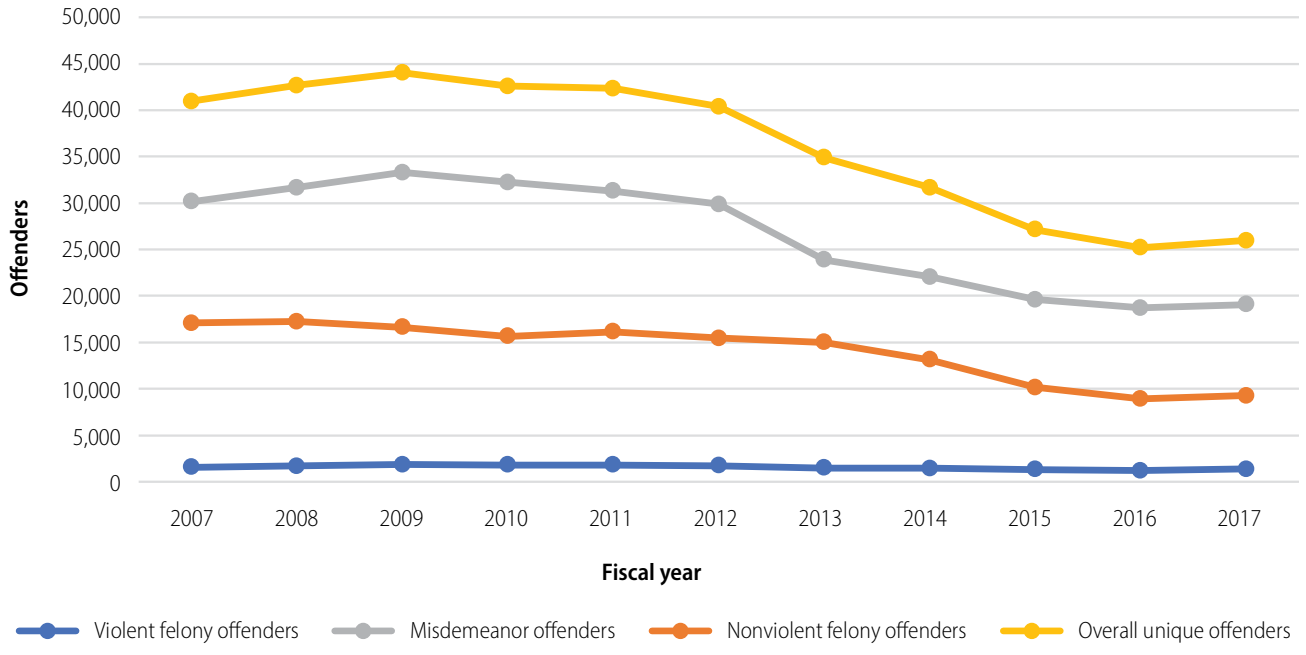
decreased by a steeper 41 percent. Nonviolent felony offenders decreased by 45.8 percent from FY 2007 to FY 2017, while the number of summary courts-martial plummeted 90.8 percent. And finally, the 63.4 percent decline in the numbers of special and general courts-martial was significantly sharper than the 45.8 percent decline in nonviolent felony offenders and the 14.9 percent decline in violent felony offenders.

This comparison of figures shows that the decrease in the number of alleged offenders alone does not fully account for the significant decline in commanders' exercise of disciplinary options over the past decade. Of course, other factors that make pursuing disciplinary action less feasible could certainly account for some of this decline, such as more instances of false reporting, an increase in the number of difficult cases, or a decline in the quality of law enforcement investigations. However, the concerns expressed by numerous senior military leaders over the past few years, including those of Mattis and commanders within the special operations community, suggest commanders are becoming more hesitant to initiate disciplinary action in their formations.

Self-Policing as an Element of the Profession and a Function of Command

If commanders are growing reluctant to utilize their disciplinary options when appropriate, this trend will present a significant threat to the health of the Army profession. Many soldiers may hear the term "Army profession" without fully appreciating its meaning and the extent to which it is essential to the Army's culture as a fighting force. The ability to function as a profession distinguishes the Army from the typical government bureaucracy prevalent in the remainder of the executive branch. It is what has given the Army the ability to largely regulate itself for centuries within the broad left and right limits imposed by civilian leadership.

To understand why the Army is allowed such deference, one must first look at the essential characteristics of a profession. Army Doctrine Publication 6-22, *Army Leadership and the Profession*, lays out these characteristics: (1) professions "provide a vital service to society"; (2) require "expertise and skill developed through years of training, education, and experience"; (3) "establish standards of practice and certify that their members are qualified to



(Figure by author)

Figure 3. Active Duty Offenders

serve"; (4) "live by an ethic with both legal and moral foundations"; and (5) "self-police."[17] The last two characteristics in particular distinguish the military profession from other governmental entities. Doctrine further explains that because of professions' adherence to these characteristics, "society trusts professions and grants them autonomy and discretion with prudent, balanced oversight or external controls."[18] In short, the people give the Army significant autonomy considering the power it wields only to the extent that it maintains the people's "trust and confidence in the Army as an ethical profession."[19]

Due to the importance of maintaining this trust, doctrine gives commanders the responsibility and the obligation to take actions that place the needs of the Army as a whole above those of the commander or the unit.[20] It makes commanders stewards of the profession.[21] Commanders have many means at their disposal to effectively steward the profession, including the disciplinary system. The various options that make up this system are the commander's tools for self-policing, allowing him or her to "prevent misconduct, enforce the standards of the profession, and take action to stop unethical practices" impartially and consistently.[22] These tools are so critical that doctrine states standards and discipline "are the point of departure for leading Army organizations."[23]

When the commander neglects this obligation to police standards and discipline in the force, he or she risks the health of both the unit and the profession. The Army will not remain a profession as that term is defined above through words in a doctrine publication alone. Those words must be backed up with conduct. The Army profession is accountable to its client, and its client, "in this case the American people—gets to determine if an institution is treated as a venerated profession meriting the autonomy necessary to do its expert work."[24] If the client determines that elements of the force are not operating within established ethical and legal standards and that the Army is not policing these failures, only the essential characteristics of all other government bureaucracies will be left.[25] At that point, the Army will no longer warrant its status as a profession, and its client will begin to handle it accordingly.

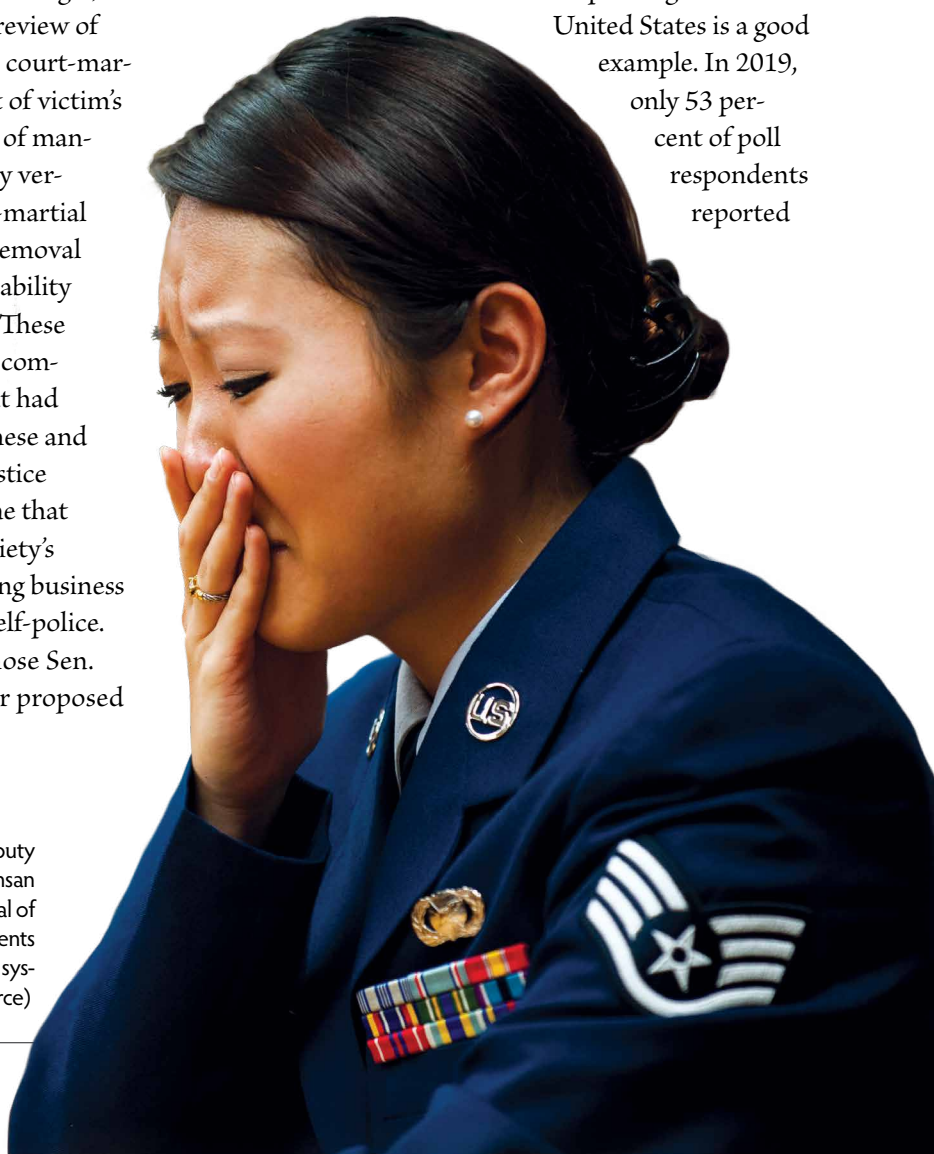
So why should anyone be concerned about this risk? Because if the client loses faith in the Army's ability or willingness to police itself, the client, through increased external oversight and regulation, will take

this privilege away from the Army.[26] An example of this dynamic is Congress's increased oversight and regulation of the Armed Forces stemming from the scrutiny of sexual assault in the military over the past decade. The issue of handling sexual harassment and sexual assault allegations has more recently become a widespread concern throughout society, including in corporate America, Hollywood, colleges and universities, and Congress itself. But the Armed Forces have been criticized on this front for several years now.

As a result of that criticism, there has been a string of changes in the functioning of the military justice system over most of the past decade. For example, in the National Defense Authorization Act for FY 2012, Congress directed that the Armed Forces institute an expedited transfer process for alleged sexual assault victims, allowing those soldiers to request a transfer to another installation following a sexual assault report.[27] Then in FY 2014's National Defense Authorization Act, Congress instituted a number of significant changes, including a process for higher commander review of decisions not to refer sexual assault cases to court-martial, the implementation of an expansive set of victim's rights and protections, the implementation of mandatory discharges or dismissals upon a guilty verdict and required referral to general courts-martial for certain sexual assault offenses, and the removal of convening authorities' largely unfettered ability to grant clemency following a conviction.[28] These changes reflected congressional doubt as to commanders' ability to administer a process that had been their exclusive domain for decades. These and other changes have resulted in a military justice system fundamentally different than the one that existed in 2010. They all reflect, in part, society's displeasure with the way the Army was doing business and a lack of faith in the Army's ability to self-police.

These changes pale in comparison to those Sen. Kirsten Gillibrand has advocated for in her proposed Military Justice Improvement Act. That bill would altogether remove the commander from the court-martial referral decision for serious offenses and instead hand that responsibility over to judge advocates.[29] She has pushed this legislation forward for years due to "the military's failure to combat sexual assault in the ranks or provide a military justice system that holds assailants accountable."[30] Filibusters from senators who support retaining commanders in the referral decision are the only thing that has prevented the legislation from passing.[31] The fact that the Senate is on the cusp of stripping commanders of one of their most fundamental disciplinary functions should serve as a warning of the repercussions the Army faces if the public loses faith in its ability to police itself.

Beyond the risk of additional regulation and interference with military functions and operations, one must also consider other potential issues that follow from a profession losing the client's faith. The current crisis in policing in the United States is a good example. In 2019, only 53 percent of poll respondents reported



First Lt. Son Lee, 8th Fighter Wing Public Affairs deputy chief, testifies during a mock trial 16 April 2014 at Kunsan Air Base, South Korea. The Wolf Pack put on a mock trial of a sexual assault case for First Term Airman Center students to provide a realistic portrayal of the military justice system. (Photo by Staff Sgt. Clayton Lenhardt, U.S. Air Force)

The Trial Defense Service provides counsel for the accused 7 August 2018 during the 167th Theater Sustainment Command's 4th annual mock court-martial at the Calhoun County Courthouse in Anniston, Alabama. (Photo by Staff Sgt. Katherine Dowd, Army National Guard)

they had a great deal or quite a lot of confidence in the police, as compared to 73 percent of poll respondents reporting a great deal or quite a lot of confidence in the military.[32] Large portions of the public have lost faith in police departments' ability to abide by rules and regulate their own due to numerous highly publicized allegations of police misconduct, particularly against minority communities. This erosion of trust has resulted in increased suspicion and external regulation of the police, including greater use of body cameras and citizen review boards. It has also caused, in some cases, recruiting shortfalls (particularly in minority communities), reluctance to work with police departments, and open hostility toward officers.[33] These are consequences the Army should seek to avoid.

Maintaining the Public Trust and the Profession

Fortunately, maintaining the profession and avoiding these repercussions is not complicated, though it does require some hard work and patience. The two essential characteristics of a profession discussed above that distinguish it from a mere bureaucracy are operating within established ethical and legal standards, and self-policing. These characteristics are linked to the disciplinary system, and commanders must be willing to exercise this system when appropriate. As Mattis noted, the commander has a duty to do so where the circumstances warrant to address substandard conduct, regardless of the "[t]ime, inconvenience, or administrative burdens" involved.[34]

Commanders can mitigate some of the burdens of going through these processes by establishing standard operating procedures, and planning and executing them like other operations. Commanders can, for example, establish a clear task organization and clearly assign responsibilities to ensure things like medical processing and escort duties are smoothly executed. These actions will not eliminate the time and resource commitments required, but they will help the command anticipate and mitigate their effects. Notably, the Army's Judge Advocate General's Corps recently implemented a military justice redesign that promises to increase efficiency in the processing of disciplinary actions on the government side and has increased

resourcing for defense counsel to give them more time to advocate for their clients.[35] Although going through the various aspects of the disciplinary process can be time and resource intensive, appropriately exercising the processes is the best means available to maintain good order and discipline and protect the profession, while also ensuring that soldiers' rights are respected.

In exercising these processes, commanders must understand and embrace the secretary of defense's "Non-Binding Disposition Guidance," which provides factors that convening authorities and commanders should consider when exercising their disciplinary function.[36] These factors are designed to "promote regularity without regimentation," "encourage consistency without sacrificing necessary flexibility," and avoid mandating any particular decision or result.[37] These suggested factors commanders should consider, among others, include the effect of the alleged misconduct on the command; the nature and seriousness of the offense; the soldier's culpability; the views of the alleged victim and the extent of harm caused to the alleged victim; whether the evidence is likely to obtain a conviction; and the appropriateness of administrative action.[38] Full consideration of these factors will help commanders to "exercise their authority in a reasoned and structured manner, consistent with the principle of fair and even-handed administration of the law."[39]

Finally, commanders can maintain the health of the profession by ensuring that when making disposition decisions, the disciplinary processes are applied fairly. In addition to knowing when to utilize their disciplinary options, commanders maintain trust by having the judgment and personal courage to refrain from exercising their disciplinary authority when such restraint is warranted. Commanders must resist societal and institutional pressure to overcorrect and to act where the circumstances do not justify doing so. Taking no action in a case is specifically listed as a disposition option for the commander in the Rules for Courts-Martial for a vital reason: some cases of alleged misconduct simply do not warrant disciplinary action.[40] This can be challenging to do when the profession is under such intense scrutiny. But by using the "Non-Binding Disposition Guidance," commanders can ensure they apply a uniform and justifiable process to evaluate all allegations of misconduct on their own merit. Furthermore, commanders must always remember that allegations are simply allegations until adjudicated and that the results of disciplinary processes must be respected. Treating accused soldiers fairly, and consistently protecting the process and outcome of disciplinary proceedings can help to avoid issues that will inevitably cause delay and extra work during disciplinary proceedings. And more importantly, these are just the right things to do.

By following these basic guidelines, commanders can help ensure that the Army effectively and fairly polices itself and addresses misconduct within the ranks. Doing so is vital to the Army continuing to enjoy the privileged status of a profession and the resulting trust placed in it by the American people and its civilian leadership. As the commanding general of the U.S. Special Operations Command stated following a spate of misconduct in those forces, this trust is "paramount and must never be compromised."[41] Compromising the trust placed in the Army will eventually render the Army just another government bureaucracy, and invite a level of oversight and external regulation previously unseen by the force. It is up to Army leaders to ensure this does not happen. ■

The author thanks Dr. Jack Kem of the U.S. Army Command and General Staff College for his suggestions and comments on drafts of this article.

Notes

1. Mary J. Bradley and Charles J. Strong, preface to *Military Law Review* 165 (September 2000): viii.

2. Kate Andrews, "Navy SEAL Pleads Guilty in Case of Strangled Green Beret," *New York Times* (website), 16 May 2019, accessed 14 August 2020, https://www.nytimes.com/2019/05/16/world/africa/navy-seal-logan-melgar-death.html; Dan Lamothe, "Navy SEALs Kicked Out of Iraq for Drinking Alcohol after Reported Sexual Assault, Officials Say," *Washington Post* (website), 25 July 2019, accessed 14 August 2020, https://www.washingtonpost.com/national-security/2019/07/25/navy-seal-platoon-kicked-out-iraq-drinking-alcohol-while-deployed-officials-say/; Geoff Ziezulewicz, "Internal Report Exposes Cocaine Abuse, Lax Testing, Inside SEAL Team 10," *Navy Times* (website), 22 July 2019, accessed 14 August 2020, https://www.navytimes.com/news/your-navy/2019/07/22/internal-report-exposes-cocaine-abuse-lax-testing-inside-seal-team-10/.

3. Commander, Naval Special Warfare Command, memorandum to Major Commanders, Naval Special Warfare, "Guidance from the Commander," 20 August 2019, accessed 14 August 2020, http://cdn.cnn.com/cnn/2019/images/08/23/radm.green.guidance.directive.pdf.

4. *Manual for Courts-Martial, United States* (Washington, DC: Joint Service Committee on Military Justice, 2019), R.C.M. 306. Courts-martial can be general, special, or summary depending on the level of command at which the charges are referred to court-martial and the seriousness of the alleged offenses.

5. Ibid.

6. Ibid., R.C.M. 401–404, 407.

7. Ibid., Preamble.

8. Ibid., R.C.M. 701–703, 706, 801, 905–907.

9. Ibid., R.C.M. 901, 911–912B.

10. Army Regulation (AR) 635-200, *Active Duty Enlisted Administrative Separations* (Washington, DC: U.S. Government Publishing Office [GPO], December 2016), chap. 1, 2, 14. Officer discharges can be even more onerous as they require a board of inquiry once an officer is past his or her probationary period; AR 600-8-24, *Officer Transfers and Discharges* (Washington, DC: U.S. GPO, February 2020), chap. 4.

11. James J. Mingus, "Profession of Arms and Mission Command—Panel Discussion" (Command and General Staff College, Fort Leavenworth, KS, 30 October 2019).

12. Army Doctrine Publication (ADP) 6-22, *Army Leadership and the Profession* (Washington, DC: U.S. GPO, November 2019), 5-7, 6-7.

13. Secretary of Defense, memorandum to Secretaries of the Military Departments, Chiefs of the Military Services, Commanders of the Combatant Commands, "Discipline and Lethality," 13 August 2018, accessed 14 August 2020, https://www.marines.mil/News/Press-Releases/Press-Release-Display/Article/1605285/secretary-of-defense-message-to-the-force/.

14. Ibid.

15. *Joint Annual Report of the Code Committee Pursuant to the Uniform Code of Military Justice, October 1, 2016 to September 30, 2017* (Washington, DC: Department of Defense [DOD], 2018), 34–55; *Joint Annual Report of the Code Committee Pursuant to the Uniform Code of Military Justice, October 1, 2015 to September 30, 2016* (Washington, DC: DOD, 2017), 30–51; *Joint Annual Report of the Code Committee Pursuant to the Uniform Code of Military Justice, October 1, 2014 to September 30, 2015* (Washington, DC: DOD, 2016), 33–49; *Joint Annual Report of the Code Committee Pursuant to the Uniform Code of Military Justice, October 1, 2013 to September 30, 2014* (Washington, DC: DOD, 2015), 34–56; *Joint Annual Report of the Code Committee Pursuant to the Uniform Code of Military Justice, October 1, 2012 to September 30, 2013* (Washington, DC: DOD, 2014), 30–52; *Joint Annual Report of the Code Committee Pursuant to the Uniform Code of Military Justice, October 1, 2011 to September 30, 2012* (Washington, DC: DOD, 2013), 30–51; *Joint Annual Report of the Code Committee Pursuant to the Uniform Code of Military Justice, October 1, 2010 to September 30, 2011* (Washington, DC: DOD, 2012), 1–23; *Joint Annual Report of the Code Committee Pursuant to the Uniform Code of Military Justice, October 1, 2009 to September 30, 2010* (Washington, DC: DOD, 2011), 1–23; *Joint Annual Report of the Code Committee Pursuant to the Uniform Code of Military Justice, October 1, 2008 to September 30, 2009* (Washington, DC: DOD, 2010), 1–25; *Joint Annual Report of the Code Committee Pursuant to the Uniform Code of Military Justice, October 1, 2007 to September 30, 2008* (Washington, DC: DOD, 2009), 3–21; *Joint Annual Report of the Code Committee Pursuant to the Uniform Code of Military Justice, October 1, 2006 to September 30, 2007* (Washington, DC: DOD, 2008), 2–23.

16. *FY2017 Army Crime Report* (Washington, DC: Office of the Provost Marshal General, December 2018), 15–20; *FY2013 Army Crime Report* (Washington, DC: Office of the Provost Marshal General, April 2014), 10–13.

17. ADP 6-22, *Army Leadership and the Profession*, 1-1 to 1-2.

18. Ibid., 1-2.

19. Ibid., 1-1.

20. Ibid., 6-8.

21. Ibid.

22. Ibid., 1-3, 2-10.

23. Ibid., 5-6.

24. Don M. Snider, "Five Myths about Our Future," *Parameters* 46, no. 3 (Autumn 2016): 52.

25. ADP 6-22, *Army Leadership and the Profession*, 1-1. "The Army has a dual nature as both a military department of government and a trusted military profession."

26. Ibid., 1-2.

27. National Defense Authorization Act for Fiscal Year 2012 § 582, Pub. L. No. 112-81, 125 Stat. 1386 (2011).

28. National Defense Authorization Act for Fiscal Year 2014 § 1701–1716, 1744, Pub. L. No. 113-66, 127 Stat. 952 (2013).

29. Military Justice Improvement Act of 2019, S. 1789, 116th Cong. (2019).

30. "Military Justice Improvement Act," Kirsten Gillibrand, United States Senator for New York, accessed 25 August 2020, https://www.gillibrand.senate.gov/mjia.

31. Ibid.

32. "Confidence in Institutions," Gallup, accessed 14 August 2020, https://news.gallup.com/poll/1597/confidence-institutions.aspx.

33. Luke Barr, "US Police Agencies Having Trouble Hiring, Keeping Officers, According to a New Survey," ABC News, 17 September 2019, accessed 14 August 2020, https://abcnews.go.com/Politics/us-police-agencies-trouble-hiring-keeping-officers-survey/story?id=65643752.

34. Secretary of Defense, "Discipline and Lethality."

35. Charles N. Pede and Stuart W. Risch, "Military Justice's New Blueprint," *Army Lawyer*, no. 4 (2019): 2.

36. *Manual for Courts-Martial*, app. 2.1.

37. Ibid.

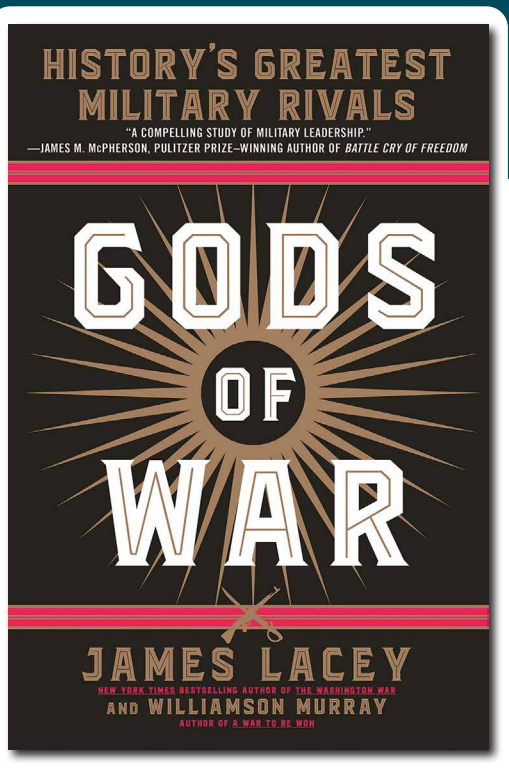
38. Ibid.

39. Ibid.

40. Ibid., R.C.M. 306(c).

41. Eric Schmitt, "Commandos' Behavior Prompts Pentagon Review of Special Operations Culture," *New York Times* (website), 12 August 2019, accessed 14 August 2020, https://www.nytimes.com/2019/08/12/us/politics/special-operations-pentagon-review.html.

REVIEW ESSAY



Gods of War

History's Greatest Military Rivals

James Lacey and Williamson Murray, Bantam Books, New York, 2020, 416 pages

Mark Montesclaros

The intriguing title of this book is bound to attract intellectual curiosity, whether in reference to Greek or Roman mythology or to military warfare as implied. For this reviewer, a fairly obtuse reference comes to mind—Tom Wolfe's *The Right Stuff*, when describing the plight of the Mercury 7 astronauts in their quest for the heavens against the vaunted Russians, he introduces the concept of "single combat warrior."[1] This hero, representing his people or the state, would do battle with a similarly endowed counterpart in order to resolve conflict without unnecessary bloodshed. Of course, the rivals considered by prominent historians James Lacey and Williamson Murray did not go it alone, as they were aided by armies of varying sizes, but the head-to-head matchup is a compelling one nonetheless. Whether in warfare or in more common pursuits such as sports, nothing captures the attention more than a contest between two supremely gifted and equally talented rivals. If *Gods of War* were about sports, perhaps an appropriate analogy would be the "Thrilla in Manila," or Ali-Frazier III, the rubber match that culminated the heavyweight campaign between two historic juggernauts. However, do not take this analogy too far; *Gods of War* is a serious intellectual exercise despite its eye-catching title.

In *Gods of War*, Lacey and Murray demonstrate their considerable talents in analyzing and synthesizing six such matchups between equally adept opponents—the key term here is *evenly matched*. These case studies constitute the core of the book (chapters 2–6) and span roughly 2,200 years of military history—an impressive exercise in time, space, and purpose reminiscent of John Keegan's *A History of Warfare* and *The Mask of Command* or Victor Davis Hanson's *Carnage and Culture*, all of which challenge readers to think critically across the tactical, operational, and strategic realms of warfare. Two of the case studies deal with the ancient world—Hannibal and Scipio, and Caesar versus Pompey. The next—Richard I and Saladin during the Second Crusade—matches the two greatest military leaders of medieval times, according to the authors. These are followed by sections that

are perhaps more familiar to attendees or graduates of professional military education institutions across the services—Napoleon and Wellington, Grant versus Lee, and Rommel versus Montgomery and Patton. The six rivalries can be read separately or sequentially as they are self-contained, each with its own contextual introduction, body, and conclusion. They are bookended by two very thought-provoking pieces (chapters 1 and 8)—the first setting the context, or "framework for war," as the authors put it. The final chapter concludes the discourse, and like the first, effectively connects the dots between the six rivalries and provides the "so what" and "where do we go from here" intellectual underpinnings for the book.

While it is beyond the scope of this review to analyze each of the chapters in depth, some overarching comments are appropriate. Perhaps the most cogent is *Gods of War* will challenge the reader's assumptions and is bound to stimulate further inquiry into a number of issues. Lacey and Murray—pardon the repeat boxing analogy—pull no punches in this regard. They make a number of assertions that may cause readers to do a double take and then explain them in terms that are clear and accessible, especially to military professionals. (After all, both authors have extensive experience teaching and writing at the military academies and/or professional military education institutions across the services.) An early example of such an assertion appears as the authors consider the efficacy of "military genius" in chapter 1: "Acknowledging the misery caused by many of history's military geniuses, it is surely a good thing that there have been so few of them."[2] The authors then go on to explain their rationale, arguing that military genius is contextual and idiosyncratic in nature, and has often caused more harm than good to the societies that produced this quality in their leaders.

A second example is in the authors' consideration of what constitutes decisive battle. Referring to the World War II case study, they state, "There were certainly no decisive battles in the conduct of the war."[3] Generations of students raised on the criticality of engagements such as Midway, El Alamein, Stalingrad, and the Battle of Britain may scratch their heads at this assertion. However, the authors effectively explain that the importance of the single, decisive engagement was already on the wane toward the end of the Napoleonic period based on changes in the nature of warfare brought on by the Industrial and French Revolutions. Henceforth, campaigns rather than battles came to the fore. Consequently, *Gods of War* focuses its attention in its latter chapters on how campaigns, rather than tactical engagements, were prosecuted by the rivals. The authors contend that the unrelenting pursuit of a single, decisive victory (à la Hannibal at Cannae, covered in chapter 2) eventually did in exemplary battlefield commanders such as Robert E. Lee and his Army of Northern Virginia, and continues to impact military doctrine even today. These examples help set the tone for the case studies that follow and establish themes that provide continuity throughout the book.

Another overarching comment—and one of the book's strengths—is that *Gods of War* provides great insight into the complexity of military genius and its relationship to leadership. Throughout the case studies and the chapters that bookend them, Lacey and Murray really do teach their readers about warfare, perhaps their most important goal as stated in the book's preface. And because the authors converse in a style and language that military professionals will recognize, readers will no doubt be readily equipped to challenge—as well as learn from—the authors' point of view. Regarding military genius, the authors clearly parse this somewhat amorphous concept and differentiate its multiple aspects. One way is through the levels of war paradigm; in their articulation of the case studies, they often refer to the how the rivals performed at the strategic, operational, and/or tactical levels of war. As an example, they conclude that of the six sets of rivals, only Saladin (during the Third Crusade) and Ulysses S. Grant (after assuming command of the Union army during the Civil War) had a strategic vision and saw it through to a successful outcome. Virtually all of the rivals succeeded at the tactical level as great battlefield generals—which seems to be a sine qua non for "military genius" status, but that did not necessarily translate into operational or strategic success. Hannibal, Richard I, Napoleon, Robert E. Lee, and Erwin

Mark Montesclaros
is an assistant professor in the Department of Joint, Interagency, and Multinational Operations at the Fort Gordon Satellite Campus of the U.S. Army Command and General Staff College. A thirty-year Army veteran, he holds a BS from the U.S. Military Academy, an MA in Latin American studies from the University of Texas at Austin, and an MSS from the U.S. Army War College. He has taught strategy at the Army War College and served as defense attaché to the Republic of Panama.

Rommel come to mind in this regard—audacious battlefield generals skilled at maneuver and firepower but unable to achieve strategic success due to either the nature of the regimes they served or to personal flaws that eventually derailed them.

Turning briefly to the topic of leadership, in *The Mask of Command*, eminent historian Sir John Keegan wrote, "The first and greatest imperative of command is to be present in person."[4] All of the rivals excelled in this regard, without exception. One of *Gods of War*'s strengths is to bring to light some of the tactical exploits of the rivals as junior or intermediate leaders during their formative years—some of which are perhaps less well known to general readers. Scipio, Pompey, Saladin, Wellington (Arthur Wellesley), and Montgomery all led by example and exhibited elements (to varying degrees) of personal courage, audacious action, leading from the front, and identifying with their men. The authors effectively set the contextual tone for each case study by highlighting these tactical leadership strengths and how those strengths contributed to the generalship exhibited in later campaigns against their vaunted rivals.

A final observation deals with the case studies themselves; like the rest of the book, they are highly readable, insightful, and thought provoking. Each case study considers the plight of the protagonists before, during, and after the campaign in question—no easy feat considering the longevity of luminaries such as Hannibal, Caesar, and Napoleon, to name a few. (As a quick aside, the authors consider Caesar, not Alexander, as the greatest general in the ancient world.) The artistry in synthesizing so much history in the span of a chapter is evident; Lacey and Murray provide sufficient buildup to make the "matchup" exciting and have the reader anticipating the event. And while the conduct and results of the historical campaigns are generally well known, the authors provide their own analysis and expertise such that the recounting of events is never dull, never rote. They provide insightful analysis on the winners and losers of each rivalry, explaining why each conflict ended the way it did and using the prism of the aspects of military genius mentioned above. So, to employ one final sports analogy—perhaps fitting for a book discussing six of the greatest rivalries in military history—who is the GOAT ("greatest of all time")? While not stated in quite that manner, the evidence seems to favor Ulysses S. Grant, whose stock has risen over time (one piece of recent evidence—the History Channel's recent, critically acclaimed three-part biopic). The authors laud Grant for his ability to link all of the levels of warfare—particularly the strategic and operational—and his recognition that only by bringing "hard war" to the South could the Union be preserved. In particular, they mention that many consider Grant's operations against Vicksburg "the most brilliant campaign ever undertaken by an American general."[5]

The book is not without some minor flaws. A small example is Saladin's capture of Jerusalem; it occurred in the year 1187, not in 1177 as stated in the book. Graphically, some of the diagrams depicting ancient orders of battle are a bit dark and ambiguous, and the authors include a graphic of Operation Market Garden that is somewhat superfluous due to its relative lack of coverage in the text. Perhaps a map of the European theater of operations would be a better accompaniment to the chapter on Erwin Rommel, George Patton, and Bernard Montgomery. Obviously, these shortcomings are far outweighed by the book's many positive aspects as noted above.

Gods of War is highly recommended to military professionals and would make a worthy addition to the services' reading lists. It would also serve well as a graduate-level text due to its case-study format, power of analysis, and depth of research. As noted earlier, authors Lacey and Murray seek to teach their readers something about warfare. With *Gods of War*, they more than accomplish that goal, providing their audience much to ponder and discuss. They make a great contribution to lifelong learning and to the intellectual development of military professionals in this highly readable, accessible and thought-provoking work. ■

Notes

1. Tom Wolfe, *The Right Stuff* (New York: Bantam Books, 1983), 101.
2. James Lacey and Williamson Murray, *Gods of War: History's Greatest Military Rivals* (New York: Bantam Books, 2020), 6.
3. Ibid., 31.
4. John Keegan, *The Mask of Command* (New York: Penguin Books, 1987), 329.
5. Lacey and Murray, *Gods of War*, 272.

TITLE INDEX

AUTHOR INDEX

SUBJECT INDEX

Africa

U.S. Army; Chief Warrant Officer 4 Jesse R. Crifasi, U.S. Army; and Chief Warrant Officer 3 Nick Rife, U.S. Army (November-December): 38

"Tactical Data Science," Col. Harry D. Tunnell IV, PhD, U.S. Army, Retired (July-August): 123

Terrorism

"Tweeting Terror Live: Al-Shabaab's Use of Twitter during the Westgate Attack and Implications for Counterterrorism Communications," Victoria Fassrainer (March-April): 85

Training & Education

"Adapting to the COVID-19 Pandemic: Transitioning from Literal to Virtual Teaching at the Command and General Staff School (CGSS)," Lt. Col. George Hodge, U.S. Army, Retired; Lt. Col. Richard A. McConnell, DM, U.S. Army, Retired; and Lt. Col. Thad Weist, U.S. Army, Retired (August online exclusive)

"Connecting the Dots: Developing Leaders Who Can Turn Threats into Opportunities," Lt. Col. Richard A. McConnell, DM, U.S. Army, Retired (May-June): 27

"Decisive Action Goes Digital," Col. Chad LeMay, U.S. Army, Retired; Lt. Col. Timothy J. Brown, U.S. Army, Retired; Lt. Col. David S. Collins, U.S. Army, Retired; and Lt. Col. M. Shane Perkins, U.S. Army, Retired (September online exclusive)

"Key Ingredient in Army Leader Development: Graduate School," Maj. George Fust, U.S. Army (January-February): 108

"Lightning Strike," Brig. Gen. Joel B. (J. B.) Vowell, U.S. Army; Maj. Benjamin Scott, U.S. Army; and Maj. Edward Guelfi, U.S. Army (March-April): 19

"Preventing the Collapse: Fighting Friction after First Contact at the National Training Center," Lt. Col. Brian P. Schoellhorn, U.S. Army (March-April): 6

"Sluss-Tiller Tests the Cultural Competence Special Operations Forces Need," Louise J. Rasmussen, PhD (March-April): 106

"Tactical Data Science," Col. Harry D. Tunnell IV, PhD, U.S. Army, Retired (July-August): 123

"Training in the Time of COVID-19," Maj. Thomas Michael Warth, Kansas Army National Guard (October online exclusive)

"We Are Missing Opportunities to Build Sustained, Total Force Readiness Inside Brigade Combat Teams," Lt. Col. Nicholas Melin, DPhil, U.S. Army (March-April): 30

Transformation

"Tactical Data Science," Col. Harry D. Tunnell IV, PhD, U.S. Army, Retired (July-August): 123

Turkey

"Istanbul: A Tale of Three Cities" (Review Essay), Robert D. Spessert, JD (July-August): 151

Unit Status Reports

"Unit Status Reports and the Gaming of Readiness," Capt. Theo Lipsky, U.S. Army (July-August): 148

Urban Terrain

"The 2003 Battle of Baghdad: A Case Study of Urban Battle during Large-Scale Combat Operations," Maj. Nicolas Fiore, U.S. Army (September-October): 127

U.S. Navy

"Admiral Bill Halsey: A Naval Life" (Review Essay), Lt. Col. John H. Modinger, PhD, U.S. Air Force, Retired (January-February): 128

"Sailing True North: Ten Admirals and the Voyage of Character" (Review Essay), Lt. Col. John H. Modinger, PhD, U.S. Air Force, Retired (September-October): 158

Uzbekistan

"Rethinking Uzbekistan: A Military View," Maj. Daniel J. O'Connor, U.S. Army (March-April): 116

Venezuela

"Venezuela in Light of Anti-American Parties and Affiliations in Latin America," Lt. Col. Geoffrey Demarest, JD, PhD, U.S. Army, Retired (July-August): 110

Warfighter Exercise

"Lightning Strike," Brig. Gen. Joel B. (J. B.) Vowell, U.S. Army; Maj. Benjamin Scott, U.S. Army; and Maj. Edward Guelfi, U.S. Army (March-April): 19

Warfighting Functions

"Information on the Twenty-First Century Battlefield: Proposing the Army's Seventh Warfighting Function," Capt. Charles M. Kelly, U.S. Army (January-February): 62

World War II

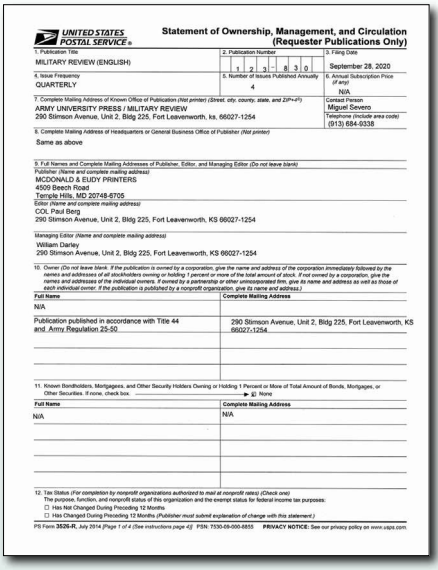
"Admiral Bill Halsey: A Naval Life" (Review Essay), Lt. Col. John H. Modinger, PhD, U.S. Air Force, Retired (January-February): 128

"Assault on Fortress Europe: Military Deception and Operation Fortitude South," Lt. Jason Carminati, U.S. Navy (September online exclusive)

"The Early Air War in the Pacific: Ten Months That Changed the Course of World War II" (Review Essay), Lt. Col. Jesse McIntyre III, U.S. Army, Retired (March-April): 130

"Option 17: Military Law and Vigilante Justice in Prisoner of War Camps during World War II," Mark M. Hull, PhD, JD, FRHistS (January-February): 100

"Preventable Casualties: Rommel's Flaw, Slim's Edge," Col. Ronald F. Bellamy, MD, U.S. Army; and Col. Craig H. Llewellyn, MD, U.S. Army, Retired (May-June): 46



UNITED STATES POSTAL SERVICE®

Statement of Ownership, Management, and Circulation (Requester Publications Only)

1. Publication Title: MILITARY REVIEW (ENGLISH)
2. Publication Number: 1 2 3 - 8 3 0
3. Filing Date: September 28, 2020
4. Issue Frequency: QUARTERLY
5. Number of Issues Published Annually: 4
6. Annual Subscription Price (if any): N/A
7. Complete Mailing Address of Known Office of Publication (Not printer) (Street, city, county, state, and ZIP+4®): ARMY UNIVERSITY PRESS / MILITARY REVIEW, 290 Stimson Avenue, Unit 2, Bldg 225, Fort Leavenworth, ks, 66027-1254
Contact Person: Miguel Severo
Telephone (Include area code): (913) 684-9338
8. Complete Mailing Address of Headquarters or General Business Office of Publisher (Not printer): Same as above
9. Full Names and Complete Mailing Addresses of Publisher, Editor, and Managing Editor (Do not leave blank)
Publisher (Name and complete mailing address): MCDONALD & ELIOY PRINTERS, 4509 Beech Road, Temple Hills, MD 20748-9705
Editor (Name and complete mailing address): COL Paul Berg, 290 Stimson Avenue, Unit 2, Bldg 225, Fort Leavenworth, KS 66027-1254
Managing Editor (Name and complete mailing address): William Darley, 290 Stimson Avenue, Unit 2, Bldg 225, Fort Leavenworth, KS 66027-1254
10. Owner (Do not leave blank. If the publication is owned by a corporation, give the name and address of the corporation immediately followed by the names and addresses of all stockholders owning or holding 1 percent or more of the total amount of stock. If not owned by a corporation, give the names and addresses of the individual owners. If owned by a partnership or other unincorporated firm, give its name and address as well as those of each individual owner. If the publication is published by a nonprofit organization, give its name and address.)

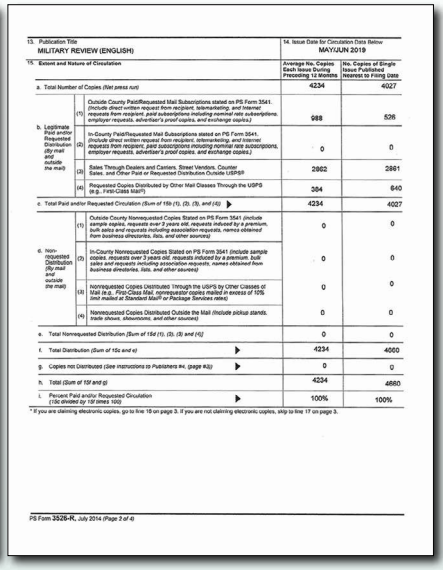
Full Name	Complete Mailing Address
N/A	
Publication published in accordance with Title 44 and Army Regulation 25-50	290 Stimson Avenue, Unit 2, Bldg 225, Fort Leavenworth, KS 66027-1254

11. Known Bondholders, Mortgagees, and Other Security Holders Owning or Holding 1 Percent or More of Total Amount of Bonds, Mortgages, or Other Securities. If none, check box: → ☒ None

Full Name	Complete Mailing Address
N/A	N/A

12. Tax Status (For completion by nonprofit organizations authorized to mail at nonprofit rates) (Check one)
The purpose, function, and nonprofit status of this organization and the exempt status for federal income tax purposes:
☐ Has Not Changed During Preceding 12 Months
☐ Has Changed During Preceding 12 Months (Publisher must submit explanation of change with this statement.)

PS Form 3526-R, July 2014 [Page 1 of 4 (See instructions page 4)] PSN: 7530-09-000-8855 **PRIVACY NOTICE:** See our privacy policy on www.usps.com

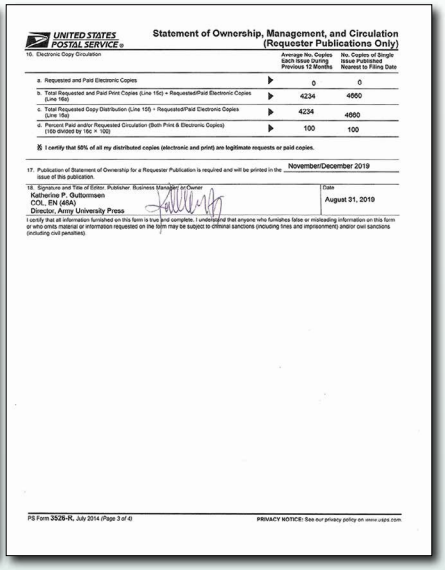


13. Publication Title: MILITARY REVIEW (ENGLISH)
14. Issue Date for Circulation Data Below: MAY/JUN 2019

15. Extent and Nature of Circulation			Average No. Copies Each Issue During Preceding 12 Months	No. Copies of Single Issue Published Nearest to Filing Date
a. Total Number of Copies (Net press run)			4234	4027
b. Legitimate Paid and/or Requested Distribution (By mail and outside the mail)	(1)	Outside County Paid/Requested Mail Subscriptions stated on PS Form 3541. (Include direct written request from recipient, telemarketing, and Internet requests from recipient, paid subscriptions including nominal rate subscriptions, employer requests, advertiser's proof copies, and exchange copies.)	988	526
	(2)	In-County Paid/Requested Mail Subscriptions stated on PS Form 3541. (Include direct written request from recipient, telemarketing, and Internet requests from recipient, paid subscriptions including nominal rate subscriptions, employer requests, advertiser's proof copies, and exchange copies.)	0	0
	(3)	Sales Through Dealers and Carriers, Street Vendors, Counter Sales, and Other Paid or Requested Distribution Outside USPS®	2862	2861
	(4)	Requested Copies Distributed by Other Mail Classes Through the USPS (e.g., First-Class Mail®)	384	640
c. Total Paid and/or Requested Circulation (Sum of 15b (1), (2), (3), and (4)) ▶			4234	4027
d. Non-requested Distribution (By mail and outside the mail)	(1)	Outside County Nonrequested Copies Stated on PS Form 3541 (include sample copies, requests over 3 years old, requests induced by a premium, bulk sales and requests including association requests, names obtained from business directories, lists, and other sources)	0	0
	(2)	In-County Nonrequested Copies Stated on PS Form 3541 (include sample copies, requests over 3 years old, requests induced by a premium, bulk sales and requests including association requests, names obtained from business directories, lists, and other sources)	0	0
	(3)	Nonrequested Copies Distributed Through the USPS by Other Classes of Mail (e.g., First-Class Mail, nonrequestor copies mailed in excess of 10% limit mailed at Standard Mail® or Package Services rates)	0	0
	(4)	Nonrequested Copies Distributed Outside the Mail (Include pickup stands, trade shows, classrooms, and other sources)	0	0
e. Total Nonrequested Distribution (Sum of 15d (1), (2), (3) and (4))			0	0
f. Total Distribution (Sum of 15c and e) ▶			4234	4660
g. Copies not Distributed (See instructions to Publishers #4, (page #3)) ▶			0	0
h. Total (Sum of 15f and g)			4234	4680
i. Percent Paid and/or Requested Circulation (15c divided by 15f times 100) ▶			100%	100%

* If you are claiming electronic copies, go to line 16 on page 3. If you are not claiming electronic copies, skip to line 17 on page 3.

PS Form 3526-R, July 2014 (Page 2 of 4)



UNITED STATES POSTAL SERVICE®

Statement of Ownership, Management, and Circulation (Requester Publications Only)

16. Electronic Copy Circulation	Average No. Copies Each Issue During Previous 12 Months	No. Copies of Single Issue Published Nearest to Filing Date
a. Requested and Paid Electronic Copies ▶	0	0
b. Total Requested and Paid Print Copies (Line 15c) + Requested/Paid Electronic Copies (Line 16a) ▶	4234	4660
c. Total Requested Copy Distribution (Line 15f) + Requested/Paid Electronic Copies (Line 16a) ▶	4234	4660
d. Percent Paid and/or Requested Circulation (Both Print & Electronic Copies) (16b divided by 16c × 100) ▶	100	100

☒ I certify that 50% of all my distributed copies (electronic and print) are legitimate requests or paid copies.

17. Publication of Statement of Ownership for a Requester Publication is required and will be printed in the November/December 2019 issue of this publication.

18. Signature and Title of Editor, Publisher, Business Manager, or Owner: Katherine P. Guttormsen, COL, EN (ARA), Director, Army University Press. Date: August 31, 2019

I certify that all information furnished on this form is true and complete. I understand that anyone who furnishes false or misleading information on this form or who omits material or information requested on the form may be subject to criminal sanctions (including fines and imprisonment) and/or civil sanctions (including civil penalties).

PS Form 3526-R, July 2014 (Page 3 of 4) **PRIVACY NOTICE:** See our privacy policy on www.usps.com

Farewell, Col. Paul Berg

Congratulations to Col. Paul Berg, the director of the Army University Press (AUP) and the editor in chief of *Military Review*, on his retirement after twenty-nine years of service in the U.S. Army.

While his tenure as director of AUP was unfortunately short, he had a positive impact on our organization for a much longer time. The staff of *Military Review* has had the good fortune to work with Col. Berg since early 2017 when he assumed responsibility as the editor in chief of the *Journal of Military Learning*. He oversaw publication of this peer-reviewed academic journal through its first seven issues. Col. Berg also supervised the production of AUP's highly touted Large-Scale Combat Operations book series. And, as director of AUP, he provided crucial leadership as the organization rapidly transitioned to teleworking due to the COVID-19 pandemic.

Col. Berg will be missed by everyone in our organization, but after his successful Army career, we anticipate hearing of his continued accomplishments as a civilian in the field of education and as a military veteran.

AN ARMY UNIVERSITY PRESS PUBLICATION

https://www.armyupress.army.mil
PB-100-20-11/12
Headquarters, Department of the Army
Approved for public release
Distribution is unlimited–Distribution A

PIN: 207775-000