

COUNTERING THREATS IN THE FUTURE OPERATIONAL ENVIRONMENT



Subscriptions: Free unit subscriptions are available by emailing the editor at usarmy.huachuca.icoe.mbx.mipb@mail.mil. Include the complete mailing address (unit name, street address, and building number).

Don't forget to email the editor when your unit moves, deploys, or redeploys to ensure continual receipt of the bulletin.

Reprints: Material in this bulletin is not copyrighted (except where indicated). Content may be reprinted if the MI Professional Bulletin and the authors are credited.

Our mailing address: MIPB (ATZS-DST-B), Dir. of Doctrine and Intel Sys Trng, USAICoE, 550 Cibique St., Fort Huachuca, AZ 85613-7017

Commanding General

MG Anthony R. Hale

Chief of Staff

COL Norman S. Lawrence

Chief Warrant Officer, MI Corps

CW5 Aaron H. Anderson

Command Sergeant Major, MI Corps

CSM Warren K. Robinson

STAFF:

Editor

Tracey A. Remus
usarmy.huachuca.icoe.mbx.mipb@mail.mil

Associate Editor

Maria T. Eichmann

Design and Layout

Emma R. Morris

Cover Design

Emma R. Morris

Military Staff

CPT Michael J. Lapadot

Cover image: Map depicting the original Air Identification Zone line from 1947 and the latest modifications from 2009. (U.S. Department of Defense)

Purpose: The U.S. Army Intelligence Center of Excellence publishes the **Military Intelligence Professional Bulletin (MIPB)** quarterly under the provisions of **AR 25-30**. MIPB presents information designed to keep intelligence professionals informed of current and emerging developments within the field and provides an open forum in which ideas; concepts; tactics, techniques, and procedures; historical perspectives; problems and solutions, etc., can be exchanged and discussed for purposes of professional development.

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
2106300

From the Editor

The following themes and deadlines are established:

July–September 2021, *Theater Intelligence Operations*. This issue will focus on theater army-level, regionally focused intelligence capabilities and operations supporting Army and joint forces across the specific regions. Deadline for article submission is 1 May 2021.

October–December 2021, *Intelligence Disciplines*. This issue will focus on new, critical, and refocused aspects of the intelligence disciplines and complementary intelligence capabilities. Deadline for article submission is 1 July 2021.

January–March 2022, *Targeting and Intelligence*. This issue will focus on how intelligence operations are evolving to support the delivery of lethal and nonlethal effects against intended targets. Deadline for article submission is 21 September 2021.

Although MIPB targets quarterly themes, you do not need to write an article specifically to that theme. We publish non-theme articles in most issues, and we are always in need of new articles on a variety of topics.

For us to be a successful professional bulletin, we depend on you, the reader. Please call or email me with any questions regarding article submissions or any other aspects of MIPB. We welcome your input and suggestions.



Tracey A. Remus
Editor

The views expressed in the following articles are those of the authors and do not necessarily reflect the official policy or position of the Departments of the Army or Defense, or the U.S. Government. Article content is not authenticated Army information and does not supersede information in any other Army publication.

It is with our most sincere appreciation that we would like to thank COL Rob Wagner, Deputy G-2, U.S. Army Training and Doctrine Command, and COL Jimmy Blejski, Deputy Director of Intelligence and Security, U.S. Army Futures Command, for their proactive involvement as the “stakeholders” for this issue. Their enthusiasm and overall vision for the project brought together a variety of perspectives from around the military intelligence community and resulted in a truly outstanding peer and emerging threats issue.

FEATURES

- 8 Ensuring a Seamless Army Narrative for the Operational Environment**
by COL Jimmy Blejski and COL Rob Wagner
 - 14 Future Operational Environment and Emerging Threats**
by the Future Operational Environment Directorate, Futures and Concepts Center; and the Directorate of Intelligence and Security, U.S. Army Futures Command
 - 20 Training the Operational Intelligence Force: On Target for Military Intelligence Readiness in 2022**
by COL Timothy J. Parker
 - 25 The Operational Environment in Multi-Domain Operations**
by Mr. Darryl Ward
 - 31 Technology Protection: Securing Modernization Efforts**
by the Directorate of Intelligence and Security, U.S. Army Futures Command
 - 35 Joint Operating Environment 2040**
by Mr. Jeffrey Becker
 - 38 Battlefield Development Plans: Threat Analysis Enabling Multi-Domain Operations**
by Mr. Earl S. Bittner
 - 43 Russian Perspective and Operational Framework**
by Mr. David P. Harding, COL David Pendall (Retired), and LTC Steven J. Curtis
 - 53 Forecasting the Threat within the Future Operational Environment**
by Dr. Elyssa Dunfee, Mr. Ralph Edwards, and Dr. Christopher Beiter
 - 59 Training Today’s Army for Tomorrow’s Threats**
by Ms. Jennifer Dunn
 - 62 China’s Sustained Success in Sub-Saharan Africa: Letting China Pick Up the Check**
by CW4 Charles Davis
 - 68 Freely Associated States**
by Mr. Geoffrey Goudge, Maj. Christopher Neal, and MAJ Mark Swiney
 - 76 Fighting the Division Intelligence Enterprise in Large-Scale Ground Combat Operations**
by LTC James Leidenberg
 - 83 Setting the Theater: Intelligence and Interoperability in DEFENDER-Europe 20**
by MAJ Chad Lorenz
-
- 88 COVID-19 Surveillance: Hidden Risks and Benefits for Identity Intelligence**
by Ms. Christine Kaiser, Mr. Gregory Smith, and Mr. Kasey Diedrich
 - 94 Modernization of Army Counterintelligence and Human Intelligence Collection Management**
by Ms. Erin Masly
 - 99 Mental Health in the Intelligence Community, Uncovered**
by Ms. Pamela J. Miller

DEPARTMENTS

- | | |
|--------------------------------|---|
| 2 Always Out Front | 102 Lessons Learned |
| 4 CSM Forum | 107 Proponent Notes |
| 6 Technical Perspective | 110 Military Intelligence Hall of Fame |

Inside back cover: Contact and Article Submission Information



Always Out Front

by Major General Anthony R. Hale

Commanding General

U.S. Army Intelligence Center of Excellence



We are entering a period in which we will face near-peer and peer threats constantly challenging and undermining U.S. interests across the competition continuum. This continuum envisions a world of enduring competition in which our relationship with peer adversaries alternates quickly between cooperation, competition below armed conflict, and armed conflict.¹ This operational environment includes challenges such as those we faced from the conventional forces of the Soviet Union, a threat we confronted when I first arrived at Fort Huachuca in 1991. Additionally, the operational environment includes continued asymmetric threats from violent non-state actors.

This edition of *Military Intelligence Professional Bulletin* (MIPB) will frame, define, explain, and share best practices for attacking the challenges of this new environment. You will find articles that provide greater insight into what our best and brightest believe the future operational environment will look like; details on our modernization efforts across doctrine, organization, training, materiel, leadership and education, personnel, facilities, and policy; and details on how leaders across the force can contribute and apply these efforts to their units. The U.S. Army Intelligence Center of Excellence's (USAI CoE's) top objectives are to continue to *Build Leaders* and *Drive Change* in order to support the Army's modernization efforts.

The Future Operational Environment

Refocusing on our fundamentals, the first two steps of intelligence preparation of the battlefield are to define the operational environment and to describe the environmental effects on operations. Some of the articles in this MIPB edition describe a future operational environment in which the United States will face enduring strategic competition. The global concentration of power and the pace of technological innovation will change our ability to fore-



cast the future. These shifts will affect how our joint force approaches the joint operating environment. They will also dictate how the Intelligence Corps will work across Department of Defense and agency lines to drive the convergence of resources and capabilities against our adversary.

The Military Intelligence (MI) Corps must be postured for an unpredictable environment in which relationships with adversaries progress and regress rapidly between cooperation, competition, and crisis, and then back to cooperation.

The MI Corps has two key requirements in order to operate successfully: we must continue to inform our organizations of the threat and the environment, and we must proactively drive operations.

Modernization with an Intelligence Nexus

The manner in which we aim to achieve this, to paraphrase Chief of Staff of the Army GEN James C. McConville, is the most ambitious modernization effort in 40 years. Our teams have made significant progress in peer-threat emulation and technology protection best practices. The MIPB article by the Directorate of Intelligence and Security, U.S. Army Futures Command, details challenges posed by Chinese theft of intellectual property and government secrets. As the Department of the Army G-2's priority effort, counterintelligence reform and implementation of program protection plans are vital to our ability to retain technological and intellectual advantages over adversaries.

Our goal in training, building leaders, and personnel reform, as well as modernization, must close the gaps between the fielded force and the future force. FREEDOM 2's article describes the positive effects of the Military Intelligence Training Strategy and advanced operational courses. These changes will enable operational units not only to incorporate institutional best practices without

sacrificing significant time and resources but also to enable USAICoE to continuously update course curricula and remain in lockstep with U.S. Army Forces Command. We are also looking to establish an initiative to accelerate materiel changes by using feedback directly from “line” units.

MAJ Chad Lorenz’s article provides feedback from 1st Cavalry Division’s participation in DEFENDER-Europe 20 that directly benefits our warfighter. It is not sufficient to merely understand our systems and how to operate them. Our Soldiers must be capable of fighting with them in a multi-domain environment, connecting from a tactical echelon to the national enterprise. As LTC James Leidenberg’s article describes, the Army will fight large-scale ground combat operations at the division level, rather than with brigade combat teams, to execute Army and joint force operations. This represents a paradigm shift and highlights the importance of formations like the

expeditionary-MI battalion in support of our ability to effectively conduct intelligence operations in large-scale ground combat operations.

We maintain overmatch on near-peer adversaries at present, but we can expect that lead to diminish, and vanish, in key realms in the coming decade unless we continue to *Build Leaders* and *Drive Change*. Our ultimate goal is to develop our Soldiers, training, and equipment to shorten the sensor-to-shooter timeframe, increase accuracy and consistency, and drive operations on our terms. Then we can outmaneuver our enemies and overwhelm them with synchronized effects from multiple domains and directions. All of us, as an MI team, are key ingredients to reaching these goals. – Desert-6. 

Endnote

1. Joint Chiefs of Staff, Joint Doctrine Note 1-19, *Competition Continuum* (Washington, DC: U.S. Government Publishing Office, 3 June 2019), v.

Always Out Front!

Available Now

TC 2-19.01, *Military Intelligence (MI) Company and Platoon Reference Guide*

The Combined Arms Center Commander directed the development of TC 2-19.01, *Military Intelligence (MI) Company and Platoon Reference Guide*, to address a gap in field craft skills for large-scale ground combat operations at the company and platoon levels across all branches of the Army. The principal audience for this training circular is the MI company- and platoon-level leadership. Division and brigade commanders, staffs, and trainers may also use this training circular as a reference.

TC 2-19.01 will familiarize units with skillsets they have not used often in the last 20 years of stability-focused operations. The document combines key doctrinal discussions; detailed tactics, techniques, and procedures; key training concepts; field craft; and references for MI companies and platoons. TC 2-19.01 has 19 appendixes (meant as quick reference tools) covering topics that require familiarization by MI company and platoon leaders. Some topics included are—

- ◆ Obstacle considerations.
- ◆ Movement and maneuver considerations.

- ◆ Reaction drills.
- ◆ Land navigation.
- ◆ Intelligence and electronic warfare maintenance.
- ◆ Casualty evacuation.
- ◆ Cover and concealment.
- ◆ Report formats.
- ◆ Property management.
- ◆ Standard operating procedure considerations.

The Commanding General, U.S. Army Intelligence Center of Excellence, approved TC 2-19.01, and it has been submitted to the Army Training Support Center for publication. In the interim, readers can download and use the final approved draft at <https://ikn.army.mil/apps/dms/Home/GetDocument?Id=0d19a99b-a83b-4967-892e-d1be224cb30a> (common access card login required).



CSM Forum

by Command Sergeant Major Warren K. Robinson
Command Sergeant Major of the MI Corps
U.S. Army Intelligence Center of Excellence



Several years ago, while working in my office, I heard someone yelling down the hall. When I went to see what was going on, I found a major addressing a captain about his failure to accomplish some tasks. After telling the major he had a phone call in the command group, I sat with the captain and we discussed what had taken place. The captain was serving as the battalion executive officer, a key developmental position for a major. We discussed expectation management. We also talked about whether we had appropriately invested in his ability to successfully execute the duties and responsibilities of the position. This included talking about the captain's understanding of his role and ability to assist in leading the battalion into several new missions.

This brings me to the two key priorities of our Commanding General, MG Anthony Hale: *Build Leaders* and *Drive Change*. This means we must *build leaders* so that they are equipped to *drive change*. Most would agree this should be easy because we have been doing some semblance of this for years. The reality is that the events of 9/11 forced our Army to transition, almost overnight, from training for large-scale combat against a peer adversary to training for counterinsurgency. In our haste to meet this requirement, the Army lost its emphasis on a number of tasks that tied leadership and technical expertise together to meet current and future missions. MG Hale's priorities provide the focus for leaders to go back and recapture these skills.

We have to accept that leader development is no longer implied. It is common to hear senior commanders talking about the tasks they expect junior and mid-grade leaders to accomplish in order to meet their vision and end state, when in fact roles and responsibilities are not always known or understood. This problem affects all three cohorts: officer, warrant officer, and noncommissioned



officer (NCO). For example, many officers do not understand their role in training management, warrant officers believe it is their responsibility to train Soldiers, and NCOs are often unsure of their role and wait for others to lead their Soldiers. Furthermore, one entity passes responsibility to another entity without fixing the problem.

When considering how to build leaders, we must discuss the Army's three learning domains: *institutional* (institutional training and education system), *operational* (such as day-to-day operations or training conducted at home station and during joint exercises), and *self-development* (self-initiated, goal-oriented learning). The institutional domain is the initial domain in which Soldiers spend time, and it provides a baseline for the operational force, although this is mostly doctrine-centric and focuses on critical tasks that may or may not be mission-essential. Soldiers spend only about 5 percent of their career in the institutional domain, and this portion of their career only serves as a guide for overarching concepts. Soldiers spend the other 95 percent of their career in the operational force where they should develop and hone a large range of skills. Far too often, we are so involved in the daily mission that we lose sight of a multitude of developmental opportunities, whether technical or leadership-focused. Every Soldier is in the self-development domain 100 percent of the time. Self-development opportunities are not always readily available, and although reading doctrine and regulations empowers Soldiers with knowledge, the information can be dry and difficult to retain. Many times, we would rather simply listen to what our leaders tell us than actually read for ourselves to understand Army standards and operations. The primary concern is the information our leaders provide is not always correct, and the problem is exacerbated if they perpetuate inaccurate information that they heard from their leaders.

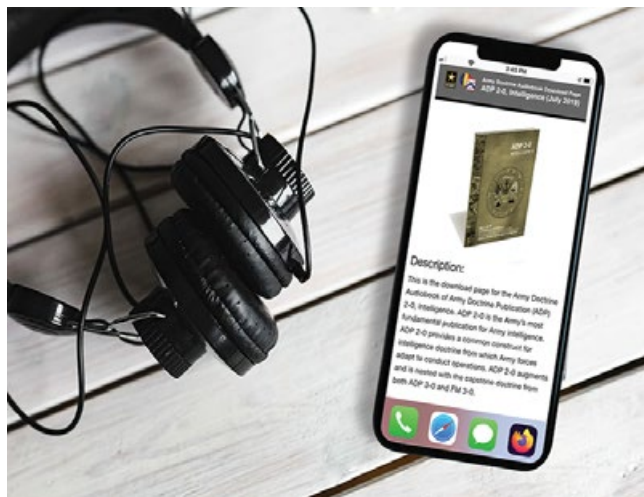
The good news is our Soldiers today are smarter than ever and can adapt quickly if only we take the time to develop them. The first place to start is with senior leaders, ensuring they know Army standards, understand doctrine, and provide clear guidance and end state. Next is defining the needed duties and responsibilities and then setting a plan on how to build other leaders. We must assess talent, determine the current capability of each individual, and define what we need that person to do in the future. From there, leaders need to deliberately plan and manage time, tasks, and priorities to facilitate each Soldier's success. We have talked about talent management, planning, and the overall management of individuals as if they

are implied, but they are not. Senior leaders need to assess each of these areas with their mid-grade leaders to ensure everyone is synchronized on standards and expectations. Again, this is another opportunity for leader development. It is imperative to inspect, rather than expect, along the way to ensure everyone maintains focus on the right outcomes.

People are our most important asset. The more we invest in them, the more return on investment we will get. If we consider our primary responsibilities of mission, Soldiers, and families, building leaders will bring success to all three. We just have to build them deliberately to prepare them to drive change. 🌟

Always Out Front!

Just Released – ADP 2-0, *Intelligence*, Audiobook



For access to the ADP 2-0 audiobook, go to –

<https://rdl.train.army.mil/catalog-ws/view/ADP2-0-Audiobook/index.html>

From this page you can listen directly from the digital library or download each chapter to your system's media player.

To access all the current doctrine audiobooks and more, go to –

<https://rdl.train.army.mil>

In the "Search The CAR" box, type in audiobook

ADP 2-0 is the Army's most fundamental publication for Army intelligence. ADP 2-0 provides a common construct for intelligence doctrine from which Army forces adapt to conduct operations. ADP 2-0 augments and is nested with the capstone doctrine from both ADP 3-0 and FM 3-0.

Audiobooks currently available

ADP 1, *The Army*
ADP 2-0, *Intelligence*
ADP 3-0, *Operations*
ADP 3-07, *Stability*
ADP 3-28, *Defense Support of Civil Authorities*
ADP 3-90, *Offense and Defense*
ADP 4-0, *Sustainment*

ADP 5-0, *The Operations Process*
ADP 6-0, *Mission Command: Command and Control of Army Forces*
ADP 6-22, *Army Leadership and the Profession*
ADP 7-0, *Training*
FM 2-0, *Intelligence*
FM 3-0, *Operations*



Technical Perspective

by Chief Warrant Officer 5 Aaron Anderson
Chief Warrant Officer of the MI Corps
U.S. Army Intelligence Center of Excellence



Teammates,

As a nation, we once again find ourselves in the midst of a transitioning global security environment, often characterized as a *great power competition* or a *long-term strategic competition*. The most recent National Defense Strategy describes the strategic environment as “an increasingly complex global security environment, characterized by overt challenges to the free and open international order and the re-emergence of long-term, strategic competition between nations.”¹

Within this security environment, the National Defense Strategy highlights China, Russia, North Korea, and Iran as actors of primary concern. These peer and near-peer challenges are the focus of this quarter’s *Military Intelligence Professional Bulletin*.

Regardless of the adversary, the battlefield of the future is sure to be more complex and more lethal, with a faster operational tempo than ever before. Without losing our collective ability to understand and execute counterinsurgency operations, military intelligence (MI) leaders must be increasingly agile, with a deep understanding of near-peer and conventional threats across all domains. We must be prepared to operate more and more in the competition phase, parsing disinformation campaigns and dealing with digital security concerns, such as “deep fakes” within a disconnected, intermittent, and low-bandwidth environment. As intelligence practitioners, we must fully understand our adversaries’ capabilities and weaknesses. This is paramount. It is also critical that we are able to provide relevant and precise intelligence to commanders in real time, affording them the opportunity to make informed decisions on the battlefield.

Our adversaries have spent several decades examining U.S. tactics, capabilities, and equipment to identify operational gaps and material weaknesses. We must now shift



our collective efforts to closing those gaps and building new capabilities to counter emergent threats. The enemies we faced in Iraq and Afghanistan generally “lacked capabilities in the form of sustained long-range precision fires, integrated air defense systems, robust conventional ground maneuver, and electronic warfare.”² Our near-peer competitors possess all these capabilities and have the ability to contest us in multiple domains while employing varying antiaccess and area denial strategies.

While neither combatant in the recent conflict between Armenia and Azerbaijan over the disputed Nagorno-Karabakh region is considered a near-peer threat, military planners would be wise to gain an increased understanding of the technology and tactics used during the fighting. According to open-source reporting, the effective use of Azerbaijani drones and drone swarm tactics played a major role in the destruction of nearly 175 main battle tanks and armor.³ According to the Director of the Security and Defense Research Program at the Istanbul-based Center for Economics and Foreign Policy Studies, Armenian forces lacked “adequate sensors, electronic warfare cover, or counterdrone weaponry” to defend against Azerbaijan’s Unmanned Aerial Vehicles (UAVs).⁴

As we anticipate this new operational environment, we must continue to increase both rigor and complexity in our training in order to gain or maintain overmatch with near-peer competitors. In order to better educate our warrant officers here at the U.S. Army Intelligence Center of Excellence, we continue to adapt our training within the Warrant Officer Training Branch, enabling all courses to deliver material relevant to large-scale ground combat operations and multi-domain operations, reinforcing both digital and analog methods in our training. These changes are critical as we work to meet the demands of tomorrow across the intelligence enterprise.

As I close out this column, I would like to thank you and your families for your daily sacrifice, selfless service, and contributions to the Army in defense of our Nation. I would especially like to recognize those MI Soldiers who are currently serving in forward locations. Your contributions to the MI Corps and Army mission are greatly appreciated. 

Endnotes

1. Office of the Secretary of Defense, *Summary of the 2018 National Defense Strategy of The United States of America*, n.d., 2.

2. Department of the Army, Field Manual 3-0, *Operations* (Washington, DC: U.S. Government Publishing Office, 6 October 2017), 1-2–1-3. Change 1 was issued on 6 December 2017.

3. Ron Synovitz, “Technology, Tactics, And Turkish Advice Lead Azerbaijan To Victory In Nagorno-Karabakh,” Radio Free Europe/Radio Liberty website, November 13, 2020, <https://www.rferl.org/a/technology-tactics-and-turkish-advice-lead-azerbaijan-to-victory-in-nagorno-karabakh/30949158.html>.

4. Ibid.

Always Out Front! and Army Strong!

ATP 2-19.4, *Brigade Combat Teams Intelligence Techniques*: The Update

by Mr. Richard Garza

Introduction

The update to ATP 2-19.4, *Brigade Combat Teams Intelligence Techniques*, describes doctrinal techniques for intelligence support to brigade combat team (BCT) operations. Last published in 2015, ATP 2-19.4 details capabilities, organizations, and structures for brigade and below intelligence elements. It also describes the latest configuration of the BCT’s military intelligence company designed to support the various requirements placed on the infantry, armored, and Stryker BCTs. The Army has since modified its foundational doctrine to reset the doctrine library to focus on large-scale ground combat operations against a peer threat. This shift in core Army doctrine and the changes to BCT intelligence capabilities, organizations, and structure were the driving forces behind the update. In order to maintain consistency with validated Army doctrine, ATP 2-19.4 covers—

- ◆ BCT intelligence support to the warfighter through the Army’s strategic roles.
- ◆ BCT intelligence support to the operations process.
- ◆ Revised verbiage to ensure consistency with operations and intelligence doctrine and terminology.
- ◆ BCT intelligence considerations such as training strategies; pre-deployment preparation; intelligence architecture; primary, alternate, contingency, and emergency (also known as PACE) communication planning; collection management; and targeting.

Development

The development team collaborated with personnel from multiple intelligence organizations within and outside the U.S. Army Intelligence Center of Excellence (USAICoE) to develop the Army techniques publication throughout 2020. Those organizations within USAICoE included the Requirements Determination Directorate (RDD), Force Design, Information Collection Planner’s Course (ICPC), and Lessons Learned. The primary personnel outside USAICoE included instructors from the Digital Intelligence Systems Masters Gunners Course (DISMGC). Personnel from DISMGC, ICPC, and RDD assisted by providing input to the publication’s intelligence architecture appendix. The exhibited collaboration was a beneficial side effect of the coronavirus disease 2019 work environment that turned into a doctrine best practice.

ATP 2-19.4 underwent two worldwide staffings, including senior leadership reviews, which produced approximately 600 comments requiring adjudication. The collaborative development of the publication is a testament to the commitment—from doctrine leadership, the development team, and the force at large—to create unique doctrine that is both relevant and timely with the goal of enhancing the readiness of the force. We anticipate final publication of ATP 2-19.4 in mid- to late-spring 2021. 

Ensuring a Seamless Army Narrative for the Operational Environment: Roles and Responsibilities of U.S. Army Training and Doctrine Command and Army Futures Command

U.S. Army photo by CPT Chelsea Hall



Soldiers from 12th Infantry Regiment, 2nd Infantry Brigade Combat Team, 4th Infantry Division, conduct explosive breaching using Bangalores during a platoon live-fire exercise, August 14, 2019, on Fort Carson, CO.

by Colonel Jimmy Blejski and Colonel Rob Wagner

Introduction

As the U.S. Army transitions from an era marked by extended counterinsurgency operations in the Middle East and South Asia and reorients on great power competition and conflict, the need to understand and assess the operational environment (OE) becomes an essential task. This is not the first time the Army has addressed a critical transition; it has happened before—at the end of World War II, after Vietnam, and at the end of the Cold War. The Army has a long history of adapting to change and preparing Soldiers, leaders, and formations for the “next war.” Indeed, assessing who our next threat is, analyzing each event or series of events that could be the catalyst for war, and preparing to operate successfully in each environment wherever we will face our next foe is what keeps intelligence professionals up at night.

Maintaining a Competitive Advantage throughout History

A quick scan through the U.S. Army’s 245 years of existence shows that our focus on potential threats has included both state and non-state actors with various degrees of capabilities. As the Global War on Terrorism started to wind down, the Department of Defense began prioritizing efforts for the next conflict. Over the past 20 years, American Service members and the national intelligence community became well versed in fighting a counterinsurgency against non-state and state-sponsored adversaries while defeating terrorist threats to the United States. However, the required shift in the 2018 National Defense Strategy evolved with the focus toward larger, more dangerous threats, particularly by our peer competitors, China and Russia. To maintain our competitive advantage over our increasingly lethal and

most capable threats, the U.S. Army must carefully modernize and continue to improve in all facets of the doctrine, organization, training, materiel, leadership and education, personnel, and facilities (DOTMLPF) framework. Two major Army commands have the important mission of helping to execute many of the complex tasks associated with preparing the U.S. Army to fight and win throughout the competition continuum.

Preparing the U.S. Army to Win the Next Conflict

Since the end of World War II, the Army has conducted several studies to review the command and control of Army ground forces within the continental United States, while assigning responsibilities for the critical functions of training, doctrine, leader, concepts, and capabilities development. The first major reorganization occurred in 1955, with the establishment of the Continental Army Command (CONARC). However, it became apparent that this formation had too large a span of control and too broad a focus. In 1973, as a result of an analysis from Operation Steadfast, CONARC was deactivated and divided into two new formations.

One formation became the U.S. Army Forces Command, which was responsible for the Army's active and reserve component combat and combat support elements in the continental United States. The second formation was the U.S. Army Training and Doctrine Command (TRADOC), which combined Service schools and individual training functions with the combat developments processes of a separate command, the Combat Developments Command. This integrated the development of doctrine and related equipment for the Army with the Service schools and functional training where it logically belonged.¹

Exactly 45 years later, after the publication of a revolutionary new National Defense Strategy, the Army decided it would require a renewed focus on the future and force modernization to ensure the transition to great power competition against near-peer and peer rivals, who are engaged in their own significant military modernization efforts. Thus, much like the decision in 1973 to establish TRADOC, the Army made the bold decision to establish U.S. Army Futures Command (AFC) effective 1 July 2018.² The establishment of AFC required the Army intelligence enterprise to create a new approach to understanding and assessing the OE that would continue to meet the needs of supporting training and doctrine, while at the same time adapting to the new demands inherent in AFC's mission. With regulatory oversight, policy, and support from the Headquarters, Department of the Army, G-2, and general support from the greater Army intelligence enterprise and intelligence community, TRADOC and AFC are responsible for describing and

The History of CONARC and Operation Steadfast

The establishment of the Continental Army Command (CONARC) combined the command and control of all active units and all training functions in a single headquarters.³ In 1962, during the height of the Cold War, another study broadened CONARC's mission and responsibilities to include all training centers, schools, and doctrine development. A result of the study also centralized all materiel functions in the Army under the Army Materiel Command and created the Combat Developments Command responsible for combat developments and concepts. By the early 1970s, with the de-escalation of U.S. participation in Southeast Asia and the necessary changes to the Army structure in the continental United States, it was evident that the span of control for CONARC was too large for a single headquarters.⁴ The Chief of Staff of the Army, GEN Creighton W. Abrams Jr., ordered another study, Operation Steadfast, as part of an overhaul of the entire U.S. Army structure. Orchestrated by Assistant Vice Chief of Staff, LTG William E. DePuy, Operation Steadfast resulted in the deactivation of CONARC on 1 July 1973 and the establishment of two new organizations in its place—U.S. Army Forces Command and U.S. Army Training and Doctrine Command.



This repository is part of the U.S. Army Training and Doctrine Command (TRADOC) Historian's archives at TRADOC Headquarters, Fort Eustis, VA. It depicts the volumes of data that went into Operation Steadfast and chronicles several previous studies.

Prelude to Operation Steadfast: A Timeline

- ◆ 1942, Army Ground Forces.
- ◆ 1948, Office of the Chief of Army Field Forces.
- ◆ 1955, CONARC.
- ◆ 1962, Project 80 reorganization.
- ◆ 1969, Parker Board.
- ◆ 1970, CONARC Management Improvement Panel.
- ◆ 1972, Establishment of Operation Steadfast.

delivering a consistent narrative spanning the current and future OE. The continuity of an OE narrative prevents disconnects between TRADOC's leader development, training, education, and doctrine; AFC's concepts and capabilities development; and all other Army-wide DOTMLPF missions.

Since its establishment, TRADOC has focused on leader development, training, education, doctrine, concepts, and capability development. The merging of these functions in 1973 was intended to ensure a holistic approach to an evolving Army ready for the challenges of the future. Many examples illustrate the impact and long-lasting effects TRADOC has had on the Army. TRADOC's efforts in training and leader development led to the creation of the combat training centers and Mission Command Training Program to ensure our leaders are prepared for their next threat. Its efforts in concepts and capabilities development led to the fielding of the "Big Five" combat systems, which have been steadily upgraded and are still dominant today against all adversaries.

The "Big Five" Combat Systems

In the 1970s and 1980s, the U.S. Army embarked on a series of procurement programs designed to revitalize the force, and to counter the overwhelming numerical advantage of the Warsaw Pact. The "Big Five" represented a collection of procurement programs designed to re-establish the technological supremacy of U.S. land forces, and reinvigorate conventional capabilities in the wake of the Vietnam War. These systems, including the M1A1 Abrams main battle tank, the Bradley Fighting Vehicle, the Patriot air-defense system, the AH-64 Apache attack helicopter, and the UH-60 Black Hawk utility helicopter, continue to provide the foundation of U.S. military landpower.⁵

TRADOC continues to record key observations and assessments of friendly and threat actions during all stages of competition, crisis, and conflict worldwide to produce relevant doctrine for the U.S. Army. One of the best and most recent examples of how doctrine, combined with concepts and capabilities development, was applied and executed with overwhelming success is the 1980s *AirLand Battle*. The Army first circulated FM 100-5, *Operations*, in 1981, and then carefully taught, trained, and exercised it throughout all institutional and operational structures with the sole objective to defeat the large combat formations of the Soviet Union in a potential conflict in Europe. This strategy was convincingly proven in the deserts of Iraq and Kuwait during Operation Desert Storm in 1991. More recently, FM 3-24, *Insurgencies and Countering Insurgencies*, provided a blueprint for United States Army operations in Iraq and Afghanistan, turning the tide into a more successful strat-

egy. Both of these doctrinal publications set the foundation for U.S. Army training, education, leader development, and force changes that acknowledged "the distilled wisdom" of combat captured in doctrine.

The realization that our peer competitors possess the intent and capability to challenge us in competition and conflict, combined with the realization that the current way of modernizing the Army was not going to keep pace, Army senior leaders decided to establish one command focused on modernization. The 2018 National Defense Strategy, highlighting Russia's and China's modernization activities, drove the Army to focus on threat-based modernization rather than capability-based modernization. The importance of maintaining overmatch in key warfighting functions and advancing key technologies is forcing the Army to look deeper both into the current threat and into the deeper future, including potential alternative futures. It immediately became apparent to TRADOC and AFC leadership that both organizations must work together to reach the desired end state of fielding a multi-domain operations-capable force that can prevail against our pacing threats in competition and conflict. It also became apparent that the first step in the process was the establishment of a close and effective working relationship between the elements of TRADOC and AFC tasked with understanding the OE. Two years since the historic decision to create a new command, the TRADOC and AFC relationship has matured as we continue to ensure consistency in the current OE and the future OE for the U.S. Army.

Roles and Responsibilities of the TRADOC G-2

Today, TRADOC—

- ◆ Recruits, trains, and educates the Army's Soldiers.
- ◆ Develops leaders.
- ◆ Supports training in units.
- ◆ Develops doctrine.
- ◆ Establishes standards.
- ◆ Builds the Army by developing and integrating operational and functional concepts and organizational designs for the fielded force.⁶

Within this structure, one of TRADOC's core functions under the TRADOC G-2 purview is the oversight and development of the Army's current OE. Specifically, the TRADOC G-2 is responsible for developing, describing, and delivering the current OE to support the Army's preparations to fight and win the Nation's wars. TRADOC accomplishes this by integrating support and fostering collaboration with Army and unified action partner stakeholders and partners from the intelligence community, academia, and industry.

The TRADOC G-2 has historically produced a suite of products that not only outlines lessons learned, threat tactics, and assessments of particular OEs but also provides forecasts 10 to 15 years into the future in a series of OE estimates. The most recent estimate is *The Operational Environment and the Changing Character of Warfare*, released initially in 2018 and officially published as TRADOC Pamphlet 525-92 in October 2019. This document provides a concise overview of trends and emerging threats the Army will confront from our strategic competition in an increasingly contested battlefield across every domain. The intent of the TRADOC G-2's work is like all organizational intelligence organizations—to inform the commanding general's decisions. In this case, it informs decisions about the azimuth for training, leader development, education, and changes needed for the fielded force to deal with near-term threats and circumstances.

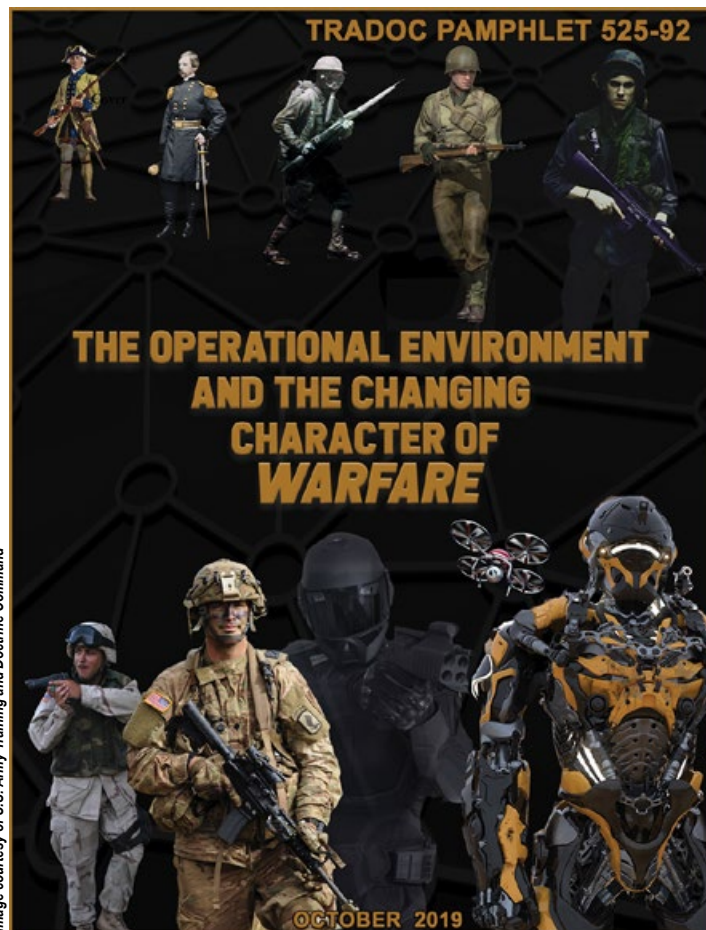


Image courtesy of U.S. Army Training and Doctrine Command

Once those decisions are made, the TRADOC G-2 develops and delivers OE content to support those decisions across the U.S. Army. The threat tactics Army techniques publications, the opposing force manuals (TC 7-100 series), and the decisive action training environment series are examples of this work. The TRADOC G-2 actively maintains and updates these references for relevancy. They play a critical

role in ensuring the threat is accurately replicated through the accreditation of the opposing force at the combat training centers and Mission Command Training Program, and indirectly throughout all home station training. Additionally, the TRADOC G-2 is a key advisor throughout the training and education's program objective memorandum discussions and budget cycles affecting Army readiness and modernization investments.

Roles and Responsibilities of the AFC Directorate of Intelligence and Security

As outlined in AGO 2018-10, *Establishment of United States Army Futures Command*, AFC leads the Army's future modernization enterprise. Specifically, AFC—

- ◆ Assesses and integrates the future operational environment, emerging threats, and technologies to develop and deliver concepts, requirements, and future force designs.
- ◆ Supports the delivery of modernization solutions.
- ◆ Postures the Army for the future by setting strategic direction.
- ◆ Integrates the Army's future force modernization enterprise.
- ◆ Aligns resources to priorities.
- ◆ Maintains accountability for modernization solutions.⁷

In AGO 2018-10, AFC's first task was to describe and assess the future operational environment and emerging threats, looking 15 to 30 years into the future to design the next Army. The command set out on a path to undertake an early and continuous assessment of the future operational environment and to closely monitor future threats. AFC is leading a transformation of Army modernization in order to provide future warfighters with the concepts, capabilities, and organizational structures they require to dominate a future battlefield. This involves thoroughly examining the future operational environment and assessing how our adversaries will fight. The first publication of the AFC future operational environment is AFC Pamphlet 525-2, *Future Operational Environment: Forging the Future in an Uncertain World, 2035-2050*. This document describes four alternative futures based on two key drivers—the concentration of power and the rate of technology adaptation.

The AFC Directorate of Intelligence and Security (DoIS) orchestrates activities throughout the intelligence and security communities to describe and assess the future operational environment and protect the Army's investments. The future is inherently unknowable and difficult to forecast. To provide the Army modernization enterprise with strategic

FUTURE OPERATIONAL ENVIRONMENT: FORGING THE FUTURE IN AN UNCERTAIN WORLD

2035-2050



"The Future Operational Environment will force us to think differently and seek opportunities in nontraditional space. If we do not imagine large and reach deep, we will not be successful in future battlefields."
-General John "Mike" Murray

U.S. ARMY FUTURES COMMAND

DISTRIBUTION STATEMENT A.

This document is approved for public release; distribution unlimited.

Image courtesy of Army Futures Command

intelligence estimates that look into the deep future, DoIS works collaboratively with the intelligence community, academia, think tanks, and other Department of Defense organizations to develop a series of products supporting the decision cycle of Army modernization. For example, DoIS leads a monthly session for AFC's Commanding General, focusing on a specific intelligence topic that describes what activities and investments our adversaries are making now to gain overmatch in the future. DoIS shapes future investments by anticipating and identifying emerging threats as they evolve. These efforts confront the loss of overmatch to a range of peer, near-peer, and non-state actors.

AFC DoIS provides critical threat intelligence to Army modernization efforts, prioritizes technology protection strategies, integrates intelligence and requirements, provides security guidance and oversight, and informs modernization investment strategies. DoIS coordinates a shared, and validated, threat picture that supports Army modernization. This is done by developing and understanding potential future operational environments, reviewing intelligence products for the Army Requirements Oversight Council and the Strategic Portfolio Analysis and Review, and driving the publication of relevant Validated Online Lifecycle Threat products. DoIS also operates closely with the testing and

modeling and simulation communities to ensure the developers of systems evaluation capabilities and concepts pursue future Army systems in direct response to realistic and adaptive future threats.

Beyond intelligence, DoIS implements protection and security requirements in support of Army modernization, and directly supports the Army's transformation to a threat-based force. To achieve and maintain overmatch, AFC DoIS provides guidance and oversight with intelligence, protection, and security elements working together to shield intellectual property, key technologies, and specific program details as part of a systematic effort. Maintaining speed and agility requires situational awareness of various security threats and a better understanding of specifically what, and when, to protect. Because of limited resources, these security and protection tasks are only accomplished with rigorous engagement, partnership, and coordination with the whole community of security-focused organizations.

Collaborative Relationships, Consistency, and the Way Ahead

Today, the TRADOC G-2 provides support to training and readiness, leader development, education, doctrine development, and fielded force integration for the Army. TRADOC G-2's role in this effort is to develop current OE forecasts and content, and to develop and maintain baseline and supporting functional and regional OE assessments. These products and services inform fielded force integration; synchronize with AFC's future operational environment work for concepts, capability development, and related activities; and support the establishment of representative conditions for individual and collective training across the Army. These functions underpin how the Army organizes, trains, equips, and operates in the near- and mid-term, and they assist the Army in developing the "Waypoint Force" that describes an Army of 2028. The Waypoint Force is a comprehensive initiative that merges near-term needs by operational forces and provides the platform to achieve the "Aimpoint Force" of 2035. Key to this effort is satisfying the near-term needs for Army forces while not creating evolutionary dead ends that would squander resources in moving to the Aimpoint Force. This ensures that OE content provides the complex OE foundation to foster internal Army warfighting functions, combined arms, and joint and multinational force integration.

To ensure the continuity of the narrative describing the OE and threats, both current and future, AFC DoIS and TRADOC G-2 continuously collaborate on intelligence products. As the current threat transforms and modernizes into the threats of the future, it is critically important for the fielded

force to understand what threats it will face in the near future. It is just as critical for the future force to understand what potential future environments and threats it will face and to prepare early to operate in those environments and counter those threats.

The TRADOC G-2 and AFC DoIS have the challenging task of assessing current capability gaps caused by threat activities and changes to the OE, while also working through the Army's complex force management process. At the same time, they must keep an eye toward the future. Forecasting the future is not designed to describe "what will be" but rather to project "what could be" the future conditions the Army might face. One will not ever get it right, but the challenge is to be close. To quote a great American philosopher, Yogi Berra, "The future ain't what it used to be." 

Endnotes

1. Jean R. Moenk, *Operation STEADFAST Historical Summary, A History of the Reorganization of the U.S. Continental Army Command (1972-1973)* (Fort McPherson, GA: U.S. Army Forces Command, 1974).
2. Department of the Army, General Orders (AGO) 2018-10, *Establishment of United States Army Futures Command* (Washington, DC, 4 June 2018), 1.
3. Moenk, *Operation STEADFAST*.
4. Ibid.
5. Robert Farley, "What if the U.S. Army's 'Big Five' Weapons Programs Had Failed?" National Interest website, September 1, 2018, <https://www.yahoo.com/news/imagine-army-never-built-m1-140000807.html>.
6. Department of the Army, AGO 2018-10, *Army Futures Command*, 2.
7. Ibid., 1.

COL Jimmy Blejski serves as the Deputy Director of Intelligence and Security of the U.S. Army Futures Command. His previous assignments include Assistant Chief of Staff, G-2, for the 18th Airborne Corps; Department of the Army staff; and numerous assignments in the Special Operations community, including battalion-level command. He is a graduate of the National War College, the Naval War College, and The Citadel.

COL Rob Wagner serves as the Military Deputy G-2 of the U.S. Army Training and Doctrine Command. His previous assignments include various tactical through strategic intelligence positions in 4th Infantry Division, U.S. Army Human Resources Command, U.S. Army Intelligence and Security Command, North Atlantic Treaty Organization, and U.S. Africa Command. He commanded the Nashville Recruiting Battalion, and he is a graduate of the Naval War College and the University of Texas at Arlington.

The Military Intelligence Training Strategy (MITS) series of publications are available for download from—



APD | ARMY PUBLISHING
DIRECTORATE

1. The Army Publishing Directorate at <https://armypubs.army.mil/>,
then - Publications - Doctrine and Training - Training Circulars

-or-



Directorate of Training

Customer Focus | Products & Outreach | Development & Integration | Educational Design & Development | Training the Team

2. The Intelligence Knowledge Network (IKN) at <https://ikn.army.mil/apps/dot> select "MI Training Strategy (MITS)" link on the left side of the page.

Select "Links" under the MITS banner at the top of the page to access the training circulars plus a variety of other related resources.

Future Operational Environment and Emerging Threats



DIPLOMATIC



MILITARY



INFORMATION



ECONOMIC



by the Future Operational Environment Directorate, Futures and Concepts Center;
and the Directorate of Intelligence and Security, U.S. Army Futures Command

Introduction

This article discusses plausible possibilities of what the future operational environment could look like for the U.S. Army in 2050. It is a running baseline that provides a systematic/analytical framework for follow-on analysis. It assumes that the future operational environment will be a definable state by 2050 and that the state will not be in a period of transition. It is intended to be the basis for Army deliberation and decision making about concepts, capabilities, force design, and science and technology investments. The goal is to aid creative thinking about “the realm of the possible” and to generate topics for follow-on rigorous intelligence analysis based on Army modernization priorities.

Using the first two steps of the intelligence preparation of the battlefield process—to define the environment and to describe the effects of that environment on operations—we created four alternative futures that will underpin future concepts, and we developed an analysis of sociological, technological, environmental, economic, and political trends. The intent is to focus concept development to generate Army strategies designed to secure future readiness. By anticipating the future, the Army will gain time to prepare and posture to adapt to change.

Structural Trends

Structural trends, both global and defense, are variables in a future landscape. Global trends that affect the shaping of the proposed four futures are—

- ◆ Global environmental change.
- ◆ Shifting energy markets.
- ◆ Enhanced and novel infectious diseases.
- ◆ Demographic changes.
- ◆ Challenges to domestic governance and legitimacy.
- ◆ Non-state actors.
- ◆ Defense developments.

Defense trends include—

- ◆ Artificial intelligence.
- ◆ Additive manufacturing.
- ◆ Nanotechnology.
- ◆ Advanced biotechnology tools.
- ◆ Leaps in energy storage and performance.

Key Factor 1: Concentration of Global Power

The four future alternative scenarios are framed by two interdependent key factors, the first of which is the concentration of global power.

Bipolar System. In this type of world order, the majority of global diplomatic, informational, military, economic, and cultural influence is held between two states. Relations between the two “superpowers” might range from being intensely competitive to cooperative, or be somewhere in between (*détente*). Although parity and potential economic interdependencies would lower the risk of large-scale conflict between the two states, protracted zero-sum competition would be very likely.

Concentration of Global Power

- ◆ Bipolar System—Superpowers
- ◆ Multipolar System—Security Alliances

Global Technological Innovation

- ◆ Evolutionary—gradual, incremental, and continuous improvement
- ◆ Revolutionary—rapid, leap-ahead improvement

Factors Influencing Alternative Futures

Threats in this future would also emerge from second-tier states and regional powers. These states may pursue their own interests by allying with one of the superpowers or forming coalitions within themselves. Regional rivalries among competing states could draw the United States into localized disputes, especially if they threaten U.S. access to resources.

Multipolar System. Alternatively, the concentration of global power may be more widely distributed across three or more actors, including non-state actors. Multipolar systems are more likely to result in the formation of security alliances: the absence of outsized diplomatic and military “checking” influence of hegemonies may raise mutual fears among near-peer competitors and, therefore, preemptive coalition building.

Key Factor 2: Global Technological Innovation

The second interdependent key variable that frames the four future scenarios is global technological innovation.

Technology advancements and the diffusion of that technology will play a crucial role in shaping future competition and conflict. Because breakthroughs remain unpredictable and nonlinear, the future state of technology will remain uncertain. Our alternative futures consider two broad trajectories—“evolutionary” and “revolutionary” technological innovation. Most innovations are considered *evolutionary*, consisting of gradual, incremental, and continuous improvements to existing concepts and systems. *Revolutionary* innovations, on the other hand, result in rapid, leap-ahead improvements to existing concepts and systems, or even completely new ways of solving problems, potentially transforming markets and economic activity.

Public-Private Incentives. Technological trends largely depend on the interaction of global public and private investments in basic and applied research. Innovation trends will track public and private incentives to invest in more predictable and incremental improvements to existing technologies to solve current and emerging problems rather than more unpredictable, risky, leap-ahead technologies. Some technologies envisioned for the future, even if successfully demonstrated in a laboratory or by prototype, may not be cost-effective to scale.

Excludability and Diffusion. Many investment decisions hinge largely on the “excludability” of innovations, i.e., whether conditions limit knowledge diffusion and confer first-mover advantages. Under such scenarios, developers enjoy monopolies, ideally for periods of time sufficient to cover investment costs. Military research and development programs may be a source of such innovations. These programs may be exceedingly expensive for commercial investment or highly complex relative to commercial applications—especially if necessary components or data are unavailable on commercial markets—and will thereby preclude emulation.

If, instead, innovations are diffuse, then investments in leap-ahead technologies and systems will be discouraged by a second-mover advantage in which competitors can avoid incurring sunk research and development costs. This kind of diffusion can occur because of increasingly sophisticated communications technologies and dense information networks, widespread commitments to open-source development, plausible reverse engineering and mimicry, and economic and intellectual espionage and theft. It can also occur in situations in which breakthroughs have significant profit potential and are rapidly commercialized.

Adoption Capacity. The relative influence of technological inventions and innovations is limited by the state’s educational system, the industrial base available to serialize production, and the military’s adoption and use.

The Alternative Futures

The aforementioned framework resulted in four distinct alternative futures:

- (1) a bipolar system with revolutionary technological innovation,
- (2) a multipolar system with revolutionary technological innovation,
- (3) a bipolar system with evolutionary technological innovation, and
- (4) a multipolar system with evolutionary technological innovation.

In this article’s descriptions, attention is devoted primarily to the consequential futures of greatest concern to the Army that would consume the most resources and without a guaranteed positive outcome.



Alternative Future Number 1: The New Cold War

Alternative Future Number 1: The New Cold War. In this potential future, the United States and China compete to achieve global supremacy. In doing so, competition will dominate the United States–China relationship. Superpower competition will drive global trade and diplomacy. Competition will not necessarily be ideologically based but rather will focus on a systemic struggle between liberal democracies versus authoritarian, centralized regimes. An intense focus will be on access to the markets, commodities, and global commons. In this future, the United States and China may cooperate on less contentious issues like counter-piracy, disaster relief, and terrorism.

Global economics will be heavily influenced not only by traditional factors such as trade agreements and technology transfer but also by digital trends in cryptocurrency. To enable its global economic aspirations, China invests heavily in disruptive technologies. China uses these technologies to gain economic and military advantages over the United States in sectors like space, biotechnology, and quantum computing. Access to and control of information will continue to be a strategic commodity. Adversaries will use data analytics to manipulate personal information to target individuals in the information domain. Disinformation campaigns will favor the offense and the actor who best dominates and controls the narrative.

Since advanced weapons and economic interdependencies will likely deter the two superpowers from engaging in large-scale conventional warfare, the powers will engage in a series of proxy wars around the world. Conflict and competition will likely occur in dense urban environments that will involve elements of the U.S. Army.

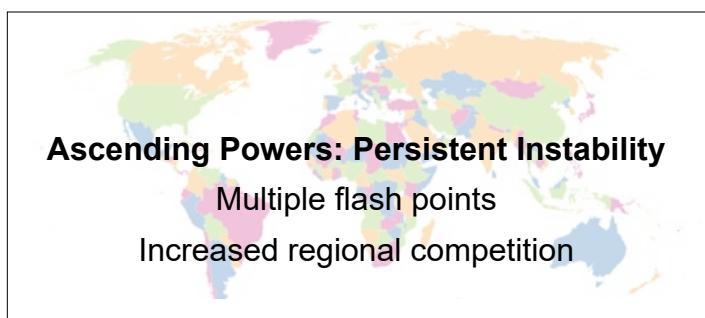
China continues its military growth and modernization efforts by developing and fielding advanced technologies. The People’s Liberation Army, the regular armed forces of the People’s Republic of China, continues to exploit the space and cyberspace domains and is increasingly proficient in semi-independent maneuver, extended expeditionary capabilities, hypersonic and supersonic missiles, advanced long-range precision fires, and directed energy weapons.

The People’s Liberation Army’s Strategic Support Force has the capabilities to target U.S. logistics systems and installations and impede U.S. naval and expeditionary maneuver by cyber-directing autonomous merchant traffic into congested sea lines of communication and port facilities. To erode any United States-backed defense coalition, China is able to use economic warfare instruments to drive a wedge through United States alliances by threatening American partners with economic isolation if they do not agree to favorable security pacts and trade agreements with Beijing instead.

Total war between the superpowers is not likely but is possible. If the United States secures a limited capability that China does not have, Beijing may feel compelled to act before the United States has a chance to field the system. Alternatively, if China develops a niche capability, it may also feel bound to act first to maintain its advantage. Total war could also result from misperceptions or an unexpected escalation of hostilities.

In this future, threat projection will be geographically predictable and centrally focused on one peer adversary. The Army must consider how threats could manifest in a number of ways. The introduction of nuclear-capable hypersonic/supersonic missiles launched from various platforms truncates response time and, coupled with ambiguity of origin, increases the probability of miscalculation. Digital maneuver capability (cyberspace defense/attack, virtual power projection, and digital information operations), increased robotics and autonomy, and attacks on critical infrastructure and sustainment systems are increasingly important to achieve the advantage in military operations. Protection capabilities will require the adoption of system-level defense strategies like multidimensional protection, the inclusion of critical civilian infrastructure, and the reemergence of capabilities such as biodefense (pandemic response), economic warfare, and information control.

Alternative Future Number 2: Ascending Powers. This future is marked by persistent instability and conflict with “revolutionary” technological innovation. The transition to this world is marked by considerable unrest, which is exacerbated by the threat of highly disruptive, revolutionary military technologies. The long-running political and economic struggles between the United States and China now result in economic stagnation, while emerging powers leverage decades of liberal economic order to consolidate wealth critical to their military power. Economically, this future experiences an economic rebalancing that shifts power away from a Western rules-based global banking environment toward systems dependent on foreign currencies and



Alternative Future Number 2: Ascending Powers

cryptocurrencies. In this future, regional powers will check each other to maintain a relative balance and prevent the rise of any one power. Several actors (for example, United States, China, Russia, India, and Europe) constantly face “balancing” forces from one another and from other aspirational powers. In doing so, actors expend valuable resources in a protracted struggle for dominance and advantage.

A number of states expend valuable resources, including military power, in a protracted struggle to gain advantage. In the absence of a global superpower to mitigate conflict escalation, competing security coalitions and the race for resources create persistent levels of conflict between states. At the same time, the disintegration of power within states fuels social unrest and insurgencies, which are increasingly lethal as non-state actors secure advanced weapons systems and external powers entangle themselves in local wars as a way to challenge rivals.

Diplomacy in this alternative future is no longer dominated by the interests of two global superpowers, transforming instead into a highly dynamic—and, at times, brittle—system conforming to the interests of many more peer and near-peer states. Moreover, because technological innovations emerge from multiple actors in this alternative future—not from only two superpowers—states will use technology diffusion to serve their interests, leveraging highly valuable, exclusive revolutionary technologies as diplomatic centerpieces.

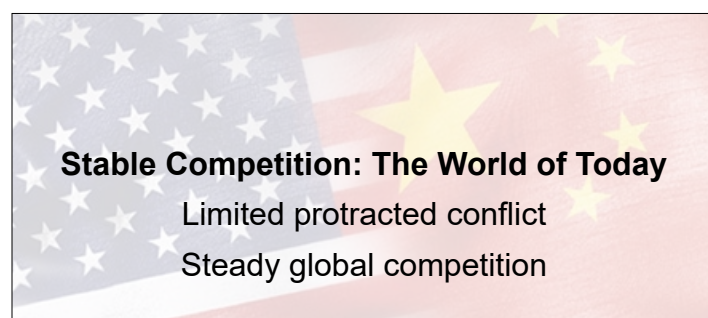
In this alternative future, threats are geographically unpredictable, occur across multiple domains, and are dispersed widely among numerous adversaries with varying degrees of temporary overmatch and intentions. The U.S. Army is forced to engage in many types of conflict, perhaps simultaneously, in which Soldiers face a range of highly capable adversaries—from conventional forces to insurgents, as well as transnational criminal organizations, mercenary armies, and proxy forces. Due to heightened international competition and the primacy of security coalitions, the U.S. Army acts as a secondary player in many conflicts, with allies taking the lead on grounds of national interests or niche technological leadership. Alliances are critical to shore up U.S.

defense and strike capability, deter economic aggression, and mitigate distributed information warfare campaigns.

Alternative Future Number 3: Stable Competition. In many ways, this alternative future resembles the world of today. In it, enduring economic and political effects of successive global pandemics cause the United States to lose its position as the sole superpower, while China ascends to superpower status on the back of its thriving economy.

China continues to disperse its economic production activities globally to its spheres of influence, challenging United States multinational corporations. China guarantees the manufacture of military, medical, and supplies vital to national security through domestic means or from trusted bilateral partners. China continues to invest heavily in leading-edge technologies. The Communist Party places the highest priority on any investment that maintains wealth generation critical to its legitimacy.

The pace of technological advancement results in marginal change to the deployment speed and lethality of military systems, moderating fears among competitors and lowering the risk of preemptive strikes in reaction to perceived military gains. Military parity and continuing economic interdependencies between China and the United States are deterrents to large-scale conventional warfare. In the unlikely event of large-scale conflict, however, Chinese forces would rely on legacy systems—perhaps employed in novel ways—or marginally disruptive technologies involving artificial intelligence and autonomy.



Alternative Future Number 3: Stable Competition

China attempts to conduct covert economic and financial warfare against the United States—including artificial intelligence-enabled malware and ransomware attacks against commercial, defense-logistics, public-infrastructure, and installation targets—in order to undermine United States military capability and achieve marginal economic advantages. However, the evolutionary pace of technological change allows sufficient time for potential targets to develop reliable countermeasures, undermining China’s ability to attack in non-attributable ways.

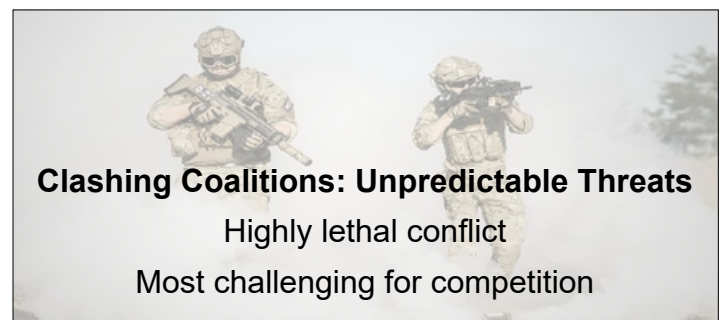
In an emerging bipolar world, lower-tier states pursue bilateral relationships and economic and security blocs increasingly aligned to Chinese economic, diplomatic, and military interests, as well as parochial pacts with whoever best affords security and economic opportunities. China plays a more active role in leading the international order, partly through its participation in key international institutions. It seeks to lead on emerging technological standards and agreements but otherwise continues to weaken international norms of human rights and political freedoms, transparency, and accountability. Many of China's international relationships will be transactional in nature.

In this alternative future, the United States military must prepare to confront a familiar array of challenges such as Chinese military modernization and expeditionary operations, increased Russian proxy warfare and land-grabs in Europe and Central Asia, Iranian and North Korean nuclear development, and the ever-present threat of insurgency and terrorism. It will do so within a system of degraded alliances.

Alternative Future Number 4: Clashing Coalitions. In this alternative future—a multipolar system with an “evolutionary” rate of technological innovation—rising and declining states compete with one another, regional rivals, and even non-state actors for resources and global influence. A protracted era of globalization—including free trade, investment, and labor-flow regimes—has been a central feature of the leveling dynamic, producing several regional hegemonies. Any moves toward protectionism or bilateral or regional trade exclusivity will undermine economic stability; therefore, such behavior is rare. Partial defections from the current globalized economic order occur in limited situations in which ascending regional powers challenge the standing of their respective regional hegemonies. Because ascending powers are incapable of acquiring truly provocative “leap-ahead” capabilities, this kind of event is uncommon.

In order to maintain wealth generation critical to military power, all regional hegemonies invest heavily in domestic infrastructure and human capital. Furthermore, these states continue to support the private engines of their economies, facilitating the dispersal of economic production activities globally. Multinational corporations wield significant political-economic influence. In this environment, first-mover advantages are marginal and fleeting, except where actors are able to maintain periods of excludability around highly marketable marginal innovations or novel convergences of existing technologies.

The evolutionary pace of technological innovation does not produce large military disparities among competitors, or the corresponding atmospheres of uncertainty and fear.



Alternative Future Number 4: Clashing Coalitions

Lower-tier states can band together to force the negotiation of institutions over which regional hegemonies attempt to maintain disproportionate sway. Acute diplomatic disputes and sporadic military conflict may occur over access to critical, ever-dwindling natural resources. Furthermore, there is a heightened risk that states will misinterpret the increasingly complex network of mutual “red lines,” or the extent to which a competitor will go to defend their interests.

In a world of evolutionary technological innovation, strategies of discreet, marginal improvements to one's relative economic and military standing—including through impeding competitors' progress—are particularly effective. Many regional hegemonies conduct covert economic and financial warfare against adversaries' commercial, defense-logistics, public-infrastructure, and installation targets.

As in the multipolar alternative future with “revolutionary” technological innovations, threats in this world are geographically unpredictable, occur across multiple domains, and are dispersed widely among numerous adversaries with varying intentions. The U.S. Army has to engage in many types of conflict, perhaps simultaneously, in which its Soldiers face a range of highly capable adversaries.

Conclusion

These alternative futures are neither definitive nor all-inclusive. Regardless of whether the United States finds itself in a bipolar system or a multipolar system, the trends suggest that the Army should prepare itself for a range of threats in a world where the United States is no longer the sole superpower.

The intent of this article was to generate critical discourse among Army and Department of Defense senior leaders about the future, implications for the Army, and requisite investments in concepts, technology, materiel, and training. As a next step, a future operational environment running-estimate will explore various key topics in order to challenge and enrich the descriptions in this article. The information presented here should be taken as the first word, not the last, in preparing to think about how to fight, win, and forge the future. 🌟

The Future Operational Environment Directorate, Futures and Concepts Center, assesses the threat and future operational environment. It also develops future concepts, requirements, and an integrated modernization pathway to increase lethality and overmatch to enable Soldiers and units to compete—and, if necessary—deploy, fight, and win future wars.

The Directorate of Intelligence and Security, U.S. Army Futures Command, orchestrates the evaluation and assessment of current, emerging, and future threats and the development of the operational environment; synchronizes multi-disciplined technology protection activities; and conducts intelligence and requirements integration for the Future Force Modernization Enterprise to build a multi-domain operations (MDO)-capable force by 2028 and an MDO-ready force by 2035.

Check out the Army Futures Command's new AFC Pamphlet 525-2, *Future Operational Environment: Forging the Future in an Uncertain World 2035-2050*!



The publication is available at: <https://community.apan.org/wg/tradoc-g2/mad-scientist/b/weblog/posts/check-out-the-army-futures-command-s-new-afc-pamphlet-525-2-future-operational-environment-forging-the-future-in-an-uncertain-world-2035-2050>

Training the Operational Intelligence Force: On Target for Military Intelligence Readiness in 2022

by Colonel Timothy J. Parker

U.S. Army photo by SGT Melissa N. Lessard

A Soldier with 163rd Military Intelligence (MI) Battalion, 504th MI Brigade, pulls security while conducting a certification exercise for their MI platforms, March 20, 2019, at Camp Bullis, TX.

As I've listened to commanders talk about readiness, there's concern we haven't spent enough time truly mastering the basics. It's not fair to compare our Army against any other, so I compare us against ourselves...I don't want us to move on to a higher level of training until we have completely mastered the previous one...If we can't win at the point of contact, we're probably not going to win at all. Mastering the fundamentals is critical and a top priority.

—GEN Michael X. Garrett
Commanding General, U.S. Army Forces Command

Introduction

The U.S. Army Forces Command (FORSCOM) Commanding General, GEN Michael X. Garrett, directed his active and reserve component commanders to focus on winning at the point of contact. He recognized a mismatch between training strategy, our readiness models, and readiness metrics.¹ Further, GEN Garrett proffers “mastering the fundamentals” as the way to address the mismatch, making it critical and a top priority.²

In this article, I discuss three key concerns for the operational intelligence force—organization, maintenance, and training—and how we are addressing each concern. We, as members of the intelligence warfighting function, must take personal and professional responsibility for fixing ourselves. Embedded are concrete actions that we can take to master the fundamentals and achieve readiness in the operational intelligence force.

GEN Garrett's “Freedom Six” Priorities³

1. **Maximize Unit Readiness:** Focus leadership, training, and resources on improving unit combat readiness to meet Combatant Command demand and contingency requirements.
2. **Operationalize Army Total Force Policy:** Take actions to advance and instill one standard of manning, equipping, and training to build decisive action readiness across the Total Force.
3. **Master the Fundamentals:** At all echelons, codify and enforce standards and warfighting doctrine to ensure every Soldier, leader, and unit is resourced and ready to win in combat.
4. **Strengthen Leader Development:** Develop agile, adaptive leaders of character through Army development programs and tough/realistic training.
5. **Care for Soldiers, Civilians, and Families:** Enhance individual performance and resilience foundational to building unit readiness by improving unit, community, and institutional focus upon the health of the force and families.
6. **Inform the Future Force:** Leverage our role as the Secretary of the Army's conventional Service Force Provider and largest operating force command to shape development of the future force.

Historical Context

It was clear to me when I assumed the role of corps G-2 in 2015 that the intelligence warfighting function was having a tough time transitioning from counterinsurgency to large-scale ground combat operations. Within the first couple of months after arriving at I Corps, Joint Base Lewis-McChord, Washington, I had to replace one of my brigade combat team (BCT) S-2s who had lost the confidence of his commander. I selected a strong, capable major to backfill him, and he deployed with the BCT to the National Training Center less than 90 days later.

The rotation was a disaster for the intelligence warfighting function. The post-mortem exposed three enterprise-level faults: *systemic organizational dysfunction, foundational maintenance flaws, and a lack of intelligence Soldier experience and training to meet the needs of large-scale ground combat operations*. We needed a concerted, synchronized, and sustained effort to get well. Army military intelligence (MI) leaders became aware of the issues, and efforts were underway to correct them. More importantly, key innovators in our warrant officer and noncommissioned officer corps also recognized these faults, were not satisfied with the status quo, and were motivated to elevate the skills within the operational intelligence force. FORSCOM partnered with the U.S. Army Intelligence and Security Command (INSCOM) and the U.S. Army Intelligence Center of Excellence (USAICoE) to form a unified effort. The triad leveraged Foundry program resources and leader empowerment at the lowest level to achieve readiness. As a result, the operational intelligence force is on track to master the fundamentals by the end of fiscal year (FY) 2022; however, we must remain ever vigilant and unrelenting in the pursuit of readiness or risk a loss of momentum.

Organization

Some may still remember the transformation from the Army of Excellence to the modular Army in 2003, when the MI force design transitioned from fighting divisions and corps to a BCT-centric modular force designed for success in counterinsurgency. With the counterinsurgency requirements diminished, we are returning to a design that can meet the threats from peer competitors in *large-scale ground combat operations*. An approved force design update will take effect in FY 2022; it will transition the BCT MI company from counterinsurgency to large-scale ground combat operations. The update will integrate signals intelligence (SIGINT) with electronic warfare military occupational specialties (MOSs) to create a new intelligence cell. These changes will enhance and codify an improved BCT

collection management capability needed for transition to large-scale ground combat operations. In addition to force design updates for the BCT, new intelligence and electronic warfare (IEW) battalions will be activated to provide direct support to division and corps operations. These redesign efforts optimize information collection resources to maximize fires, effects, and decision making for commanders. We have proven the concepts behind the new design in exercises and codified the design in the new organization with a forward look at future multi-domain operations support requirements. Although designing these organizations has been challenging, the energetic efforts of personnel at Fort Huachuca, Arizona, both USAICoE and Army Futures Command, have brought a critical capability to the operational intelligence warfighting function.

Organization: What You Can Do Now to Prepare

- ◆ Know when your unit is scheduled to transition or receive new formations.
- ◆ Know the space, equipment, doctrine, and training requirements for that formation, and request the required additional resources as soon as possible.
- ◆ Lean forward—begin the transition to new force design updates 12 months before activation.
- ◆ Schedule progressive training and certification for the new organization.
- ◆ Coordinate support from division and your local Foundry site.

Maintenance

Over the past 15 years, our Army created the most effective counterinsurgency intelligence operation that ever existed—bar none. However, rapid innovation and fielding led to a reliance on contract maintenance and an overall atrophy of maintenance systems and processes at all levels. The Army IEW maintenance system is regaining its health thanks to a herculean effort by the Program Executive Office—Intelligence, Electronic Warfare and Sensors; system program managers; FORSCOM G-4; and IEW maintenance professionals throughout the Army. By the end of calendar year 2020, FORSCOM intelligence systems should all be fully integrated into the Global Combat Support System—Army, which will enable the execution of standard maintenance practices. We must implement and maintain rigorous training and inspection programs to ensure maintenance standards across the operational intelligence force. Maintenance is a fundamental that we must master to enable success in operations.

Maintenance: What You Can Do Now to Get Your Equipment Ready

- ◆ Ensure your systems are in the Global Combat Support System–Army, and review weekly for proper preventive maintenance checks and services. No faults? No parts on order? It is either a miracle or poor maintenance. PROBABLY NOT A MIRACLE.
- ◆ Ensure your systems have scheduled services that synchronize with the brigade engineer battalion or IEW battalion maintenance program.
- ◆ Ensure your unit has a command maintenance discipline program. Get copies of inspection checklists, and conduct an internal command maintenance inspection!
- ◆ Ensure your units have adequate IEW maintenance facilities.

Training

The three pillars of the FORSCOM intelligence training effort are nested in the *Army Intelligence Training Strategy 2020* to achieve the FORSCOM Commanding General's mastering the fundamentals objective by the end of FY 2022.⁴

- ◆ The first pillar is the Military Intelligence Training Strategy (MITS), which is the process to certify the operational intelligence force and sets the training bar for units.
- ◆ The second pillar is the Comprehensive Operational Training Support to MITS program, which is a series of courses that drive us toward mastery of each intelligence discipline, with the Digital Intelligence Systems Master Gunner (DISMG) course as the culminating achievement.
- ◆ The third pillar is the FORSCOM Intelligence Warfighting Program, which focuses on enabling corps and division G-2s and expeditionary-military intelligence brigade (E–MIB) commanders to achieve mastery of intelligence support to large-scale ground combat operations.

Essential to all facets of FORSCOM MI training is the Foundry program, the engine of FORSCOM's intelligence training and readiness, which provides top secret and National Security Agency network access and infrastructure, access to training and instructors, and funding to execute collective and specialized intelligence training.

Military Intelligence Training Strategy

MITS is modeled on the maneuver training system of four tiers, each with multiple tables. The tiers progress from Tier 4 (individual) to Tier 3 (crew) through systems certification in Tier 2. An example of Tier 2 is scenario-driven collection and analysis tasks for the BCT SIGINT collectors working with

the SIGINT analysis node to demonstrate collective SIGINT proficiency. The Army caps MITS at Tier 1, which is an integrated evaluation with the BCT field training exercise. This is usually a BCT's pre-combat training center or deployment exercise. USAICoE published the final BCT MITS training circular in 2019 after testing and refinement using a series of training pilots.⁵

Four BCTs conducted a MITS Tier 2 and Tier 1 pilot program in FY 2019. The results were immediate and tangible as certified crews arrived at the combat training center with operational equipment and were able to fight their systems. Although this might not seem like a high bar to achieve, it signified the turning of a training proficiency corner. In FY 2020, FORSCOM Operations Order 151221 required units to complete all four MITS tiers: for 31 FORSCOM active component BCTs, annually; and for 27 component 2 BCTs, every 5 years. While deployments and the coronavirus disease 2019 pandemic significantly reduced the number of Tier 1 (BCT collective) events in FY 2020, most units found a way to train the other tiers with positive results. The three major challenges identified that—

- ◆ BCT and brigade engineer battalion commanders lacked an understanding of MITS and therefore failed to fully support it.
- ◆ Insufficient skilled observer, coach/trainers were available because of the operational tempo.
- ◆ There was a need to further enrich the MITS scenarios.

MITS: What You Can Do Now

- ◆ Noncommissioned officers must constantly train on MITS Tier 4 (individual) skills with their Soldiers. Seize every opportunity to master the fundamentals!
- ◆ Once certified, commanders must stabilize crews so that they continue to increase in proficiency, especially before employment at a combat training center or operation.
- ◆ Ensure your MITS training synchronizes with your brigade engineer battalion and BCT training schedule, and coordinate through your division G-2 and Foundry program director. BCT and division training calendars should reflect MITS Tier 2 and 1 at a minimum.
- ◆ Every Foundry site has a MITS planner called the collective training exercise integrator; find that person and leverage their expertise to help plan your training!
- ◆ Volunteer to be an observer, coach/trainer for another unit's MITS training. It is a great way to learn.
- ◆ Get to the combat training center for an opposing force or observer, coach/trainer ride along. See how MITS is applied in the fight.

USAICoE is committed to continuously improving MITS, and the INSCOM Foundry program manager is committed to supporting MITS execution with exercise control capabilities, Intelligence and Electronic Warfare Tactical Proficiency Trainer integration, and IEW range facilitation. In FY 2021, you can expect the Army to publish training circulars for battalion S-2 MITS; MOS 12Y, Geospatial Engineer; MOS 35L, Counterintelligence Agent; and division and corps-level MITS. We will develop E-MIB MITS alongside the new concept for employment and doctrine for the new IEW battalion Total Army Analysis effort.

Comprehensive Operational Training Support to MITS

MITS has dramatically improved the standard block and tackle tasks of our BCT intelligence warfighting function, arguably achieving a level of competence across the force. Our experience at the dirt combat training centers made it clear that we had lost mastery-level skills needed to apply our craft to large-scale ground combat operations. We had systems that worked and crews that could operate them, but we lacked mastery of the application of the intelligence warfighting function. We looked to the extraordinarily successful FORSCOM DISMG program for a solution. The DISMG program brought together determined intelligence subject matter experts to construct a rigorous course of “cutting-edge” best operational practices. DISMG course graduates return to home station and teach the Gunner Entry Program preparatory course to build more capability at home station and ultimately create more DISMG candidates to continue the cycle. DISMG course graduates can be credited with the initial turnaround in the BCTs. FORSCOM, in coordination with INSCOM and USAICoE, conducts the DISMG course, along with all the Comprehensive Operational Training Support to MITS courses, at the Army Foundry Platform located on Fort Bragg, North Carolina.

Using the DISMG course model, we developed advanced operational courses (AOCs) for each intelligence discipline. AOC-Geospatial Intelligence and AOC-Human Intelligence are fully operational, while AOC-SIGINT, AOC-All Source, AOC-Counterintelligence, and AOC-IEW Maintenance are moving through the development cycle toward completion. We intend for every AOC graduate to be capable of returning to home station and teaching the Intermediate Operational Course; in some disciplines, reach-back to the Army Foundry Platform or the intelligence warfighting function enterprise may be necessary. Units can gain expertise very quickly using the Intermediate Operational Course/AOC process, and over time, FORSCOM could build train-

ing depth and expertise while normalizing best practices. We develop the AOCs in concert with both the institutional training base at USAICoE and the functional intelligence base in INSCOM. Lastly, the DISMG courses and AOCs maintain a block of time to engage the related program managers, Army capability managers, and Army Futures Command to give feedback, or to provide thoughts, on new systems, capabilities, and modernization of the force. Once again, the Foundry program, supported by INSCOM Soldiers and Civilians, serves as the foundation for the Comprehensive Operational Training Support to MITS program.

Comprehensive Operational Training Support to MITS/AOCs: What You Can Do Now to Enhance Your Skills Capability

- ◆ Plan your training to get DISMG course and AOC graduates before your MITS and combat training center/employment execution. This is even more important for Reserve and National Guard units!
- ◆ Use your DISMG course and AOC graduates to train the rest of your force at the discipline-appropriate Intermediate Operational Course and Gunner Entry Program sessions at home station. Uplift your entire force!
- ◆ Require your MI professionals to complete the “Digital Intelligence Systems Foundational Course.” This online training course teaches what we should know as professionals and sets the stage for follow-on learning. It can be found at https://ellc.learn.army.mil/webapps/portal/execute/tabs/tabAction?tab_tab_group_id=_2_1.

FORSCOM Intelligence Warfighting Program

With most Army officers only experienced in intelligence support to counterinsurgency, the G-2 sections slashed in manning by 35 percent in FY 2016, and the current E-MIB designed for counterinsurgency, we needed to put a concerted effort to rapidly build competency leading to mastery in our G-2 sections and E-MIBs. This need became the genesis of the FORSCOM Intelligence Warfighting Program. The cornerstone of the program is the FORSCOM intelligence warfighting forum, a 1-week academic forum focused on professional education and discussions with corps and division G-2s and E-MIB commanders, ending in Mission Command Training Program wargame vignettes. FORSCOM conducts two sessions of the forum per year, and based on captured best practices and experience, we are constantly updating and improving the forum. The feedback following the first two forum events has been very positive. The FORSCOM intelligence warfighting forum is only one part of the larger intelligence warfighting program. A newly created FORSCOM G-2 position, the division/corps intelligence program manager, focuses on enabling the division and corps intelligence

warfighting function as they prepare for warfighter exercises and other exercises and operations. The division/corps intelligence program manager is linked into planning conferences in order to synchronize support and orchestrate architectural and training requirements. Another addition is the INSCOM Foundry senior intelligence advisor, who is the most crucial element of the program. A seasoned former G-2, the senior intelligence advisor focuses on coaching and mentoring division-level intelligence warfighting function leaders on their path toward a warfighter exercise or deployment. Lastly, the synchronization with, and support from, Mission Command Training Program ensures we move forward with consistency and relevancy.

FORSCOM Intelligence Warfighting Program: What You Can Do Now to Master Intelligence Warfighting

- ◆ All G-2/E-MIB commanders should attend an intelligence warfighting forum; follow-on participation can help inform new selectees and keep you up to date on latest tactics, techniques, and procedures.
- ◆ Ensure you are lined in with the FORSCOM G-2 division/corps intelligence program manager and the Foundry senior intelligence advisor.
- ◆ Ride along with the Mission Command Training Program world class opposing force!
- ◆ Be a guest observer, coach/trainer with Mission Command Training Program for another unit warfighter exercise.
- ◆ Round out gaps in division and corps exercises to gain experience in your unit.

Conclusion

GEN Garrett highlighted the need for intelligence professionals to master the fundamentals. We will use all of FORSCOM's intelligence warfighting function capability, partnered with INSCOM and USAICoE, to master the fun-

damental skills needed to win against a peer threat. By addressing the three major concerns for the operational intelligence force—organization, maintenance, and training—intelligence leaders can address these challenges in the context of their operational environment.

We, as leaders, cannot let known obstacles (for example, distractions in garrison and the grind of daily Army life) or “black swan events” (such as pandemics and hostile actions by state/non-state actors) distract us from achieving mastery of our intelligence skills. We cannot falter in our drive for, and personal responsibility to achieve, comprehensive readiness. Readiness and mastery will not only win wars but will also deter them, and in doing so prevent the unbearable cost inherent in large-scale wars. 🌟

Epigraph

Arpi Dilanian and Matthew Howard, “Mastering Fundamentals: An interview with Gen. Michael Garrett,” *Army Sustainment* 52, no. 1 (January–March 2020): 58.

Endnotes

1. Michael X. Garrett, “Winning at the Point of Contact,” U.S. Army Worldwide News, August 13, 2020, <https://www.army.mil/article/238107>.
2. U.S. Army Forces Command (FORSCOM), *FORSCOM Campaign Plan* (26 October 2017).
3. Paul Boyce, “FORSCOM Commander’s Forum highlights people, Army readiness, modernization, reform,” U.S. Army Worldwide News, November 13, 2019, https://www.army.mil/article/229766/forscom_commanders_forum_highlights_people_army_readiness_modernization_reform.
4. U.S. Army Intelligence Center of Excellence, *Army Intelligence Training Strategy 2020* (May 2020).
5. Units should review TC 2-19.400, *Military Intelligence Training Strategy*, for further information on the Military Intelligence Training Strategy (MITS). The U.S. Army Training and Doctrine Command published training circulars for the brigade combat team MITS tiers in TC 2-19.401 through TC 2-29.404.

COL Timothy Parker is the Deputy Chief of Staff, G-2, U.S. Army Forces Command at Fort Bragg, NC. He is a 1992 graduate of the University of Dayton Army Reserve Officer Training Corps program and holds graduate degrees from the U.S. Army Command and General Staff College and School of Advanced Military Studies. COL Parker was a 2012 U.S. Army War College Fellow to the Central Intelligence Agency and recently served as the I Corps G-2 and the U.S. Army Intelligence and Security Command G-3. He had operational tours in Macedonia and Bosnia, had combat tours in Afghanistan and Iraq, and served as an intelligence officer in special mission units.



In December 1946, the 430th Counter Intelligence Corps Detachment in Salzburg, Austria, uncovered a black-market smuggling operation involving the artificial sweetener saccharine. A worldwide sugar shortage during the war and postwar period put saccharine in high demand. Dubbed “Operation Sugar,” the investigation netted a number of prominent Nazis involved in underground operations.

The Operational Environment in Multi-Domain Operations



by Mr. Darryl Ward

Introduction

As an operational environment (OE) evaluator supporting the Army Quality Assurance Program, I have observed how Army centers and schools set conditions to prepare leaders for unified land operations. The Army institutional base is undergoing a major sea change in unified land operations as we transition from years of stability-centric operations to re-hone atrophied warfighting skills associated with large-scale combat operations. A key unified land operations aspect specified in ADP 3-0, *Operations*, is “across multiple domains to shape operational environments.”¹ So how do Army institutions shape OEs? More importantly, how do these institutions replicate contested multiple domains that help shape OEs? It is the latter question I will address and offer some recommendations. Tackling this question, as the Army wrestles with educating leaders to operate in contested multi-domains, enables further understanding and shaping of future OEs.

History and Past Operations

To appreciate the context of multi-domain environments, it might help to go back and recapture some of the more significant events that altered our ways of planning and prosecuting warfare. My intent is not to present an all-inclusive history lesson but rather to make it like Mel Brooks’s *History of the World: Part I*.² So for brevity, I left out several important events.

Through the centuries, warfare generally occurred in the domains of land and maritime environments. The tactics and geometries with which battles were fought on the fields and seas have certainly changed with the discovery of black powder in the 9th century and technological advancements such as optics in the early 17th century.³ These achievements led to increased ranges, lethality, and improved situational awareness; however, for the most part, warfare remained a surface-level affair until the late 18th century.

In the 18th century, specifically in the 1780s and 1790s, French experiments with hot air balloons, and then hydrogen-filled balloons, led to manned observation platforms to achieve the ultimate high ground (so they thought) and signaled the beginning of a third domain (air) that would change warfare forever. Just over a century later, these crude aerial observation platforms progressed to rudimentary delivery means for strategic bombing during World War I. Roughly three decades later, during World War II, rapid technological advances in the air domain culminated with the aerial bombings of Hiroshima and Nagasaki and helped usher in the atomic age.

World War II did more than bring a new era to the world; it also initiated a fourth (space) domain with the V-2 rocket program. The V-2 was the world’s first long-range ballistic missile that achieved an altitude anywhere between 55 and 120 miles, thus departing and reentering the Earth’s atmosphere (more or less). No distinct separation exists between the Earth’s atmospheric layers and outer space, but it is generally accepted to be at 62 miles altitude.⁴ Much like its predecessors, the space domain was and still is marked with rapid technological advances. From earlier space exploration (Sputnik, Vostok, Mercury, Gemini, and Apollo) to where we are today, much of what we take for granted in telecommunications, navigation, weather forecasting, etc., was made possible through our current perception (Gene Roddenberry fans notwithstanding) of the ultimate high ground. Today, approximately 2,000 satellites orbit in the Earth’s exosphere,⁵ making such capabilities as positioning, cellular phones, and the Internet of Things seem routine.

Considering that the air and space domains are divided around the 60-mile mark, all domains have a physically distinct feature that separates them—except for one, the cyberspace domain. Cyberspace, or “cyber” for short, is the fifth domain that interconnects with the other four domains via the electromagnetic spectrum and thus serves

as an enabler for synchronizing, coordinating, processing, and storing information. Likewise, cyber is also a lucrative target because of the relatively low cost with regard to the resources needed to execute cyber warfare compared with high gains in terms of second-order effects to the other domains. Indeed, one can acquire insight into how potential threats perceive the importance of cyber in the following excerpt from *Unrestricted Warfare*: “To a very great extent, war is no longer even war but rather coming to grips on the internet, and matching the mass media, assault and defense in forward exchange transactions, along with other things which we had never viewed as war, now all possibly causing us to drop our eyeglasses. That is to say, the enemy will possibly not be the originally significant enemy, the weapons will possibly not be the original weapons, and the battlefield will also possibly not be the original battlefield.”⁶

Multi-Domain Concepts and Doctrine

Operating in multiple domains is not new to the U.S. Army. Even the active defense doctrine from the mid-1970s, which segued to AirLand Battle 2000 in the 1980s and 1990s, contained domain aspects that orchestrated forces on land, sea, and air. In fact, AirLand Battle 2000 is where we begin to see military applications of space for reconnaissance, surveillance, and targeting. Both of these doctrines served their purpose for a defensive posture against a monolithic conventional threat. However, lessons learned from United States Army operations in Afghanistan and Iraq, which varied in conflict and operational theme, necessitated the 2008

publication of FM 3-0, *Operations*. A significant chapter in the manual is on *Information Superiority*.⁷ It is here we first learn about the Army’s informational tasks. Some of these tasks (for example, command and control warfare and information protection) and their associated capabilities evolved into the current cyberspace missions and actions we see in the 2017 FM 3-12, *Cyberspace and Electronic Warfare Operations*.⁸ Therefore, while the term *multi-domain* introduced in TRADOC Pamphlet 525-3-1, *The U.S. Army in Multi-Domain Operations 2028*,⁹ may sound new, the concept of operating in multiple domains against a near-peer or even a peer threat is not.

Guidance

From the National Defense Strategy to the Army Posture Statement, these important documents acknowledge the challenges the U.S. Army faces in an ever-competitive global security environment. The reemergence of Russia and China as pacing threats and the nuclear ambitions of rogue nations such as North Korea and Iran command our attention, and transregional terrorist groups remain a persistent threat. Given the multitude of capabilities associated with current and potential adversaries, the Army’s challenge to prevail in unified land operations, as well as our institutional base to train and educate the next generation of Army leaders, has never been greater. Perhaps the best guidance I have read is in the *Fiscal Year 2020 Combined Arms Center Command Guidance*. It says, “Enable the Army to transition **the current [counterinsurgency] COIN-centric fielded**

force to a [multi-domain/large-scale combat operations] MD-LSCO force with the capability and capacity...that can continuously compete and, when required, prevail in large scale combat against peer threats in multi-domain contested environments.”¹⁰ Army centers and schools need no more than this statement to realize why it is important to create conditions that replicate contested domains.

Future Operational Environment

We live in a world of more than 7 billion people. The National Intelligence Council estimates that by 2030 the global population will be more than 8 billion and the trend for people to



U.S. Army photo collage

For the past two years, the Army has initiated many changes to help modernize the force. Among those changes, Army Futures Command found a new home, Soldiers began receiving a new rifle, and the Army made strides to improve its hyper-sonic, networking, and artificial intelligence capabilities.

move to urban settings will increase, causing the urban population to climb to nearly 60 percent.¹¹ Think about what an extra billion means to already stressed infrastructures, increasing demands, limited global resources, and climatic changes that serve as a catalyst for reducing resources in some areas (desertification in Africa) while opening new areas in others (oil exploration in the Arctic). When you connect the dots, you see why pacing threats are modernizing their militaries.

Just as with our lessons learned, threats are studying the U.S. Army and drawing their own lessons. Threats understand that to counter a power projection capability such as the U.S. military, they must be able to separate forces in terms of time, space, and function. Threat antiaccess and area denial (A2AD) strategies will therefore include elements that attack multiple domains and fight in depth, beginning at the U.S. homeland. The earlier passage from *Unrestricted Warfare* provides a glimpse into the conceptual view of this fight to disrupt and disaggregate U.S. forces.¹²

A2AD strategies will target multiple domains. The following information is not all-inclusive but provides an idea of how threats are planning to disrupt, delay, and disaggregate. In the cyber domain, which affects all domains, information warfare elements such as computer warfare and information attacks performed via denial of service, malware emplacement, and network penetration may create abnormalities in mission command network performance, create erroneous information, and spoof end users. In the air, land, maritime, and space domains, electronic warfare through nonlethal and lethal directed-energy weapons (lasers, radio frequency) will also incapacitate or destroy mission command sensors and communication systems, jeopardize aircraft survivability, and limit performance of unmanned aircraft systems (UAS). In the not too distant future for air, land, maritime, and space domains, physical destruction through enhanced kinetic energy weapons (hypervelocity rail guns) will seek strategic high-payoff targets that might be continents away.¹³ In the air, land, and maritime domains, special-purpose forces and proxies will target strategic air and seaports of embarkation/debarkation, power grids, communication, and transportation networks. Finally, I don't want to forget chemical, biological, radiological, and nuclear (CBRN) defense. I participate in a U.S. Army Forces Command countering weapons of mass destruction working group, which anticipates discussions about CBRN as a battlefield condition in future large-scale combat operations.

Multi-Domain Impacts on Unified Land Operations

ADP 3-0, *Operations*, defines unified land operations as, “simultaneous execution of offense, defense, stability, and defense support of civil authorities across **multiple domains** to shape operational environments, prevent conflict, prevail in large-scale ground combat, and consolidate gains as part of unified action.”¹⁴ I highlighted *multiple domains* because the question is, how do we replicate contested multiple domains?

We are a land component, yet we depend on multiple domains such as cyber and space. The Army relies on space to communicate; use positioning, navigation, and timing (PNT); protect; sustain; and enable intelligence. The Army's reliance on cyber (internet, telecommunication networks, computer systems, processors, and controllers) affects every domain, warfighting function, and individual. A typical brigade combat team has more than 2,500 PNT-enabled devices and over 250 satellite communications space-enabled devices.¹⁵ An individual can easily have 13 or more cyber identifiers.¹⁶ Think about those numbers. I believe you will agree that the Army relies on multiple domains such as cyber and space to help shape the OE in order to prevail in unified land operations. Threats plan to contest these domains; therefore, it is imperative that Army centers and schools create classroom and field conditions that are conducive to getting future leaders to think about operating in contested domains.

Classroom Conditions

Replicating contested multiple domains in the classroom for Army centers and schools is a greater challenge than



Officers and noncommissioned officers within the Joint Force Headquarters-National Capital Region and the U.S. Army Military District of Washington participated in a week-long Company Commander/First Sergeant Course on Joint Base Myer-Henderson Hall, VA, 28 October to 1 November 2019.

U.S. Army photo

replicating these domains at an Army combat training center. For starters, the outcomes are different. Leader development tasks at centers and schools focus on individual learning step activities, while combat training centers focus on collective training objectives. Centers and schools lack the dedicated ground opposing forces (OPFOR) that are at the combat training centers along with a World Class Cyber OPFOR that provides direct support to the combat training centers. Finally, leader development at centers and schools occurs primarily in classroom situations using constructive means via simulations rather than the live training provided at combat training centers (the Mission Command Training Program is the exception). However, centers and schools can still take steps to create rigorous conditions for learning outcomes and get leaders in the mindset that they are operating in contested domains.

My recommendations for the following training areas are described below:

- ◆ Analog planning and battle tracking.
- ◆ Personal devices.
- ◆ Air superiority.
- ◆ Creation of a degraded electromagnetic spectrum.
- ◆ Degraded precision-guided munition (PGM) effectiveness.
- ◆ Target acquisition.
- ◆ Battle drills.
- ◆ Camouflage, cover, and concealment.
- ◆ CBRN defense.

Analog Planning and Battle Tracking. Reliance on digital systems such as Command Post of the Future has led to atrophied analog skills. Force students to maintain backup paper maps and overlays during planning and execution that maintain the common operational picture. Get students to verify data and never to assume. As previously stated, threats to PNT systems will attempt to spoof, block, or create erroneous data. If a discrepancy exists between digital and analog systems, it might indicate a threat computer warfare and/or information attack.

Personal Devices. The threat is always in the reconnaissance phase. Here is a simple multi-domain condition the instructor can create during any lesson that places students in an operational planning or execution setting. Ask students whether they have their personal electronic devices (cell phone, smartwatch, Fitbit device, etc.) with them. These items are all targetable and exploitable by the threat. We must be constantly aware that the threat wants our digi-

tal signature, and it is our responsibility to make it as difficult as possible for them to achieve that goal. Get students used to the idea of not bringing personal digital devices into the classroom, just as they should not take these devices into an operational setting.

Air Superiority. Students must understand that when planning large-scale combat operations against a peer threat, they can no longer assume the luxury of friendly air superiority.

Creation of a Degraded Electromagnetic Spectrum. A threat will attempt to interdict communications through electronic warfare. The results could be a degraded electromagnetic spectrum that disrupts communications. Force students to plan for couriers to send and receive information, limit total asset visibility, and delay the classes of resupply. These are injects that can be scripted into an exercise and do not require replication by virtual or constructive means.

Degraded Precision-Guided Munition Effectiveness. Threat nonlethal and lethal attacks against PNT systems will affect PGM effects. Space-related weather (solar winds, flares) may also naturally generate electromagnetic interference. Reconstitute constructive OPFOR in simulations to replicate ineffective PGM strikes due to threat or electromagnetic interference-induced effects. Force students when building their attack guidance matrices to plan for additional sensors to assess PGM effects.

Target Acquisition. Threat attacks against PNT systems will also affect the acquisition of high-payoff targets for time-sensitive targeting. This should be accounted for during planning, specifically during wargaming, and rehearsed by the students to develop battle drills when high-payoff targets cannot be detected or unexpectedly appear.

Battle Drills. While on the subject of battle drills, disciplines learned in the classroom will carry over to operational assignments. A noted shortcoming of staffs during combat training center rotations was their lack of battle drills when under electronic attack (jamming) by the OPFOR.¹⁷ Have students develop and rehearse battle drills such as primary, alternate, contingency, and emergency plans for responding to electronic attack and naturally occurring electromagnetic interference.

Camouflage, Cover, and Concealment. Assume others have the ability to observe us via satellites and UAS. More than 65 countries have satellites,¹⁸ and those countries without satellites, including non-nation states, may acquire satellite imagery from open sources or pay those that have it. Students should get into the habit of sound force protection practices. This includes planning for camouflage, cover, and concealment of high-value targets to avoid detection from

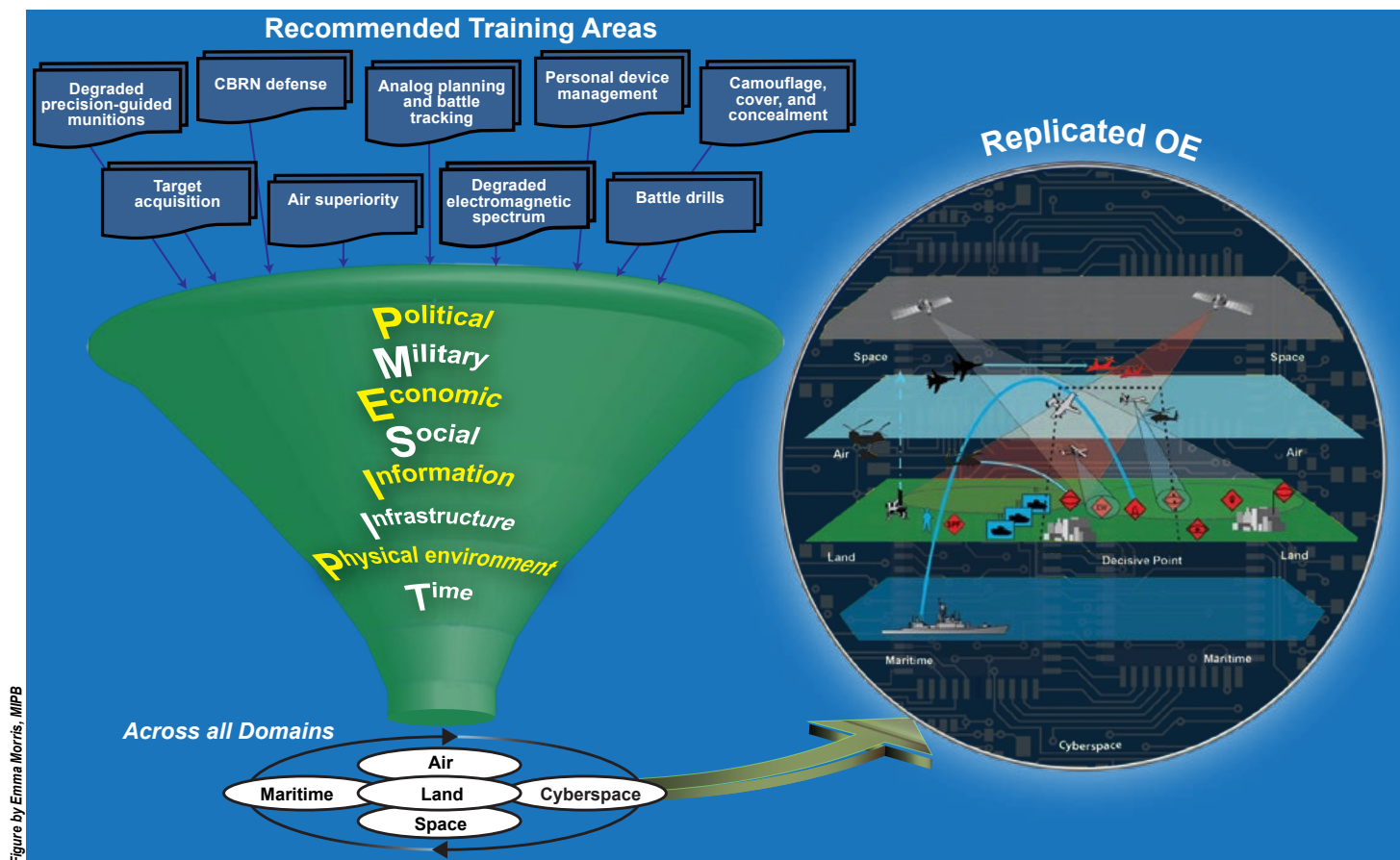


Figure by Emma Morris, MPB

U.S. Army centers and schools can take steps to create realistic training conditions that replicate contested multi-domain operational environments.

satellites and UAS. Planning for observation from space and air domain capabilities is a good practice to implement both in classrooms and in field environments.

Chemical, Biological, Radiological, and Nuclear Defense. CBRN defense is an anticipated condition in the next large-scale combat operation. The threat will target troop concentrations, logistical centers, main supply lines, and key terrain to disaggregate/slow momentum. This will disrupt timelines for reception, staging, onward movement, and integration as well as classes of resupply. Students must account for threat CBRN capabilities during the planning process.

Conclusion

Finally, I will return to my original question: How do Army institutions replicate multiple domains that help shape OEs? I will leave you with my personal observation. The doctrinal operational variables of political, military, economic, social, information, infrastructure, physical environment, and time (PMESII-PT) do not do a particularly good job in specifying the domains. This might lead to an unintentional omission during planning of domain impacts on the OE. JP 3-0, *Joint Operations*, states, “[operational areas] OAs have physical dimensions composed of some combination of **air, land, maritime, and space domains**.”¹⁹ ADP 3-0 further states,

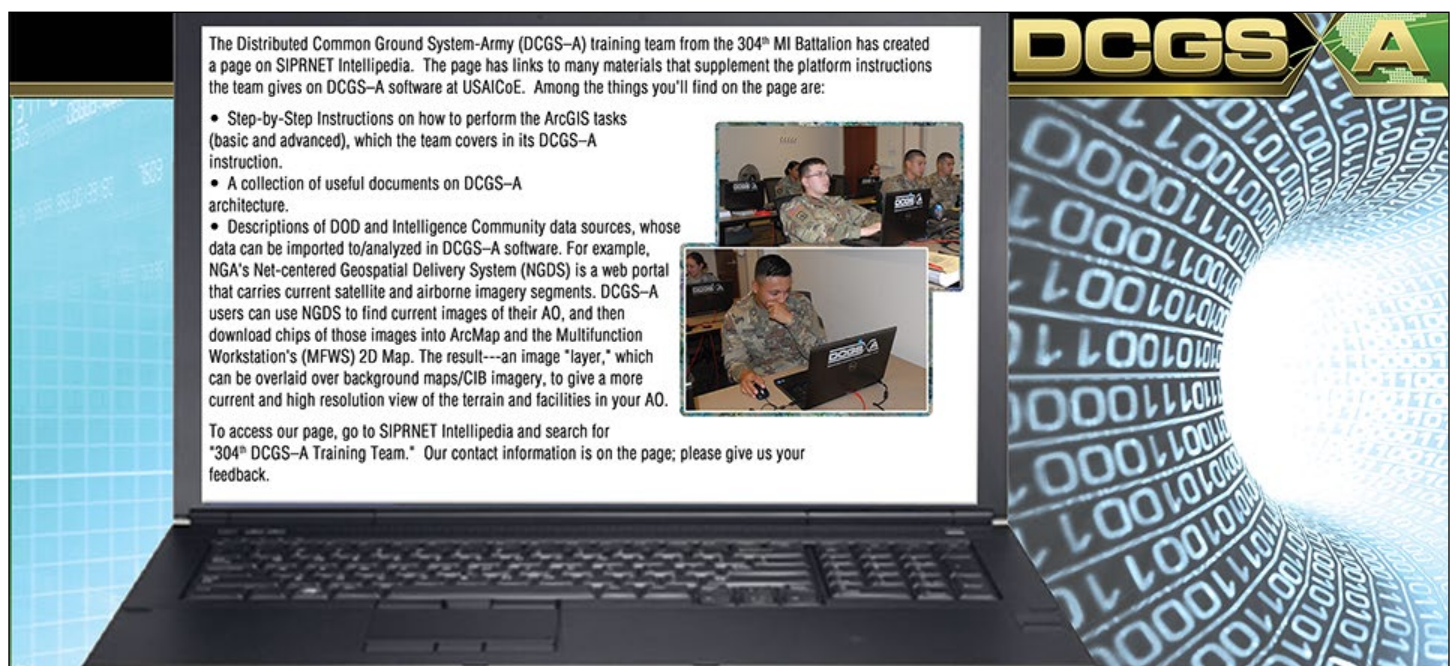
“The area of interest always encompasses aspects of the **air, cyberspace, and space domains**.”²⁰ So while PMESII-PT does not specify the five domains, if Army centers and schools get their students to think of air, cyber, land, maritime, and space as extensions of the physical environment when defining the OE, and create some of the conditions described in the classroom, this will go a long way in our ability to shape the OE. ✨

Endnotes

1. Department of the Army, Army Doctrine Publication (ADP) 3-0, *Operations* (Washington, DC: U.S. Government Publishing Office [GPO], 31 July 2019), 3-1.
2. *History of the World: Part I* is a 1981 American sketch comedy film written, produced, and directed by Mel Brooks. Despite carrying the title *Part I*, there is no sequel; the title is a play on *The History of the World* by Sir Walter Raleigh who wrote the work while prisoner in the Tower of London. He intended to write a multivolume set but only managed to complete the first volume before being beheaded. Wikipedia, s.v. “History of the World, Part I,” last modified 20 July 2020, 6:19, https://en.wikipedia.org/wiki/History_of_the_World,_Part_I.
3. Neil deGrasse Tyson and Avis Lang, *Accessory to War: The Unspoken Alliance Between Astrophysics and the Military* (New York: W.W. Norton & Company, 2018).

4. Brandon Specktor, "The Edge of Space Just Crept 12 Miles Closer to Earth," Live Science, July 25, 2018, <https://www.livescience.com/63166-outer-space-border-karman-line.html>.
5. Union of Concerned Scientists (UCS) Satellite Database, updated April 1, 2020, <https://www.ucsusa.org/resources/satellite-database>.
6. Qiao Liang and Wang Xiangsui, *Unrestricted Warfare: China's Master Plan to Destroy America* (Los Angeles: Pan American Publishing Company, 2002). Written by two colonels in the People's Liberation Army, the book was originally titled *Unrestricted Warfare*. In 1999, the Foreign Broadcast Information Service, an open-source intelligence component of the Central Intelligence Agency, made the English translation available. In 2002, the book was published in English, with the subtitle *China's Master Plan to Destroy America*. Wikipedia, s.v. "Unrestricted Warfare," last modified 25 July 2020, 17:35, https://en.wikipedia.org/wiki/Unrestricted_Warfare#cite_note-1-1; and Wikipedia, s.v. "Foreign Broadcast Information Service," last modified 13 May 2020, 23:01, https://en.wikipedia.org/wiki/Foreign_Broadcast_Information_Service.
7. Department of the Army, Field Manual (FM) 3-0, *Operations* (Washington, DC: U.S. GPO, 27 February 2008 [obsolete]), 7-1–7-13.
8. Department of the Army, FM 3-12, *Cyberspace and Electronic Warfare Operations* (Washington, DC: U.S. GPO, 11 April 2017).
9. Department of the Army, Training and Doctrine Command (TRADOC) Pamphlet 525-3-1, *The U.S. Army in Multi-Domain Operations 2028* (Fort Eustis, VA: TRADOC, 6 December 2018), GL-7.
10. Department of the Army, *Fiscal Year 2020 Combined Arms Center Command Guidance* (Fort Leavenworth, KS: U.S. Army Combined Arms Center, 2 August 2019), 1.
11. Office of the Director of National Intelligence, *Global Trends 2030: Alternative Worlds* (Washington, DC: National Intelligence Council, December 2012), 26.
12. Qiao and Wang, *Unrestricted Warfare*. An abridged version derived from a translation by the Foreign Broadcast Information Service is available at <https://www.c4i.org/unrestricted.pdf>.
13. Department of the Army, TRADOC Pamphlet 525-92, *The Operational Environment and the Changing Character of Warfare* (Fort Eustis, VA: TRADOC, 7 October 2019).
14. Department of the Army, ADP 3-0, *Operations*, 3-1 (emphasis added).
15. Department of the Army, FM 3-14, *Army Space Operations* (Washington, DC: U.S. GPO, 30 October 2019), 1-1.
16. Department of the Army, FM 3-12, *Cyberspace and Electronic Warfare Operations*, 1-14.
17. Department of the Army, Center for Army Lessons Learned Handbook No. 18-28, *Operating in a Denied, Degraded, and Disrupted Space Operational Environment* (Fort Leavenworth, KS: Center for Army Lessons Learned, June 2018).
18. UCS Satellite Database.
19. Office of the Chairman of the Joint Chiefs of Staff, Joint Publication 3-0, *Joint Operations* (Washington, DC: The Joint Staff, 17 January 2017), IV-9 (emphasis added). Change 1 was published on 22 October 2018.
20. Department of the Army, ADP 3-0, *Operations*, 4-3 (emphasis added).

Mr. Darryl Ward is retired from military service with the U.S. Army. He has 35 combined years of military intelligence experience in the Army and civil service and as a government contractor. He currently serves as a contractor in the U.S. Army Training and Doctrine Command G-27 Operational Environment/Opposing Force Program Validations Division supporting the U.S. Army Quality Assurance Program. He holds a bachelor of science in education from the University of Arkansas and a master of arts in health business administration from Webster University.



Technology Protection: Securing Modernization Efforts



by the Directorate of Intelligence and Security, U.S. Army Futures Command

Illustration by Emma Morris, MIPB

Introduction

The U.S. Army established Army Futures Command (AFC) to realign elements of the modernization efforts and bring unity of effort to the development process of the future force. The Army is modernizing **how we fight, what we fight with, and who we are as an Army**. Ensuring the Army is able to “fight tonight” while also actively seeking next-generation solutions to stay ahead of potential adversaries is fundamental to the modernization strategy. Equally fundamental, is safeguarding those solutions throughout the development and fielding processes. The AFC initiatives to safeguard technology innovations highlighted in this article are threat awareness, the protection of critical technology in order to deliver uncompromised technology to the force, and the development of more stringent disclosure programs.

Threat Awareness

Education on threats to innovation and intellectual property is the first step to protecting the technologies used in our future systems. The education program is a continual requirement that should focus on the current methodologies of near-peer adversaries to acquire U.S. intellectual property and the status of their game-changing technologies. The overall theft of U.S. intellectual property and technology has occurred on a scale that affects our national security. The financial loss from the theft of U.S. trade secrets is estimated to be as much as \$540 billion annually,

resulting in years of wasted research and development and lost jobs.¹ It also places the United States at risk for losing our leadership in advanced technologies. The AFC/Army’s challenge is to introduce applicable security practices at the moment of ideation for a new technology that could potentially overmatch an adversary. Timing is important because ideation occurs early in a project, during the generation and development of a new idea.

China is a prime example of a current adversarial challenge the Army faces. Over the past several decades, China and our other adversaries developed new and improved methods for acquiring United States technology. These new approaches are significant, as Director of the Federal Bureau of Investigation Christopher Wray stated in 2018: “I think China, from a counterintelligence perspective, in many ways represents the broadest, most challenging, most significant threat we face as a country. And I say that because for them it is a whole of state effort. It is economic espionage as well as traditional espionage; it is nontraditional collectors as well as traditional intelligence operatives; it’s human sources as well as cyber means.”²

Director Wray also sheds light on new methods of theft of intellectual property, from American academia and businesses to the traditional espionage of government secrets and legal but targeted business acquisitions. However, near-peer adversaries have increased their efforts to collect our ideas, thoughts, and research; their sources are American

university campuses, corporate boardrooms, government-sponsored research sites, and military offices. Through the Chinese Communist Party, China is able to fund these ventures, lending them money via their industrial policy, which gives Chinese companies an economic advantage and enables them to grow significantly. In 2010, for the first time, a Chinese organization was among the world's top 10 largest public companies on the Forbes Global 2000 list. In 2020, 5 of the 10 largest companies on that list were Chinese. Of the remaining five, four were U.S. companies.³

China's strategic goal is to obtain comprehensive national power through economic development by dominating its domestic markets and then by becoming a global leader, particularly in advanced technological disciplines. To achieve its strategic goals, China relies on a top-down, state-directed approach. As many as 100 different plans guide China's foreign acquisition in science and technology, making the effort broad in scale and influence. Among the most prominent are the Five-Year Plans and the Made in China Plan, also known as MIC 2025.

What is Made in China 2025?

The Chinese government has launched "Made in China 2025," a state-led industrial policy that seeks to make China dominant in global high-tech manufacturing. The program aims to use government subsidies, mobilize state-owned enterprises, and pursue intellectual property acquisition to catch up with—and then surpass—Western technological prowess in advanced industries. [It] is the government's ten-year plan to update China's manufacturing base by rapidly developing ten high-tech industries. Chief among these are electric cars and other new energy vehicles, next-generation information technology (IT) and telecommunications, and advanced robotics and artificial intelligence.⁴

To enact those plans, China uses multiple techniques, including legal business means, science and technology investments, mergers and acquisitions of United States companies, and legal means in academia. The People's Republic of China recruits individuals in those environments to acquire United States technology. While these individuals may not be trained intelligence officers, they are working for an intelligence officer and are considered co-opted by a Chinese intelligence service. When China recruits individuals who are in the private sector and academia to acquire United States technology, we refer to them as "nontraditional collectors" because they are not employees of the Chinese government and are not employed as intelligence officers.

Assistant Attorney General John C. Demers clearly captured China's efforts in a testimony before the Senate

Judiciary Committee in 2018, stating, "In all of these cases, China's strategy is the same: rob, replicate, and replace. Rob the American company of its intellectual property, replicate the technology, and replace the American company in the Chinese market and, one day, the global market."⁵ In order to stop the assault on the American economy and our status in the world, intelligence and security must work hand in hand with other government agencies to reach out to academia and businesses to educate them on the threat to their intellectual property and, by extension, national security, and we must do it early.

Protection of Critical Technology

Under the 2019 National Defense Authorization Act, Congress required the Secretary of Defense to establish cross-functional teams to tackle specific high-priority initiatives and complex problems that crosscut the Department of Defense (DoD) enterprise. In 2018, the Secretary of Defense chartered one such group, aptly named the Protecting Critical Technology Task Force (PCTTF). Its goal is to secure the defense industrial base and the research and development enterprise by **preventing loss of classified and controlled unclassified information, as well as inhibit the data exfiltration** of trade secrets by foreign adversaries. The PCTTF immediately began working on new standards to integrate security and intelligence into the requirements development and acquisition process, as well as developing strategies to counter foreign threats to secure national security and America's military superiority.

At the same time the DoD created the PCTTF, the Secretary of the Army established AFC to address several challenges to modernization, including a dispersion of effort and inability to modernize at speed or scale. This lack of unity of command and accountability, combined with the loss of information and intellectual property that Congress had identified, have begun to erode the lethality and survivability of Army forces. Thus, AFC's mission was not only to focus on modernization strategies but also to deliver the investments uncompromised.

AFC immediately began assessing technology protection gaps in the Army acquisition, security, and intelligence enterprises. Drawing from best practices of sister organizations and the expertise of PCTTF members, a multi-disciplined team created a plan to improve the protection of early technology development. This new strategy focuses on weaving security, intelligence, and counterintelligence into the acquisition process during the ideation process. AFC's science and technology investments now focus on key modernization efforts approved through a single command structure instead of disparate offices that lacked a cohesive vision.

This process allows our researchers and technologists to understand the existing and future battlefield gaps identified by intelligence and threat analysts, not just the collaborative research world, which can lack connection to the Army mission. Further integrating intelligence into science and technology planning allows the assessment and mitigation of threats before the initiation of new programs and iteratively throughout a project. Security experts are involved in the early research planning to validate appropriate acquisition strategies and funding mechanisms, develop protection measures, and ensure the appropriate application of multi-disciplined security constraints throughout each phase of work. Each of these efforts is designed to ensure future fielded systems can truly be delivered uncompromised.

Development of More Stringent Disclosure Programs

Weaving security, intelligence, and counterintelligence into the acquisition process during the ideation phase includes the introduction of security policies and tools such as disclosure guidance. AFC's disclosure program initiative created an analytic template for new and current technology development efforts. The template is a four-step process, described in detail below:

- ◆ Analysis and data identification.
- ◆ Audience category identification.
- ◆ Risk analysis and disclosure development.
- ◆ Dissemination.

Analysis and Data Identification. This step begins with the completion of a science and technology protection plan, which requires identification and a vulnerability assessment of critical enabling technologies, followed by a selection of countermeasures to mitigate the identified risks. Following this is the use or creation of a program protection plan. The creation of this plan requires the identification of critical

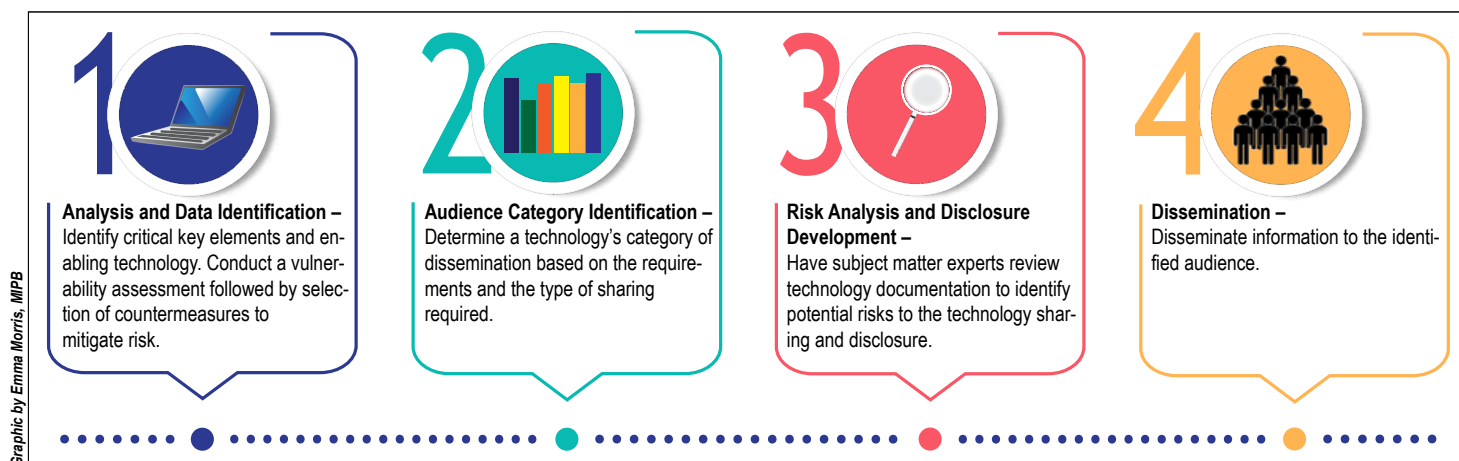
program information, controlled technical information, critical supply chain elements, and any horizontal protection considerations. When complete, the analysis and data identification process will have identified and documented key elements of technology that may be deemed—

- ◆ Revolutionary.
- ◆ Critical to system performance.
- ◆ Perishable (easily countered).
- ◆ Enabling to other systems.
- ◆ Sensitive to supply disruptions.
- ◆ Sharable with industry or foreign partners.
- ◆ Enabling for another DoD system.

Audience Category Identification. Audience category identification is a deliberate process to differentiate between categories based on requirements and the type of sharing required. Coordination with subject matter experts (SMEs) is essential to the successful execution of audience categorization. The following dissemination categories should be considered at the inception of every development effort:

- ◆ **Public dissemination:** Unlimited dissemination—known to be a source for adversary and partners alike.
- ◆ **Controlled dissemination:** Dissemination under controlled unclassified information specific to technology developments and used to protect information within audiences that have a need-to-know.
- ◆ **Limited dissemination:** Dissemination limited to specific audiences such as partner nations, briefings/symposiums, contractors, and academia.

Identifying the audience of a technology development effort from inception and maintaining that information throughout the life cycle of a technology development fosters effective communication while protecting information key to the sustainment of a U.S. technological advantage.



A stringent disclosure program is a fundamental safeguarding solution to the U.S. Army Future Command's modernization strategy.

Risk Analysis and Disclosure Development. Risk analysis occurs once a technology is mature and after identification of data sharing requirements. The risk analysis includes gathering the appropriate documentation on the technology and having SMEs review the information to identify potential risks to technology sharing and disclosure. The SMEs include—

- ◆ Technology owner representatives.
- ◆ Program managers.
- ◆ Technology SMEs.
- ◆ Research and technology protection officers.
- ◆ Foreign disclosure officers.
- ◆ Operations security officers.
- ◆ Information security officers.
- ◆ Legal staff.

The SMEs determine risk based upon the state of technology, type of application, audience required for continued development and integration, plan for transfers to foreign partners, and anticipated disclosure. With the appropriate documentation in place, the SMEs conduct a comprehensive analysis to determine the risk to adversary exploitation. The following are some the documents that should be available for the analysis:

- ◆ Science and technology protection plan.
- ◆ Security classification guides (draft or approved).
- ◆ Program protection plan.
- ◆ Critical information lists.
- ◆ Critical programs and technologies list.
- ◆ Horizontal protection list.

Dissemination. The final step is disseminating information to the required audiences and using the classification guide

or other controls that were established based on the risk analysis.

Conclusion

Securing the modernization efforts that will transform our force to compete in the future operational environments is not an easy task. Understanding how the threat to our modernization efforts has changed, understanding the ability of potential adversaries to inform our science and technology efforts, and protecting our intellectual property from inception to fielding and sustainment are all key factors for success. AFC and its partners are leading the way to change the existing paradigm and build a flexible process that adjusts to the ever-changing threat environment. 🌟

Endnotes

1. Sherisse Pham, "How much has the US lost from China's IP theft?" CNN Business website, March 23, 2018, <https://money.cnn.com/2018/03/23/technology/china-us-trump-tariffs-ip-theft/index.html>.
2. Tara Francis Chan, "FBI director calls China 'the broadest, most significant' threat to the US and says its espionage is active in all 50 states," Business Insider, July 18, 2018, <https://www.businessinsider.com/fbi-director-says-china-is-the-broadest-most-significant-threat-to-the-us-2018-7>.
3. Andrea Murphy, Hank Tucker, Marley Coyne, and Halah Touryalai, "Global 2000, The World's Largest Public Companies," Forbes, May 13, 2020, <https://www.forbes.com/global2000/#612237ff335d>.
4. James McBride and Andrew Chatzky, "Is 'Made in China 2025' a Threat to Global Trade?" Council on Foreign Relations website, May 13, 2019, <https://www.cfr.org/backgrounder/made-china-2025-threat-global-trade>.
5. *China's Non-Traditional Espionage against the United States: The Threat and Potential Policy Responses: Hearings before the Committee on the Judiciary United States Senate* (2018) (statement of John C. Demers, Assistant Attorney General, National Security Division, U.S. Department of Justice), 5, <https://www.judiciary.senate.gov/imo/media/doc/12-12-18%20Demers%20Testimony.pdf>.

The Directorate of Intelligence and Security, U.S. Army Futures Command, orchestrates the evaluation and assessment of current, emerging, and future threats and the development of the operational environment; synchronizes multi-disciplined technology protection activities; and conducts intelligence and requirements integration for the Future Force Modernization Enterprise to build a multi-domain operations (MDO)-capable force by 2028 and an MDO-ready force by 2035.



On 12 December 1776, the Continental Congress authorized the formation of the 2nd Continental Light Dragoon Regiment. It served throughout the Revolutionary War as General Washington's reconnaissance and intelligence gathering organization. The 2nd Dragoons were so successful that in recognition of the unit's importance, today's Army intelligence insignia proudly displays a dragoon's distinctive helmet, and the year 1776 is a direct reference to formation of the dragoons.

Joint Operating Environment 2040

by Mr. Jeffrey Becker



I'd rather have decent answers to the right question than great answers to irrelevant questions.

—Andrew W. Marshall
American foreign policy strategist

Introduction

What is it about strategic and military change that the U.S. military should pay attention to? What is important, and what is merely interesting? The joint operating environment development effort addresses these difficult questions. Its objective is to collect, organize, and evaluate the world's best deep futures thinking and make it accessible and usable to concept developers and force designers across the joint force, as well as allied and partner militaries. This effort consists of both a process and a document—currently, the *Joint Operating Environment 2040*, also known as *JOE 2040*.

Background

This effort to build a common, joint-level view of the future operating environment has been ongoing for more than 15 years and has led to seven versions of the study. The U.S. Joint Forces Command, while under the command of Gen. James N. Mattis, originally wrote the joint operating environment document. Later, the Joint Staff J-7 (Directorate for Joint Force Development) took the lead to revise and publish it. The effort has always been highly collaborative. It has included the contributions of Service futures organizations, combatant commands, other government agencies, and international partners, as well as world-class experts, scientists, and other thinkers, working together to build an understanding of military change and its implications for joint warfare.

The Joint Operating Environment is intended to inform Future Joint Force Development throughout the Department of Defense. It provides a perspective on future trends, shocks, contexts, and implications for future joint force commanders and other leaders and professionals in the national security field.¹

Joint Operating Environment 2040 was published in January 2020. It is the U.S. joint forces' most recent perspective on the future operating environment and the implications that environment has for joint warfighting over the next two decades. This current edition differs from earlier versions in that its development resulted from a close and sustained partnership led by the Joint Staff J-7, Defense Intelligence Agency (DIA), and Joint Staff J-2. Service futures organizations strongly supported it, including the U.S. Army Training and Doctrine Command's Mad Scientist Program and Army Futures Command. It is also the first classified edition of the document.

The basis of the new joint operating environment is an "intelligence-driven, threat informed" view of the deep future. This approach reflects a new urgency to understand and address the growing threat of adapting great and regional power adversaries as described in the most recent National Defense Strategy and to arrest—as then-Chairman of the Joint Chiefs of Staff Gen. Joseph F. Dunford Jr. described it—the erosion of our qualitative and quantitative military advantages.² The first step in correcting our trajectory was to fully understand the problem from a joint force perspective. *Joint Operating Environment 2040* dives deeply into the changing character of warfare, our adversaries' approach to addressing this change through novel ways of war, and the implications of both areas for the joint force.

Changing Character of Warfare

Joint Operating Environment 2040 looks just beyond the horizon of the current National Defense Strategy and is anchored in the *Joint Strategic Assessment*, DIA's biennial baseline assessment of the mid- to long-term strategic environment. The joint operating environment takes the strategic conditions set out in the *Joint Strategic Assessment* and describes how these large-scale geopolitical changes might change the character of war. Several important trends are clear, from new and powerful great powers to newly empowered global non-state actors, each increasing their reach and ambition. Both will stress the international system. Instead of one clear military rival with competitive military capabilities or a decentralized collection of smaller-scale security challenges, the joint force will be confronted by a combination of peer-level military rivals, a wide variety of strategically significant non-state actors, narrowing technological advantages, and an increasingly crowded yet expansive and ill-defined battlespace.

The implications of these changes are that the joint force will see faster, compounding technological changes that will accelerate change in military capabilities. In some cases, the joint force will see a separation between military forces as the newest and most advanced units outclass 20th century military forces. Acceleration and separation will encourage increasing variation among military forces as they begin to experiment with new capabilities and combinations of capabilities to develop war-winning military advantages.

Evolving Adversary Ways of War

Potential competitors and adversaries are evolving and adapting their own armed forces to keep pace with this changing character of warfare. *Joint Operating Environment 2040* describes how several countries and violent non-state actors are reshaping their armed forces and developing a novel operational concept to address their goals and objectives. Not surprisingly, the United States is focusing on long-term strategic competition with great power

competitors. The most recent unclassified National Defense Strategy summary makes several things clear:

- ◆ China is modernizing its forces to coerce and reorder the Indo-Pacific region.
- ◆ Russia is expanding and modernizing its military forces.
- ◆ Rogue regimes such as Iran and North Korea are presenting new military and strategic challenges.
- ◆ Violent extremist organizations remain an enduring threat to the global order.³

The National Defense Strategy focuses the Department of Defense on the goals and objectives that China, Russia, and others are pursuing. *Joint Operating Environment 2040* focuses on how these competitors and adversaries might shape and operate the military instrument to pursue those goals. These evolving ways of war result in a number of pressing challenges for how the joint force envisions fighting, designing, and experimenting with new operational approaches that are intended to offset, or in some cases outpace, the capabilities of the joint force. In most cases, we see adversaries striving to improve their defenses in depth. We see a growing emphasis on operations that emphasize competition below the threshold at which the United States typically employs force. Finally, adversary operations often



We require a new approach to adaptation and innovation based on joint and coalition campaign outcomes.

emphasize the lethality and decisiveness of the opening stages of a conflict, increasing the risk of unexpected and unpredictable opening blows.

Implications for the Joint Force

The changing character of warfare, along with new and potentially disruptive adversary approaches to conflict, will increase the national security risk if the joint force fails to address these conditions and evolve. In light of these changes, the joint force will likely face challenges in the following ways:

- ◆ **Contested globally.** The joint force will face efforts to slow or halt its movement around the world, eroding its ability to project power in support of worldwide commitments.
- ◆ **Fractured and disintegrated.** Joint force linkages and connections will be attacked, resulting in incoherent, disjointed, and ultimately ineffective operations.
- ◆ **Outflanked in an expanded competitive space.** The joint force could be irrelevant to adversary operations focused on the coercion and disruption of opposing societies through information confrontation and other forms of pressure and influence.

Using Joint Operating Environment 2040

Joint Operating Environment 2040 represents the U.S. joint forces' commonly developed understanding of the future operating environment over the next two decades. This is an intelligence-driven view of the future operating environment and the implications of change. Close collaboration between the Joint Staff and DIA ensures that intelligence analysis drives our understanding of the military implications of strategic and technological change. Moreover, it is a source for problem sets that future joint and Service concepts are called upon to solve for the Nation.

Joint Operating Environment 2040 was written in the spirit of Andrew Marshall, dean of defense futurists, who noted, "accurate diagnosis is the best route to strategic prescription."⁴ *Joint Operating Environment 2040* strives to do this by illustrating new future global realities and adversary ways of war in order to assist force development and design across the Department of Defense. The challenges

Andrew Marshall, Founder of the Department of Defense's "Internal Think-Tank"

After studying economics at the University of Chicago, Andrew W. Marshall joined RAND [Corporation] in 1949 when the nonprofit research organization based in Santa Monica, California, was barely a year old. During his 23-year affiliation with RAND, he researched Soviet military programs, nuclear targeting, organizational behavior theory and strategic-planning, among other concepts.

"Andrew Marshall was one of the nation's most respected and far-sighted defense experts," said Michael D. Rich, president and CEO of RAND. "He was a gifted futurist and strategist who had mentored generations of researchers, both at RAND and beyond. His influence will be felt for years to come."

Marshall was the founding director of the Office of Net Assessment, which is referred to as the Department of Defense's "internal think-tank." It provides the secretary of defense with assessments of the military balance in major geographic theaters, with an emphasis on long-term trends, asymmetries, and opportunities to improve the future U.S. position in the continuing military-economic-political competition.⁵

found here are a foundational reference for concept-driven, threat-informed capability development across the joint force, Services, and combatant commands. ✨

Epigraph

Andrew Krepinevich and Barry Watts, *The Last Warrior: Andrew Marshall and the Shaping of Modern American Defense Strategy* (New York: Basic Books, 2015), 1.

Endnotes

1. "Joint Operating Environment," Joint Chiefs of Staff website, accessed 14 October 2020, <https://www.jcs.mil/Doctrine/Joint-Concepts/JOE/>.
2. Ryan Browne and Barbara Starr, "Dunford: Military risks losing its competitive edge," CNN.com, June 13, 2017, <https://www.cnn.com/2017/06/13/politics/dunford-trump-military-budget-senate/index.html>.
3. Office of the Secretary of Defense, *Summary of the 2018 National Defense Strategy of The United States of America*, n.d., <https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf>.
4. Krepinevich and Watts, *Last Warrior*, 91.
5. "Andrew Marshall, RAND Researcher Who Founded Department of Defense's 'Internal Think-Tank,' Dies at 97," RAND Corporation website, March 26, 2019, <https://www.rand.org/news/press/2019/03/26.html>.

Mr. Jeffrey Becker is a defense contractor for the Joint Futures and Concepts Directorate, which develops comprehensive views of the future operating environment and future concepts that address emerging and future joint operational challenges and capabilities.





Battlefield Development Plans: Threat Analysis Enabling Multi-Domain Operations

by Mr. Earl S. Bittner

Introduction

During this next decade, each of the U.S. Military Services will transition to the new multi-domain operations (MDO) joint warfighting doctrine. The genesis for this new doctrine arose as adversaries, who studied U.S. warfighting doctrine and its applications closely for the past 20 to 30 years, developed concepts and capabilities designed to undermine our strengths and seize upon our weaknesses. In response, the Army and joint forces examined these new threats and developed MDO as a counter. Just as intelligence drives operations, these new threats drove the development of MDO—a divergence from previous capabilities-based doctrines. The sophistication of the threats' capabilities and warfighting concepts meant we had to use a variety of analytical methods to derive the knowledge necessary to defeat adversaries. Understanding how the Army and joint force acquired this knowledge remains important for intelligence professionals because as the threat evolves, the Army must continue this analysis so that we maintain our ability to defeat these adversaries.

Background

During the counterinsurgency wars from 2001 to 2015, the U.S. Army and joint forces became adept at targeting personnel and terror/insurgent organizations. However, as our military reoriented from predominantly counterinsurgency operations to that of large-scale combat operations, it became clear that adversaries had made advances that necessitated a change in how we evaluated threats. This fact became even more evident in the 2016 *Russian New Generation Warfare Study*, for which the U.S. Army performed an in-depth analysis of this new threat.¹ To do the study, the Army referred back to the 1970s and 1980s when it used the battlefield development plan to visualize how the Army would fight the Soviets in particular scenarios.² We then combined guidance from the National Defense Strategy, assessments about the future operational environment, and information concerning the new near-peer great power competition to modernize the battlefield development plan and used it to support

MDO.³ In developing the new battlefield development plan, we discovered the force could no longer just identify the threat's centers of gravity and high-payoff targets and then strike them with overwhelming force from a relative sanctuary. The threat now protected their centers of gravity with redundant, integrated, highly capable systems that made their destruction difficult. They also improved their capability to neutralize our fires capabilities (air and ground) that we use to attack their centers of gravity. Furthermore, threats had developed new capabilities and concepts that enabled them to contest us across the length of the battlefield, in all domains and phases, in layered, networked systems with near-real-time responses. This meant we could no longer analyze one system and figure out how to attack and destroy it as we traditionally had done in the past. We now had to understand much more complex systems of systems (also known as complexes) with which we had limited practical experience.

Battlefield Development Plan Books

Book 1: Red Forces

Book 2: Blue Capabilities

Book 3: MDO Options "Blue vs Red"

Our Analytical Approach

To comprehend these new threats, we had to examine how they operated in all domains, how the new systems functioned, and how they were nested. We also had to gain an

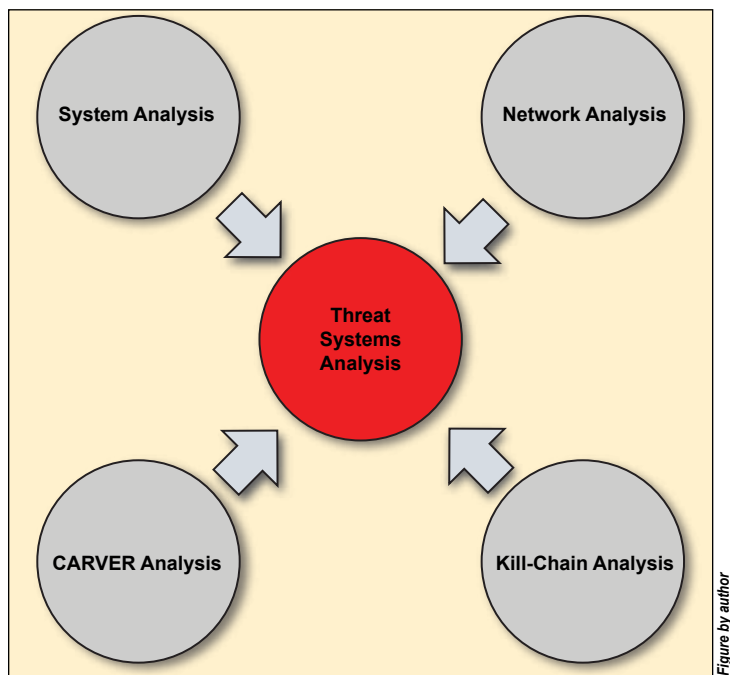
understanding of how the threats' networks operated and how redundancies were built into these networks. Another challenge was comprehending how our adversaries were using a whole-of-nation approach to war beginning in the competition phase. Further exacerbating these difficulties was the new level and sophistication that information operations brought to warfare. These are just some of the challenges posed by our adversaries that the Army and joint forces studied, and continues to study, and why we needed to analyze the threat using additional and new methods.⁴

We used analytical methods described in ATP 2-33.4, *Intelligence Analysis*, to analyze the problem set. However, given the complex nature of the threat, we had to build upon, modify, and combine analytical methods to achieve the threat comprehension required for the battlefield development plan.

We call the method we used to perform this activity *threat systems analysis*. It combines nodal/network; systems; criticality, accessibility, recuperability, vulnerability, effect, and recognizability (also called CARVER); and kill chain analytic methods with operational environment data across all domains and warfighting echelons to achieve an understanding of the threat's capabilities and vulnerabilities, and potential means for mitigation and exploitation, respectively. The method first involves understanding the system(s) and then applies that understanding to the specific operational environment.

The Concept

Since many of the emerging threats base their means of warfighting on systems warfare, our analysis began with gaining an understanding of the individual combat systems. These individual systems are normally integrated; therefore, we also viewed these systems as networks. Given the Army's recent experience and expertise in dissecting insurgent and terrorist networks, it was natural to apply counterinsurgency network analysis to this process. As in counterinsurgency network analysis, we identified nodes in the systems and networks, gained an understanding of the relationship between the nodes, and then sought to identify the strengths and weaknesses within the system and network. However, the increased complexity of systems networks over insurgent networks meant additional collection and analysis were required. With the built-in redundancies and nesting of these systems into systems of systems (or complexes), simply neutralizing select nodes would be insufficient.

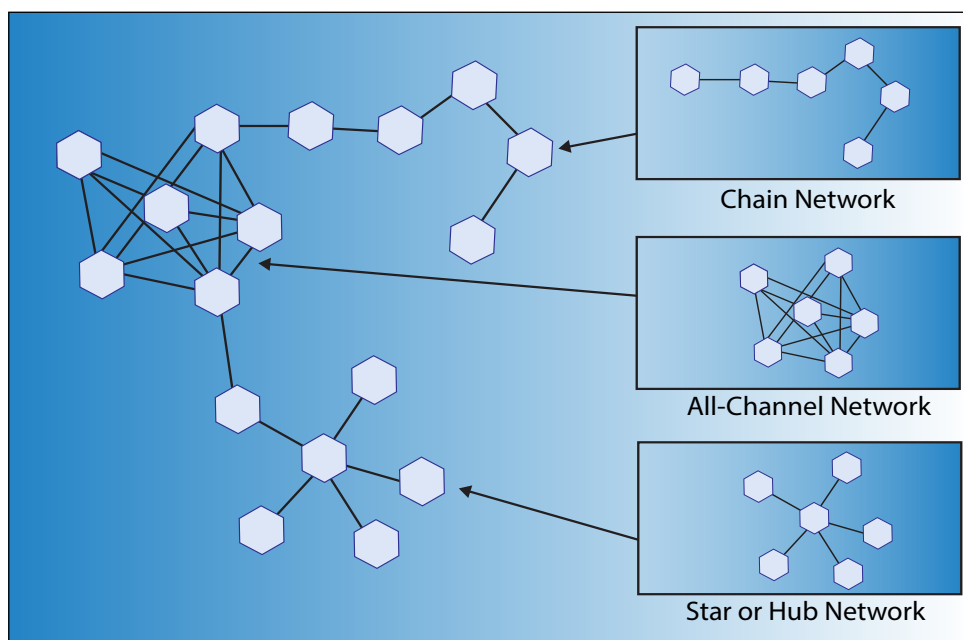


Threat Systems Analysis

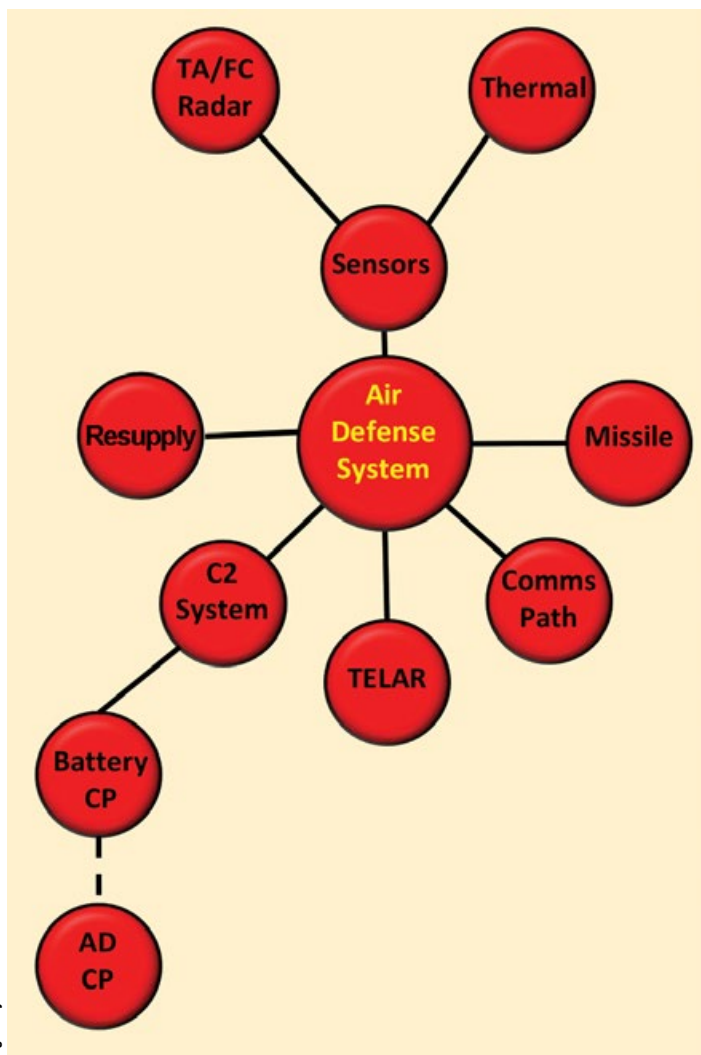
Figure by author

Next, we had to understand the process by which the systems performed their missions—the kill chain. We examined how systems went through the process from target detection, to engagement, to end of mission. This effort typically involved drawing more and more systems into the study. For instance, to understand the kill chain process of a multiple rocket launcher means you also need to understand how the unmanned aerial vehicle performs target acquisition, the communications system passes the data, the fire direction performs the fire mission calculations, and the command and control system makes a decision. Each one of these systems involved in the multiple rocket launcher's kill

chain has its own respective kill chain or information processes that needed to be examined to identify the best node or high-payoff target to neutralize. As part of this analysis of systems/complexes, it usually was not enough to simply strike one node; it was necessary to strike selected targets in a particular order. This is similar to how targets would be struck in counterinsurgency to achieve the greatest effect. Some targets must be struck simultaneously, others sequentially, and still others with a combination of both. In each step of the process, we looked for opportunities to disrupt the system's kill chain processes and identified strengths to circumvent.



Networked Organization and Structure Analysis⁵



Threat System Nodal Analysis Example

Within this context, we next examined how each of these system complexes operated within the larger battlefield framework at the tactical, operational, and strategic levels. We identified the threat's means of integrating the force, and contingencies should their primary means be disrupted or neutralized. Once we gained a strong understanding of the threat's systems, networks, and processes, we identified potential areas in which the force could affect the threat.

At this point, the process of analyzing the threat became interactive between operational and intelligence personnel. The operational analysts—experts on the future force and capabilities—identified the means to exploit the vulnerabilities, while the intelligence analysts helped refine the best manner of exploitation. In some cases, the

operational personnel developed entirely new capabilities and tactics, techniques, and procedures (TTPs), thereby creating vulnerabilities in threat systems not previously identified. Of course, as the threat continues to evolve, so too will the means to address the threat and the need to reexamine the threat.

Resources Used

In performing the analysis, we contacted a large number of organizations to fuse together each organization's expertise. A key starting point for the analysis was the joint country force assessments, which are the Defense Intelligence Agency's estimates of select countries' military forces projected into specific timeframes. This estimate aggregates Department of Defense intelligence organizations' assessments of force structure, capabilities, and disposition of forces over the specific time period. Next, to gain an in-depth understanding of systems, we consulted each Service's intelligence organizations, augmented by other national agencies as needed, to fully understand how a particular threat system operated.

Threat analysts supporting capability development are charged with basing their estimates on the current operational environment and projecting them into the future. Therefore, building off our understanding of current systems, we consulted combatant commands, current threat Army techniques publications, U.S. Army Training and Doctrine Command G-2's Foreign Military Studies Office, think tanks, other organizations with specialized subject matter expertise, and lessons learned from current operations to determine the threat's kill chains and TTPs. We then projected them into the future.

Once we gained as much understanding of the threat systems we could attain, we dissected the components, networks, and nesting of systems to determine the strengths and weaknesses. To perform this examination, we consulted Services' and combatant commands' CARVER target analysis⁶ of the projected threat in order to determine

prioritization and effectiveness of each target node. As stated earlier, as the threat suffers losses, it will employ contingencies that will have second order effects that can then change CARVER calculations and therefore next targeting plans. It is also in this stage that we had to deeply consider the operational environment. Even if the threat

Kill Chain*

- ◆ Indicators and Warnings Intelligence
- ◆ Target Detection
- ◆ Target Acquisition and Tracking
- ◆ Target Assignment
- ◆ Target Engagement
- ◆ Assess and Re-attack

*Modified as needed to fit the system

TARGET SYSTEMS	Criticality	Accessibility	Recuperability	Vulnerability	Effect	Recognizability	Total
Bulk Electric Power	5	3	3	5	5	5	26*
Bulk Petroleum	5	3	5	4	3	5	25*
Water Supply	3	5	3	5	5	3	24*
Communications Systems	3	4	5	2	2	2	18
Air Transport	1	1	3	1	2	2	10
Ports and Waterways	1	1	3	1	1	1	8
Rail Transport	2	4	4	1	4	3	18
Road Networks	1	5	3	5	2	5	21
*Indicates target systems suitable for attack. In this example, the Bulk Electric Power target system has been selected.							

Strategic CARVER Matrix Application Example⁷

remained the same, a change in the operational area might necessitate a completely different targeting approach.

Next, we described this new threat to the operational and combat development force to examine how current systems could be used to exploit potential vulnerabilities. Where possible, the operational force applied and modified current capabilities to exploit future threat vulnerabilities. In some cases, this amounted to changing TTPs, and in other cases, it involved networking existing systems differently. For particularly vexing problem sets, it required the capability developers to develop new systems that could take advantage of the system(s) weaknesses.

At this point, the Army performed a series of Army and joint tabletop exercises and experiments to determine whether particular operational capabilities and TTPs would have the desired effects against targeted threat systems. The Army, and other Services, then refined capabilities and TTPs based on lessons learned from these events to best determine the way ahead. This evolution continues as the Services, warfighting functional proponents, and joint force continue to experiment and refine capabilities.

The Future

The process described serves as a baseline analytical method for the battlefield development plans used to support MDO concept and capabilities development and is not intended to be an end-all, be-all solution, but rather a starting point. As mentioned earlier, when the operational environment changes, other approaches to neutralizing the threat may become more suitable—another reason for the continuous process and addition of analytical methodologies.

Systems that must be explored more fully as the future looms are the non-kinetic systems. These systems are the most challenging to replicate, model, and analyze. Some of this difficulty is due to the sophistication of systems in various operational environments, some is due to our lack of information concerning both threat and friendly systems, and some is due to classifications of information. Fortunately, this problem works both ways and is more vexing for potential threats because their understanding of the full effects of non-kinetic weapons is almost certainly much less complete.

Another area requiring greater focus is competition. While the U.S. industrial-defense complex has spent many decades and trillions of dollars studying threats and developing weapons for combat, in comparison, an infinitesimal amount has been applied to analysis, activities, and systems for the competition phase. Since much of our success in MDO is contingent on activities performed during competition, it is important for the intelligence community to study competition and better learn how we may influence events that will affect activities in conflict. This will likely require the incorporation or creation of additional analytic methods.

A more effective and efficient means to perform experimentation and tests will help advance our analytics. Currently, in order to run an experiment to validate capabilities and concepts, one often needs months of preparation and thousands of man-hours to simply test various elements on new concepts and doctrine. This means there is significant lag time between performing our analysis and testing whether our analytical conclusions were valid. On the other hand, when we used less sophisticated means of

experimentation, it is often oversimplified and can lead to incorrect conclusions. Advances in modeling and simulation will enhance our ability to analyze and more rapidly learn.

As the Army, other Services, and joint force continue to gain a better understanding of the threats systems, the threat is doing the same. Therefore, as part of this feedback loop, the intelligence community continues to refine data as the threat's capabilities change and are refined. Ultimately, this threat systems analysis is a living process, and it will aggregate analytical methods into the process in order to solve new problems brought about by the evolving threats. ✨

Endnotes

1. Department of the Army, *Russian New Generation Warfare: Unclassified Summary of the U.S. Army Training and Doctrine Command Russian New Generation Warfare Study* (Fort Eustis, VA: Training and Doctrine Command, n.d.), <https://www.armyupress.army.mil/Portals/7/online-publications/documents/RNGW-Unclassified-Summary-Report.pdf?ver=2020-03-25-122734-383>.

2. Eric J. Wesley and Jon Bates, "To Change an Army—Winning Tomorrow," *Military Review* 100, no. 3 (May–June 2020): 6–17, <https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/May-June-2020/Wesley-Winning-Tomorrow/>.

3. Eric J. Wesley and Robert H. Simpson, *Land Warfare Paper 131, Expanding the Battlefield: An Important Fundamental of Multi-Domain Operations* (Arlington, VA: The Association of the United States Army, April 2020), <https://www.ausa.org/sites/default/files/publications/LWP-131-Expanding-the-Battlefield-An-Important-Fundamental-of-Multi-Domain-Operations.pdf>.

4. Department of the Army, *The Battlefield Development Plan: Field Army, Corps, and Division in MDO 2028* (Army Futures Command, June 2020).

5. Figure is adapted from Figure IV-4, Network Structure, Office of the Chairman of the Joint Chiefs of Staff, Joint Publication 3-25, *Countering Threat Networks* (Washington, DC: The Joint Staff, 21 December 2016), IV-11.

6. Christopher M. Schnaubelt, Eric V. Larson, and Matthew E. Boyer, *Vulnerability Assessment Method Pocket Guide: A Tool for Center of Gravity Analysis* (Santa Monica, CA: RAND, 2014), https://www.rand.org/content/dam/rand/pubs/tools/TL100/TL129/RAND_TL129.pdf.

7. Department of the Army, Army Techniques Publication 3-05.20, *Special Operations Intelligence* (Washington, DC: U.S. Government Publishing Office, 3 May 2013), 2–11 (common access card login required).

Mr. Earl Bittner is an intelligence specialist assigned to the U.S. Army Training and Doctrine Command G-2 Operational Environment Integration Directorate and threat author for the Russian Battlefield Development Plan. He is a retired U.S. Army intelligence officer with 22 years of service, multiple deployments, and experience in a variety of analytical assignments.



The Army Intelligence Museum acts as custodian and repository for artifacts significant to the history of intelligence organizations, operations, and individuals and provides military history education. The museum highlights the role of Military Intelligence within the U.S. Army from 1775 to the present day and honors the achievements of Soldiers acting in intelligence roles. Museum exhibits include a World War II German Enigma cipher machine, a large fragment of the Berlin Wall, a vehicle operated by the U.S. Army Military Liaison Mission during the Cold War, and signals intelligence gear used by the Army Security Agency. The museum also displays of manned and unmanned intelligence aircraft at the outdoor Air Park on Hatfield Street.

Check out the MI Soldier Heritage Learning Center website at:
https://history.army.mil/museums/TRADOC/fortHuachuca_MI

Russian Perspective and Operational Framework

by Mr. David P. Harding, Colonel David Pendall (Retired), and Lieutenant Colonel Steven J. Curtis

Introduction

In the European theater, we sometimes find Russian motives and actions confusing. We can readily identify that they are competing with the West in all domains, yet we struggle to characterize Russian activity as aggressive, defensive, provocative, or simply prudent. Moreover, we have difficulty classifying their actions, using the terms interchangeably such as *asymmetric*, *irregular*, *hybrid*, and *gray zone*. In order to understand and describe their behavior, we must view the strategic operational environment through their perspective. This article summarizes a tool we have used in the U.S. Army Europe G-2/66th Military Intelligence Brigade analysis and control element to help us understand Russian actions.

The Ambiguous Strategic Environment

Among intelligence analysts and defense intellectuals, there is a thriving discussion about new technologies, the changing character of war, and the blurring spectrum

of conflict. We are struggling to understand our competitors' actions as they increasingly explore ways to sidestep Western military might. The ambiguous strategic environment generates increased risk for miscalculation and demands a shared understanding of Russia's means to ends to enable the Army to compete and win in multiple domains.

The multi-domain operations construct posits that our competitors will engage us using all means necessary to achieve their political objectives. The competition phase is critically important for them because, like most nations, they do not want to go into armed conflict if they can achieve their goals in the competition phase. Therefore, they employ a broad range of options, drawing from their total capabilities, both military and non-military, to achieve their ends. As they attempt to mitigate our strengths and gain advantage, they make every effort to remain below the threshold that would trigger armed conflict (Figure 1).

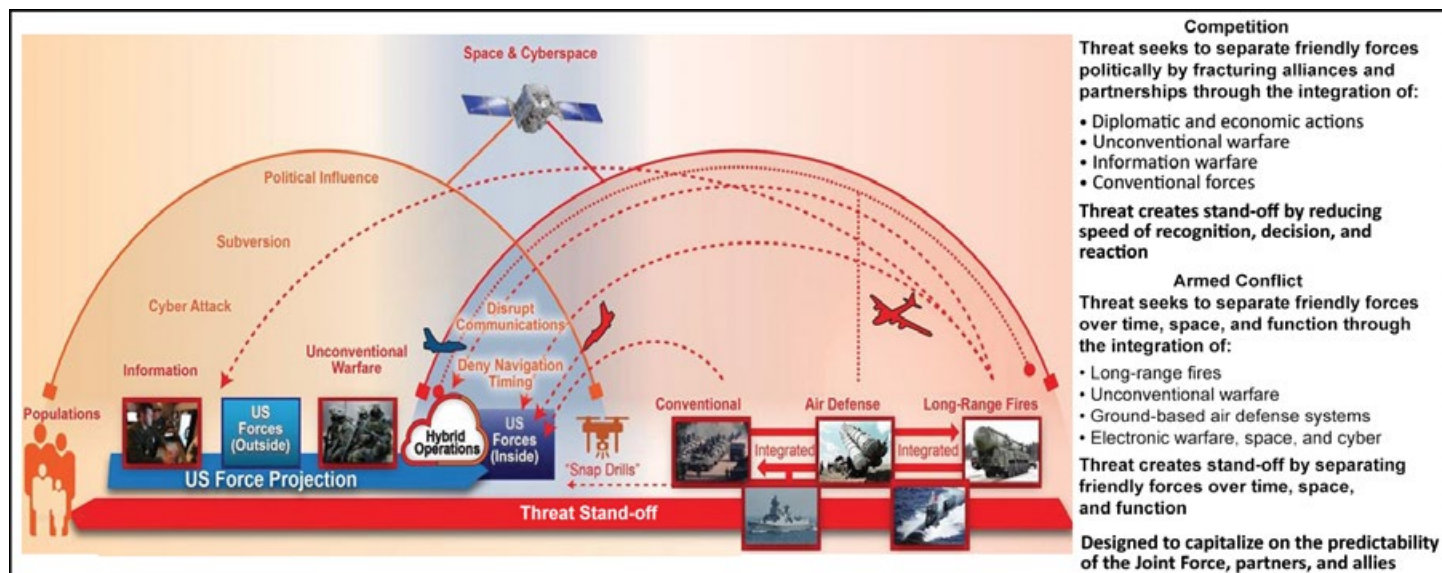


Figure 1. China and Russia in Competition and Armed Conflict¹

Ultimately, what we observe the Russians doing in the United States European Command (EUCOM) area of responsibility is rooted in history. The principles of war remain unchanged, and the strategic objectives of combatants and/or competitors, if they change at all, remain largely constant over time. What compounds our confusion about Russian actions is the observable fact that the Russians are leveraging the whole of Russian society to apply modern capabilities/technologies in creative ways to established concepts. They are intentionally blurring the line between competition and conflict by applying not strictly a whole-of-government but rather a “whole-of-Russia” approach that comprises elements outside the Russian government. Applying some basic intelligence preparation of the battlefield (IPB) elements can help clear up some of the mystery by looking at Russia’s theater campaign from the operational level of war.²

Russia does not have a monopoly on realpolitik—almost all nation states act pursuant to their survival, applying all elements of power to ensure regime survival, expand wealth, and advance their nation in the international system. Russia is a nation state with its will and means coalesced under a ruling power structure that is less democratic than we prefer—enabling greater agility and capacity to meet challenges with a whole of society response. For contrast, the United States demonstrated the power of its will and means working in concert in World War II, followed by a whole of Western society containment strategy in the Cold War. Since the end of the Cold War, the West has rightfully focused its attention on violent extremism, presenting an opportunity for Russia, and China, to modify their strategy to address a Western military overmatch.

The Russian Perspective

As the Russians look over the horizon to the west, what they see since the Soviet collapse in 1992 is a loss of substantial operational depth that has subsequently been backfilled by North Atlantic Treaty Organization (NATO) expansion and more recently by the deployment of additional NATO ground forces. For historical reasons, the operational depth afforded by the occupation of Eastern Europe figured prominently in Russian security; now a potential threat from the West is no longer 2,000 kilometers away—it is 600 kilometers to Moscow, a net loss of 870 miles. Former Defense Secretary Mark Esper’s July 2020 announcement regarding the relocation of United States land forces from Germany to Poland only corroborates Russia’s fear. A theater strike capability from air and sea comes from across the Atlantic and over the Arctic and polar cap, compounding Russia’s threat perception. Figure 2 (on the next page) represents what might be Russia’s perspective of NATO and European Union activities currently and since the 1990s.

The map shown in Figure 3 (on the next page) is straight from Russia’s National Security Strategy of 2015. As should be clear from the highlighted entries, the threat from NATO that Russia perceives is heavily in its security calculus. The annotations on the map also make clear that the Russians remain very concerned about conflict and instability in Southwest Asia, especially the threat from Islamic extremism from the north Caucasus. Russian Foreign Minister Sergey Lavrov recently articulated these concerns when reflecting on the United States-NATO exercise DEFENDER-Europe 20: “Although the entire space there is oversaturated by military facilities and weapons, although NATO’s eastward expansion has already created serious problems in the field of strategic stability in Europe, the merger of NATO and the [European Union] EU is continuing. NATO members have been trying to hold joint exercises and trying to plug in neutral EU members, such as Finland and Sweden.”³

Russian Ground Force Dispositions

As part of their effort to organize the operational environment, the Russians divide it into three zones: the disruption zone is roughly equivalent to our deep area; the battle zone is roughly equivalent to our close area, and the support zone is the equivalent of our rear area. The battle zone is where the conflict and the competition for resources and allies take place in what the Russians call the “near abroad,” or the former Warsaw Pact states and the former Soviet Republics lost after the Soviet collapse.

After many years of insufficient political backing and re-sourcing, the poor performance in 2008’s small war with Georgia focused Russia’s military leadership, and force modernization efforts began in earnest. They gave initial priority to units in the Southern Military District to contend with the Islamist threat in the North Caucasus. More recently, Russia has reconstituted a number of heavy divisions along the border with Ukraine and NATO’s eastern flank.

In addition to building up its ground forces capabilities in the Western and Southern Military Districts, Russia has constructed a complex system of air defense and fires based on the Russian exclave of Kaliningrad. As can be seen from the map in Figure 4 (on page 47), it provides a complex, layered, and redundant antiaccess and area denial capability with complementary fires that can range virtually all European port facilities. Similar efforts are underway in Crimea as Russia attempts to reconstruct a protective glacis in the western, southwestern, and southern strategic directions.

Although our (U.S. Army Europe) focus is primarily on Russian land power, or ground forces activities in EUCOM’s area of responsibility, we are aware of and monitor Russia’s

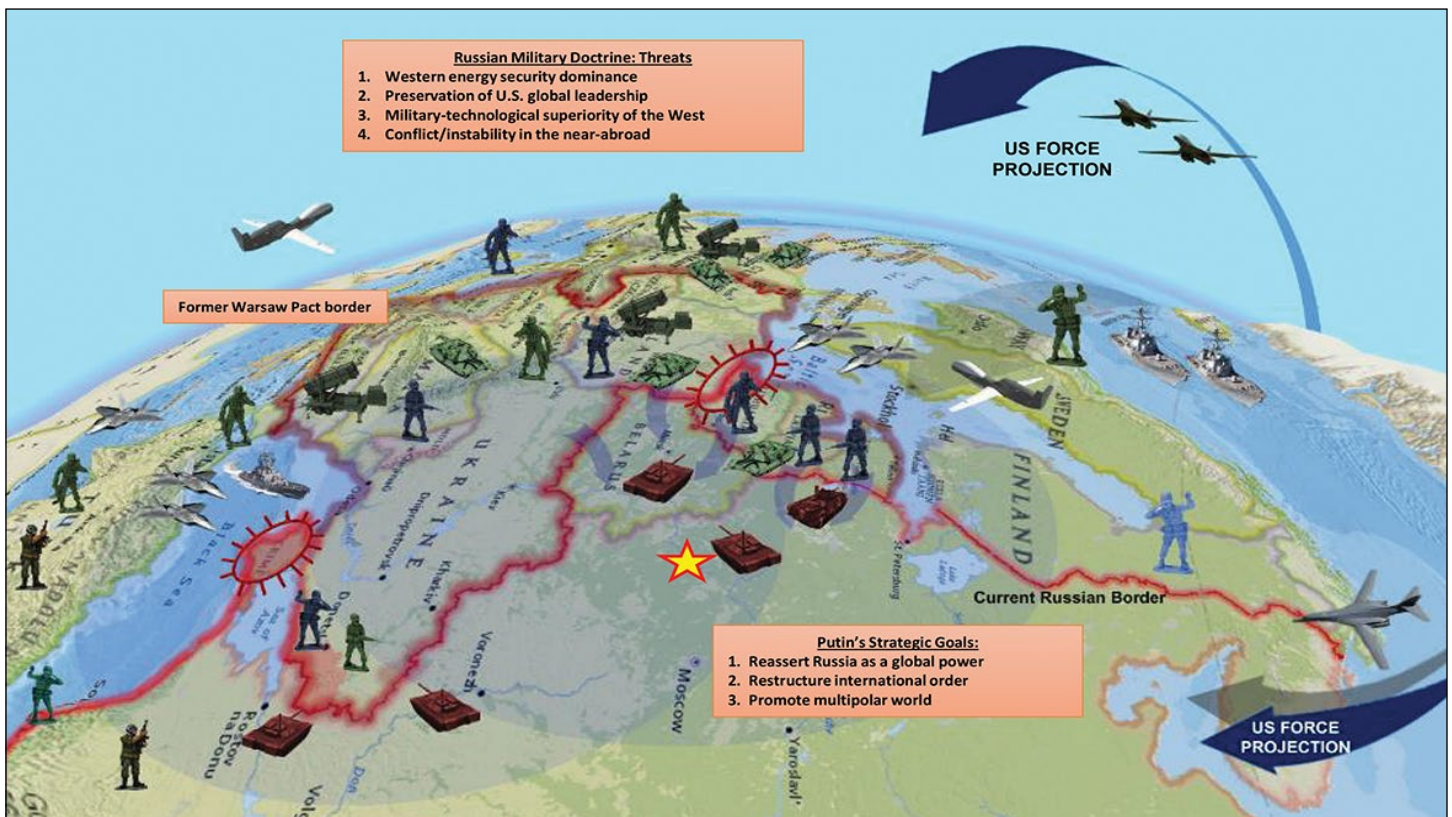


Figure 2. The Russian Perspective⁴

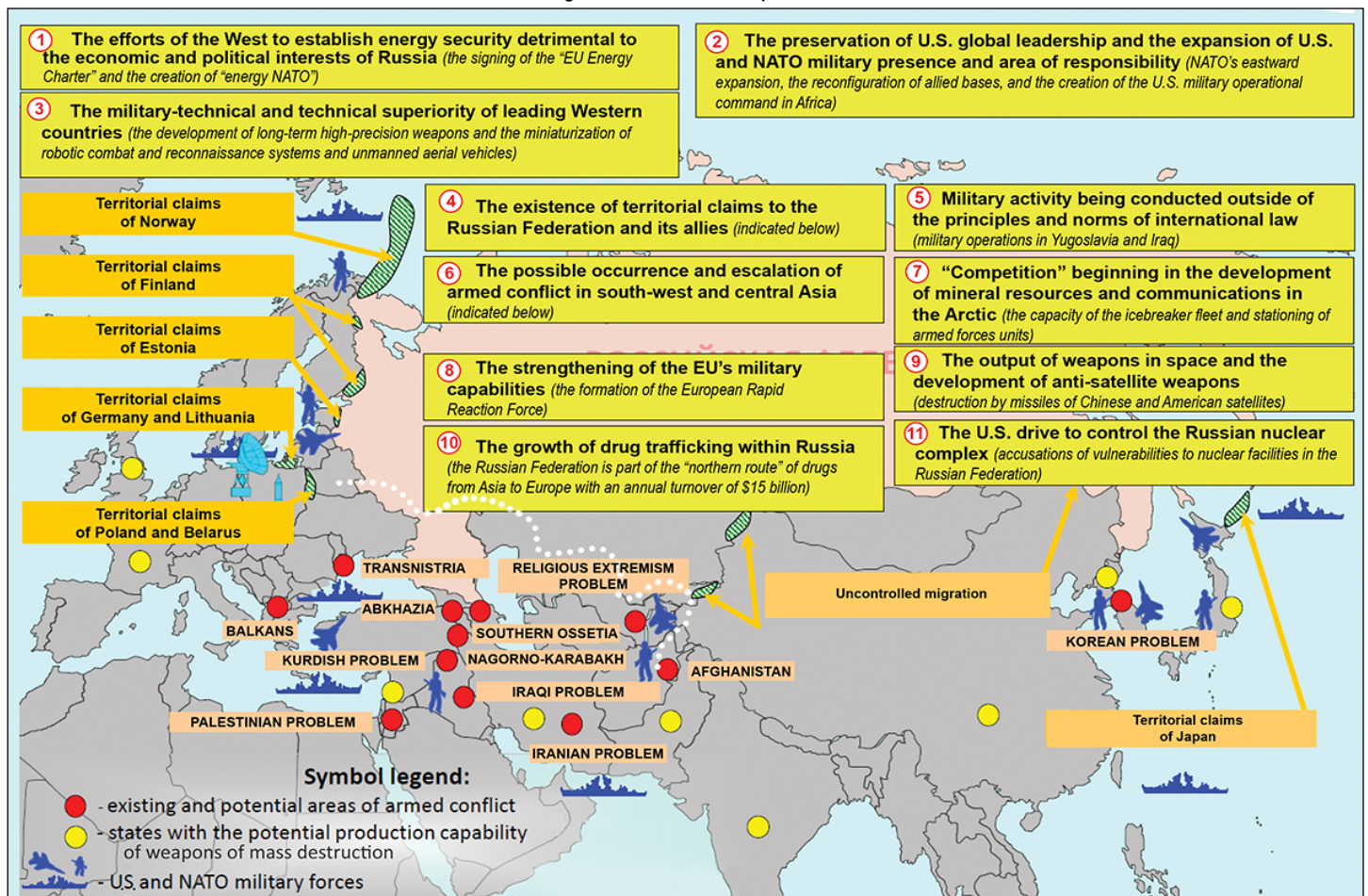


Figure 3. The Russian Perspective: Threats to the Military Security of the Russian Federation⁵

activities across the diplomatic, information, military, and economic spectrum, also known as DIME (Figure 5, on the next page). The activities listed in the figure are primarily everyday observables, and we could classify them as tactical moves. As should be clear from the figure, Russia’s military activities in the area of responsibility comprise just a small percentage of the Russian Federation’s activities. This list is meant to be representative, not comprehensive. Still, it represents a broad spectrum of activity, some of which is normal statecraft, some of which is aggressive and/or illicit. As mentioned earlier, the Russians intentionally blur the lines between the two. Our challenge is that while we generally have fairly good fidelity on Russian activities from which we can compile and catalog long lists of actions, how do we connect means to ends?

A long list of activities constitutes a lengthy catalog of measures of performance, which can result in confusion—how to sort out what the Russians are doing and why? By bridging the gap at the operational level and connecting means to ends, we can clarify what the Russians hope to accomplish and make better sense of seemingly unconnected or discrete activities across the area of responsibility. Ideally, with better understanding, we can begin to anticipate our adversary’s future moves.

We can expand warfighting functions to many forms of competition.⁶ For instance, if one were going to start a car dealership, one would need first to do market research (intelligence) to determine where to set up. Advertising is necessary and could be considered a form of information operations (fires), and we would need to find sources for inventory, electricity, warehouses, and showrooms (sustainment). Someone would have to be in charge and have responsible individuals on hand to perform various functions to keep things running (mission command). Another example might be a political campaign during which surveys are conducted and demographic data collected (intelligence), a campaign manager and their staff appointed (mission command), and advertising bought and disseminated (fires), and so on.

Warfighting Function	Activities (Linear Warfare) (Nonlinear Warfare)
Mission Command	Command post exercise/field training exercise/fast-reaction exercise, mobilization of reserves Russian society, transportation infrastructure, economy, industrial base
Movement & Maneuver	Georgia, Ukraine, Syria, long-range aviation, maritime Political system funding, candidates; “lawfare;” International bodies: Organization for Security and co-operation in Europe, United Nations, Collective Security Treaty Organization, Eurasian Economic Union, Shanghai Cooperation Organisation
Intelligence	Financial Stability Board, Main Intelligence Directorate (GRU), Special units (SPETSNAZ) active internal, external; unmanned aircraft systems, long-range aviation, maritime; penetration of NATO allies, partners Cyber exploitation, Night Wolves, criminal organizations, commercial enterprises
Fires	Artillery, cruise missiles Information operations, cyber, electronic warfare, economic, political
Sustainment	Mobilization of Russian society, transportation infrastructure, economy, industrial base; demographic manipulation external (ethnic support zones)
Protection	New ground forces divisions, counter force and force disruption capabilities, hardened facilities Conspicuous firings, leadership refresh; creation of multiple, redundant security organizations; National Guard, frozen conflicts, crowd/riot control, political assassination, suppression of free press, internal Russian narratives, media control, banning of Western non-governmental organizations in Russian Federation

Figure 6. Russian Activities Categorized as Warfighting Functions

Figure by U.S. Army Europe G-2 Analysis and Control Element

The Operational Environment and Framework

Importantly, the Russians do not use “warfighting functions” as a doctrinal construct,⁷ but we choose to bin what we see them doing in a construct familiar to us as a conceptual handrail for our own basic understanding. If we take what the Russians are doing, and bin their activities across the warfighting functions, it helps to simplify the picture. The warfighting functions depicted in black in Figure 6 are what we would expect in a conventional military conflict, or in their concept “linear warfare.”

But, what we are confronting in competition bears more resemblance to their concept of “nonlinear” warfare or conflict. In competition, the Russians are taking a “whole-of-Russia” approach to apply new (modern) capabilities/technologies to established concepts. Plotting Russian activity in our operational environment—across the area of responsibility by warfighting function—looks something like what is shown in Figure 7 (on page 48).

Insert another caveat: We accept that using tactical symbology for an operational-level graphic is not doctrinally correct. However, feedback from a wide range of senior and allied audiences to whom we presented this concept convinced us there is value in using this framework to help visualize the operational environment in competition. From the map in Figure 8 (on page 49), with the warfighting functions plotted in time and space, we can derive this operational graphic for the area of responsibility.

(U) **RUSSIAN INTENT:** Russia's intent is to: (1) **expand** political and economic influence; (2) **destabilize** and undermine faith in Euro-Atlantic institutions; and (3) **assert itself** as a viable world power. From the Russian perspective, this is a defensive maneuver designed to regain its rightful place in the international order.

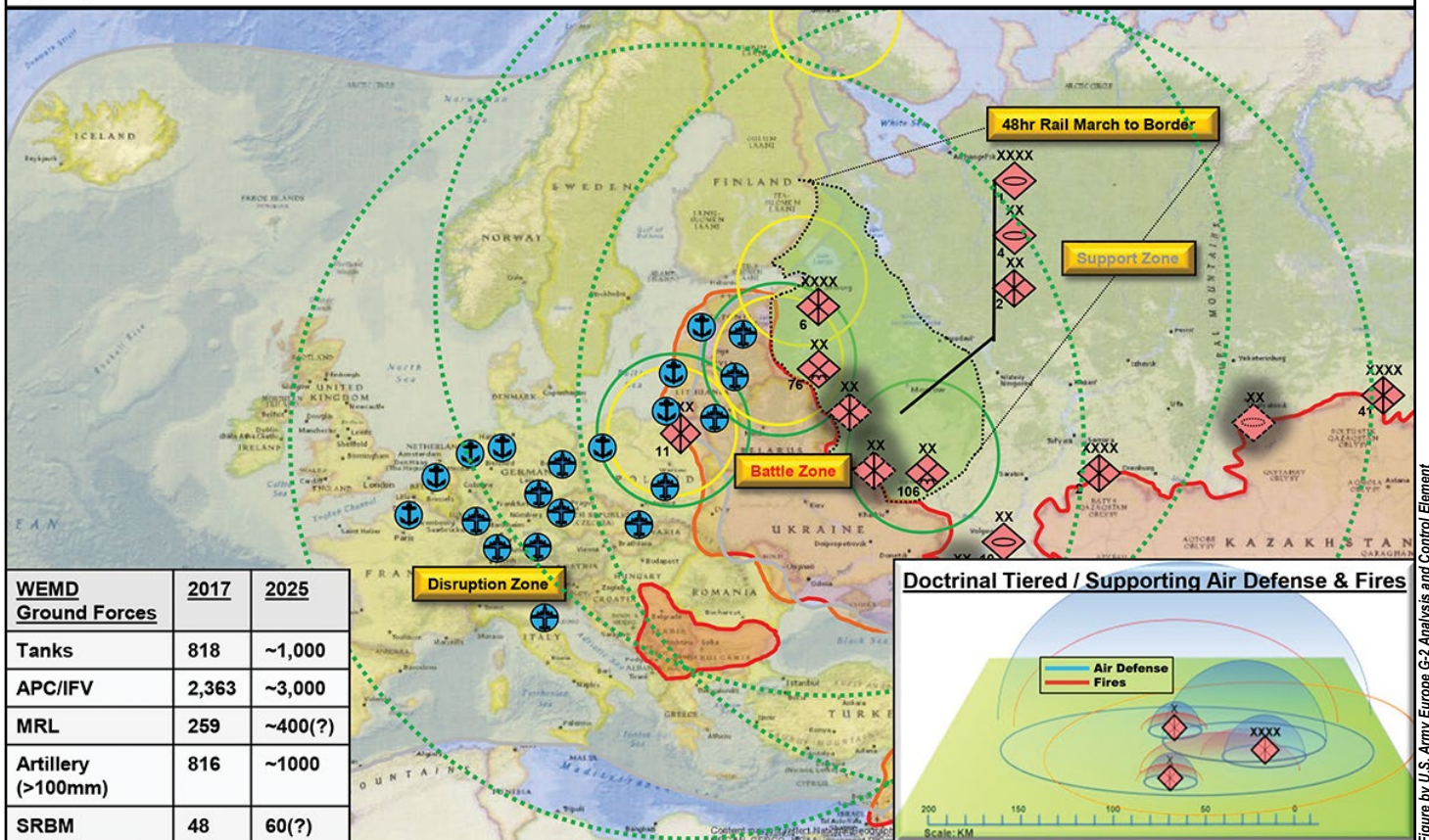


Figure 4. Russian Ground Force Dispositions in the Western Strategic Direction

ACROSS THE DIME

DIPLOMATIC

- Fund opposition parties
- Maintain "Frozen Conflicts"
- Persecute non-governmental organizations as foreign agents
- Leverage Russian Orthodox Church
- Pressure European Union leaders to reduce sanctions
- Utilize legal institutions to alter truth and challenge historical facts
- Exert bilateral pressure

INFORMATION

- Use Russian mass-media to spread inaccurate information and propaganda
- Foster ambiguity and multiple concepts of truth
- Monitor and censor domestic social media, use trolls, and filter external media
- Cyber disruptions and 'patriot hackers'
- Export Russian culture

MILITARY

- Exertion of military power along periphery
- Employ 'snap' and deliberate exercises
- Long-range Air Force and out-of-area Navy
- Maintain military bases in sphere of influence
- Employ Russian military capabilities in Ukraine

ECONOMIC

- Leverage oil, natural gas, enriched uranium dependency
- Weapons sales to non-European and European nations
- Counter sanctions and trade embargos

BLUF: Russia continues to influence Europe but has not undermined Euro-Atlantic cohesiveness. Economic ties between Europe and Russia remain important and prevent some nations from condemning Russian policy.

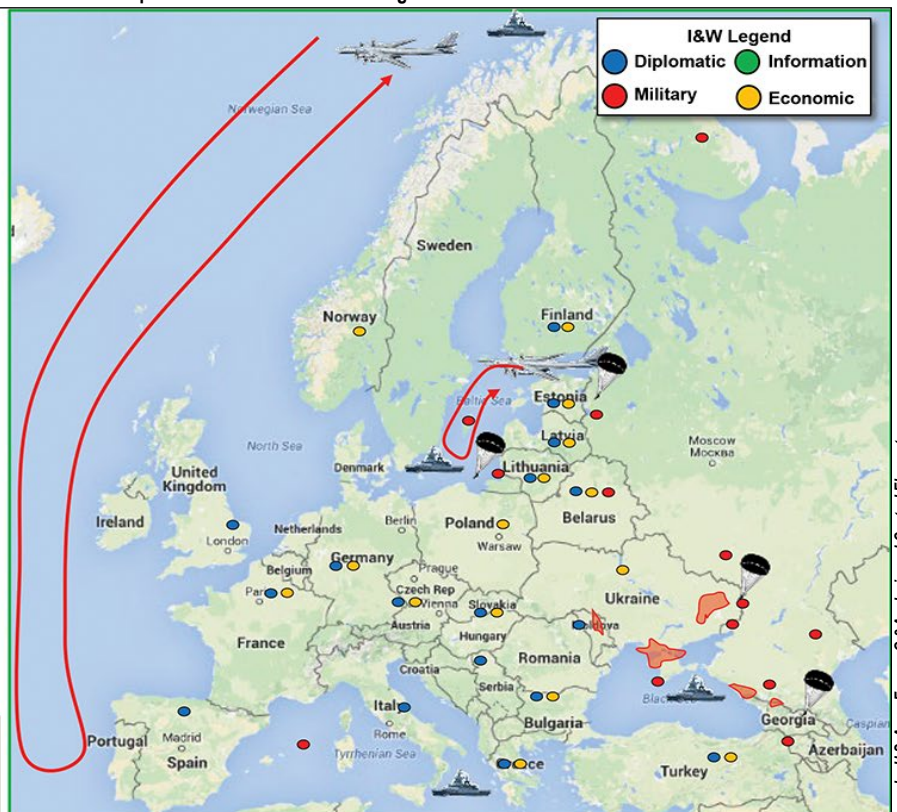


Figure 5. Representative Russian Activities in Competition

- ◆ **The decisive operation is to ensure regime survival.** Everything else is a supporting effort. This is normal nation state behavior, exhibited especially by nations with an autocrat at the helm who is preoccupied with both internal and external threats. Even in Western democracies, regime turnover creates staggering instability and presents a major security risk to a population.
- ◆ While focused on retaining key terrain, **Russia is committed to undermining the cohesion of NATO.** Russia is employing integrated operations (political, information, economic, and military) across multiple domains to *isolate* the Baltics, Turkey, and the Caucasus states while simultaneously conducting *disruption* in Scandinavia, NATO countries, and the Central Asian states. Creating fissures in NATO deprives the United States of its principal power projection platform and restores Russia's principal military strength—mass. The West created an opportunity when we misapplied our own worldview to Russia and assessed Russia as European after the collapse of the Soviet Union, seeking to bring them into the NATO tent in the fight against violent extremism. We were disappointed when Russia acted as a distinct Eurasian nation state, wholly apart from Western

- ◆ We see **Russia is aggressively conducting intelligence collection against its adversaries**, both foreign and domestic, throughout the breadth and depth of the area of responsibility and using intelligence, information confrontation, and influence to retain its own freedom of action and initiative in both the European regional and global contexts.

As a result of fixing NATO's attention on its eastern flank (Figure 9, on the next page), preventing Ukraine and Georgia from joining NATO, isolating Turkey through diplomatic advances and military cooperation, and staving off the collapse of Syrian President Assad's regime, Russia has created maneuver space for itself in Southwest Asia.

By financing opposition parties and conducting aggressive information operations in France and other European countries, Russia is attempting to undermine the cohesion of NATO and the European Union. The provision of medical supplies to Italy during the early days of the coronavirus disease 2019 pandemic is a form of Russian fires, or information operations. Using energy transfers to attain leverage over European partners is another form of fires or sustainment.

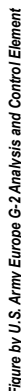


Figure 7. Visualizing the Operational Environment

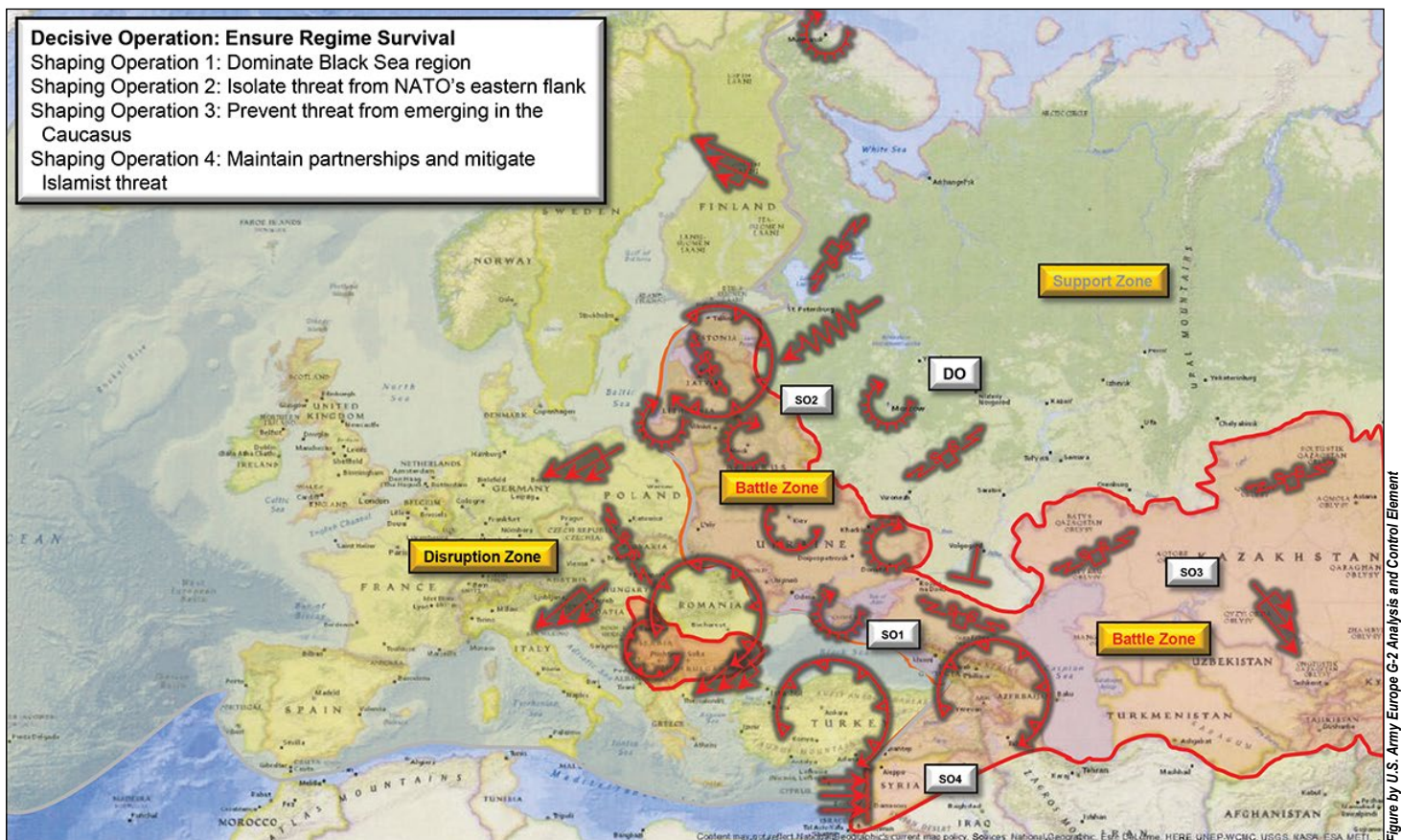


Figure 8. Russia's Operational Framework



Figure 9. Eastern Flank/Baltics

By applying pressure and intimidation on the Baltic, Russia has forced NATO to increase its forward force posture, which potentially undermines NATO's cohesion by putting additional strain on countries that have a primary threat focus on terrorism or illegal migration from North Africa.

In the Black Sea/Caucasus Region (Figure 10, on the next page), Russia wants to neutralize Ukraine as a threat while simultaneously keeping it out of NATO and other European institutions. Russia views retaining Crimea as vital to its strategic interests. A simple review of the geography reveals Crimea as key terrain. Applying pressure to Georgia keeps it isolated, while maintaining security cooperation with Armenia and supporting local conflicts helps Russia sustain its influence in this energy-rich region.

In the Balkans and along NATO's southern flank (Figure 11, on the next page), Russia is attempting to gather intelligence while undermining alliance cohesion using information operations and manipulating the refugee crisis. In addition, the Russians are providing military aid to Serbia in an attempt to isolate it from membership in western institutions. In Serbia, and in Bulgaria, Russia is using a shared cultural identity (Orthodox Christianity) as a lever between their populations and the West. The cumulative effect is to create a sense of isolation in Romania, an important NATO ally in the Black Sea region.

Conclusion

While it may appear the Russians are conducting a broad range of discrete actions across the Eurasian landmass, it is actually a campaign across the theater. The Russians are employing new technologies and techniques to accomplish traditional tasks, which often obfuscates their intent or purpose. Russia remains opportunistic, but their actions are strategically defensive. For example, in Syria and Ukraine, the Russians are gaining valuable experience in expeditionary warfare—experience they can selectively draw on to improve their capabilities in the Western strategic direction. Through some basic tools from the IPB process, we can plot their activities on a map, visualize relationships between them, and begin to identify the connections between seemingly disconnected actions and strategic objectives.

What the Russians are doing on NATO's eastern flank and elsewhere does not constitute a new form of warfare.

Rather, it is a creative application of the warfighting functions using a "whole-of-Russia" approach in competition. By simplifying what we are observing and focusing on the operational level of war, we are better able to connect seemingly discrete events and paint a more accurate picture of what Russia is attempting in EUCOM's area of responsibility. Nevertheless, Russian modernization and evolved doctrine increase the risks to NATO, specifically the Baltic countries. Russia's malign activities are effective in Eastern Europe because they are supported by a dangerous military threat.

Russia is employing an efficient, full-spectrum "whole-of-Russia" approach. The dichotomy between hybrid and conventional is a false one—Russia does not distinguish or compartmentalize warfare as the West does. This wholistic view confounds analysts who explain Russian behavior through Western constructs. Instead, when understanding Russia, and China, we should simplify their actions to one—warfare. 

Endnotes

1. Department of the Army, Training and Doctrine Command (TRADOC) Pamphlet 525-3-1, *The U.S. Army in Multi-Domain Operations 2028* (Fort Eustis, VA: TRADOC, 6 December 2018), 9.
2. Department of the Army, Army Techniques Publication 2-01.3, *Intelligence Preparation of the Battlefield* (Washington, DC: U.S. Government Publishing Office [GPO], 1 March 2019).
3. Vladimir Gerdo, "Russia to React to US-NATO Exercise Defender 2020 in Europe," TASS, 4 February 2020, <https://tass.com/politics/1116409>.
4. Office of the Joint Chiefs of Staff, *Russian Strategic Intentions, A Strategic Multilayer Assessment (SMA) White Paper* (Washington, DC, May 2019), <https://www.politico.com/f/?id=0000016b-a5a1-d241-adff-fdf908e00001>.
5. Figure adapted by authors from original Russian National Security Strategy document available on the Russian Security Council website, 31 December 2015.
6. Department of the Army, Army Doctrine Publication 3-0, *Operations* (Washington, DC: U.S. GPO, 31 July 2019), 5-2.
7. Charles K. Bartles, "Recommendations for Intelligence Staffs Concerning New Generation Warfare," *Military Intelligence Professional Bulletin* 43, no. 4 (October–December 2017): 10-17.
8. Department of the Army, TRADOC Pamphlet 525-3-1, *U.S. Army in Multi-Domain Operations*, iii.

The American way of war must evolve if we are to successfully thwart the aims of our adversaries in competition or to defeat them in conflict.⁸

—GEN Stephen J. Townsend

Statement made as Commander, U.S. Army Training and Doctrine Command, currently Commander, U.S. Africa Command



Figure 10. Black Sea/Caucasus Region

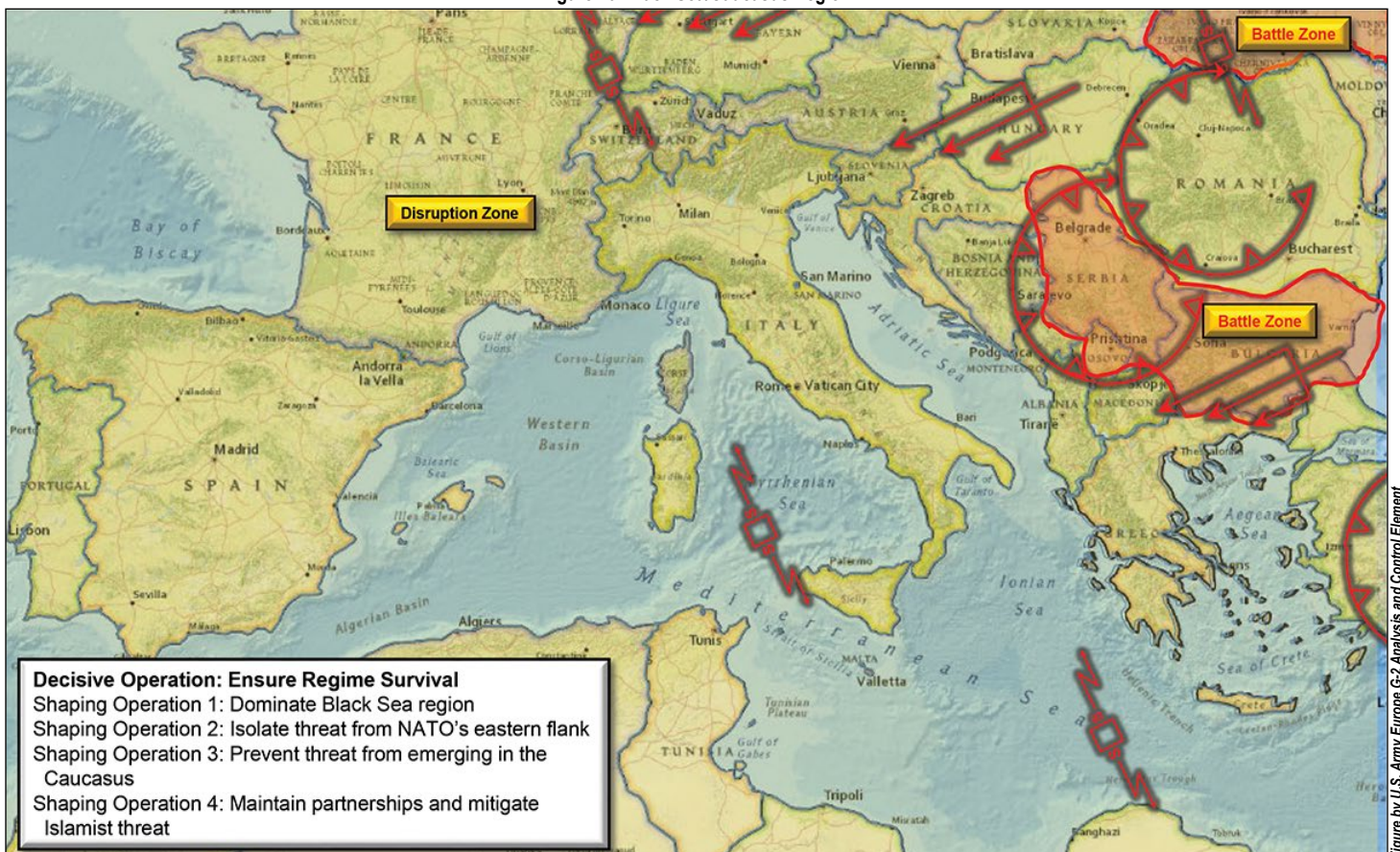


Figure 11. Balkans/NATO's Southern Flank

Mr. David Harding began his intelligence career in 1984 as a signals intelligence voice interceptor, serving in the 3rd Armored Division. His first assignment as a civilian analyst was in modeling and simulation at the Army's Intelligence and Threat Analysis Center, before it formed the General Military Intelligence component of the National Ground Intelligence Center (NGIC), where he served until 2015. Mr. Harding has expertise in a wide range of Eurasian and Middle Eastern ground forces, the full range of warfighting functions, and both conventional and irregular warfare entities, including Lebanese Hizballah and Iran's threat network. He has served variously as an analyst, team lead, liaison officer, and branch chief for the NGIC, Joint Chiefs of Staff J-2, Multi-National Force-Iraq, and Multi-National Corps-Iraq. He has also embedded with the U.S. Special Operations Command Central, U.S. Special Operations Command, U.S. Special Operations Command Europe, and a special missions unit. Mr. Harding received research fellowships from the Secretary of the Army and Office of the Director of National Intelligence, leading multi-organizational and multinational projects at the cutting edge of intelligence tradecraft. He holds a master of arts from George Mason University and an all-but-dissertation degree from the University of Virginia. He completed a 5-year tour as a Russian ground forces analyst in the U.S. Army Europe G-2/66th Military Intelligence Brigade (24th Military Intelligence Battalion analysis and control element).

COL David Pendall (retired) has extensive experience in Europe and in defense intelligence. He was a G-2, senior intelligence officer, for U.S. Army-Europe, and a commander of the 66th Military Intelligence Brigade, also based in Europe. He served as a J-2 for the North Atlantic Treaty Organization-International Security Assistance Force (ISAF) in Eastern Afghanistan and as a senior staff officer in Afghanistan's ISAF joint command and the Multi-National Corps in Iraq. He has spent more than 28 years as a career intelligence officer, serving across all levels of the U.S. Army, joint force, and defense intelligence. He has an executive certificate in national and international security from the Harvard Kennedy School of Government, has served as a fellow with the Massachusetts Institute of Technology (MIT) Security Studies Program, and was assigned to MIT Lincoln Laboratory as the senior U.S. Army liaison. He is also a member of the International Institute of Strategic Studies and the Royal Institute of International Affairs (Chatham House).

LTC Steven Curtis commands the 24th Military Intelligence (Operations) Battalion. He is an intelligence professional with deployments to Iraq and Afghanistan and service at multiple echelons, including brigade combat team S-2, Joint Staff, and congressional staff. He is a former Wilson Center fellow and holds graduate degrees in strategic intelligence and legislative affairs.

Vantage Point

Practical Solutions for Today's Intelligence Challenges



The U.S. Army Intelligence Center of Excellence is pleased to introduce Vantage Point. Vantage Point is a web-based forum designed for publishing content useful to the MI Corps in a more expedited manner than what is published in *Military Intelligence Professional Bulletin* (MIPB). Specifically, Vantage Point is primarily intended for—

- Articles focused on practical solutions to current MI challenges.
- Well-written, but less formal, short- to medium-length articles.
- Unclassified articles but can include CUI content, unlike MIPB.

If you are interested in submitting an article to Vantage Point, please contact the Vantage Point team at usarmy.huachuca.icoe.mbx.doctrine@mail.mil.

Vantage Point is available on IKN at <https://ikn.army.mil/apps/VantagePoint/>.



A Soldier from Charlie Company, 1st Battalion, 27th Infantry Regiment, 2nd Infantry Brigade Combat Team, 25th Infantry Division, conducts tactical movements after having air assaulted to an area near the objective, kicking off a week of realistic training in Hawaii, January 27, 2020. Readiness determines our ability to fight and win our Nation's wars; it is timely and relevant analytical intelligence forecasts of the threat that ensures our future success.

Forecasting the Threat within the Future Operational Environment

by Dr. Elyssa Dunfee, Mr. Ralph Edwards, and Dr. Christopher Beiter

Introduction

The U.S. Army is in a period of intense modernization and change, and it will require changes to intelligence collection, analysis, and dissemination in order to succeed in great power competition now and in the future. This article seeks to identify challenges and opportunities for Army military intelligence (MI) as it pivots to support emerging requirements in this new environment. First, we discuss issues raised by the need to fully integrate intelligence into the overarching context of the future operational environment and the Army modernization enterprise. Next, we highlight three key objectives for Army MI in adapting to these new challenges, and propose systems and processes to enable success in achieving these objectives. We describe how Army MI will emphasize a rigorous planning process to

discover and prioritize requirements, drive a dynamic collection process, and adopt a tailored analytic process. We propose that Army MI should emphasize near-real-time dissemination of analysis of current foundational data via databases supporting the current operational environment and embrace rigorous analytic methods to forecast threats in support of the future operational environment and decisions by Army senior leaders.

Intelligence to Support the Future Operational Environment

The future operational environment drives Army concepts and capabilities, dictating the modernization investments necessary to ensure that the force is adequately developed, trained, and equipped to overmatch the threat in the mid- and far-term. The Army is dependent upon the delivery

of timely, relevant, and integrated all-source intelligence that adequately forecasts the threat aspects of the future operational environment. The National Ground Intelligence Center (NGIC), in collaboration with other mission partners in the intelligence community, and especially the Defense Intelligence Enterprise, is the primary production element responsible for meeting the Army's needs in this regard.

As identified in numerous strategic documents, the United States is entering a period of enduring strategic competition that brings the potential for large-scale conflict as well as coercive activities short of war. During this time, challenges from rogue states and non-state actors will persist. Rapid technological developments will almost certainly change the character of future war, adding profound complexity and uncertainty to the future operational environment. As with the entirety of the U.S. national security apparatus, Army MI must take stock of its role in this new environment and commit to providing superior analysis of the threat in the context of this complex and fluid future operational environment. This will enable future force development and Army materiel modernization efforts.

To provide insightful analysis of the threat in this context, NGIC and intelligence community mission partners must contend with several significant issues:

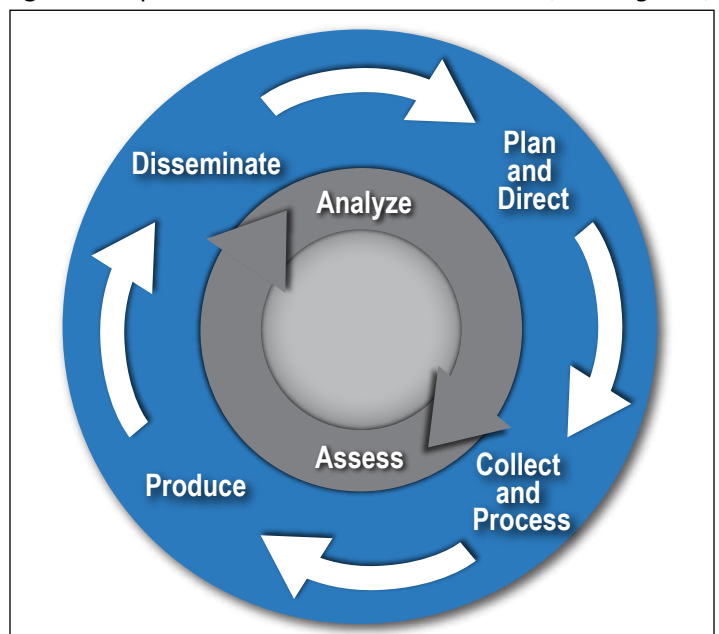
- ◆ The future operational environment affects the future threat and is itself impacted by the future threat, which means that intelligence support to the future operational environment must be agile and mindful of context.
- ◆ We must insist on conceptual clarity in our analysis. Abstract concepts must be defined consistently and used with precision. For example, confusion about what constitutes concepts such as the “competition phase” or “gray zone activities” impedes efforts to assess and clearly communicate conclusions regarding their status and effects.
- ◆ We should carefully consider the relevance of key theoretical insights gained during the most recent period of great power competition. While much has changed in the world since the Soviet era, hard-earned knowledge about issues such as deterrence and the security dilemma, for example, may help us understand the incentives and constraints that shape the future threat.
- ◆ Even with added conceptual clarity, there will always be intelligence topics relevant to the future operational environment that are emergent or defy easy categorization and, as a result, tend to be neglected or fall into seams within and between organizations. NGIC and

intelligence community partners must be vigilant and proactive in identifying these topics—such as the aforementioned “gray zone activities”—and integrating relevant expertise across organizations, if necessary, to present comprehensive analysis to customers.

- ◆ With respect to materiel capability development, detailed intelligence products on the threat are required as early as possible in the life cycle, often when capability parameters are not yet well defined. This situation demands a structured, disciplined approach to forecasting in general, and technology forecasting in particular, as it relates to adversarial applications to military capabilities. To arrive at the best possible intelligence analysis for the benefit of a capability program, managers, developers, and engineers must maintain dialogue with intelligence analysts and levy requirements germane to the program over its entire life cycle.
- ◆ If intelligence requirements are suitably maintained and validated for a program over its life cycle, and integrated analysis is generated as a result, then the concept of threat-based performance can be realized. Cost, schedule, and performance are the fundamental considerations that drive program decision making, and an effective understanding of the threat will allow the program to make appropriate adjustments and acceptable risk determinations to ensure the viability of the program through operations and sustainment.

Prioritizing Requirements

The intelligence process is the process by which intelligence requirements are satisfied. ADP 2-0, *Intelligence*,



The intelligence process¹

defines the intelligence process as composed of the continuous steps of *plan and direct*, *collect and process*, *produce*, and *disseminate*.² While all the steps are necessary for success, the *plan and direct* step offers the most return on investment in terms of maximizing efficiency in the intelligence process in order to meet expanding requirements for intelligence in a flat or decreasing resource environment. Army MI will use the Army Program of Analysis and rigorous prioritization schema to maximize efficiency in the *plan and direct* step of the intelligence process in order to drive Army and intelligence community collection, produce and integrate the most important analysis, and deliver tailored products to the intelligence consumer at the right time.

The Army Program of Analysis is both a process and a document. The document definitively represents Army all-source intelligence needs across the service. The process identifies intelligence requirements and enables prioritization and planning of collection requirements, all-source analysis, and production. Army Program of Analysis developers solicit intelligence requirements from across the Army and sort them according to a set of key intelligence questions approved by Army G-2. Analysts convert the requirements to primary intelligence questions for the purposes of prioritization and production planning. Primary intelligence questions are prioritized in order to best apply available analytic resources and to guide the Army's collection assets in pursuing the most impactful information.

In 2020, the Army Program of Analysis process focused principally on the Secretary of the Army's modernization priority. MI senior analysts selected issues addressing the pacing threat from near-peer nations and modernization efforts that were likely to affect Army Futures Command or Army cross-functional teams. This effort resulted in the down-selection of 12 top-tier priority intelligence requirements from more than 500. NGIC will produce collection support briefs and Army G-2 will produce operational directives to go after this top-tier of collection priorities. Army and intelligence community collectors, as well as the Army and joint hard target programs, will accurately focus on the Army's most important intelligence needs. Likewise, MI will derive a production plan from documented customer

intelligence requirements, which will enable purposeful integration from discrete-level questions up to the broad view required by senior decision makers, force planners, and modernization professionals.

Anticipatory Intelligence

Anticipatory intelligence that forecasts the threat out 15 or more years is critical to making long-term investment decisions, managing risk, and developing the future force. Unfortunately, this requirement frequently creates apprehension for intelligence professionals who must navigate the somewhat incongruous challenges of delivering "accurate" intelligence estimates while adequately conveying the inherent uncertainty of these estimates. Too often, this dilemma leads analysts to err in one of two ways. Those choosing to err on the side of accuracy deliver to customers a well-sourced document that more closely resembles a book report than an intelligence estimate. Those who concede to uncertainty throw their hands up and rely on their expertise to intuit a guess at the "possible" future threat. Neither approach meets the high demands of Army modernization, so how can this be resolved? We make three recommendations:

- ◆ Both analyst and customer must have a **shared definition of forecasting**.
- ◆ Analysts should embrace novel analytic methods, including data science techniques when appropriate, to **add rigor to forecasting**.
- ◆ **Analytic review chains** should view the community analytic standards as a license instead of a constraint and emphasize the distinction between unwarranted judgments and highly uncertain judgments.

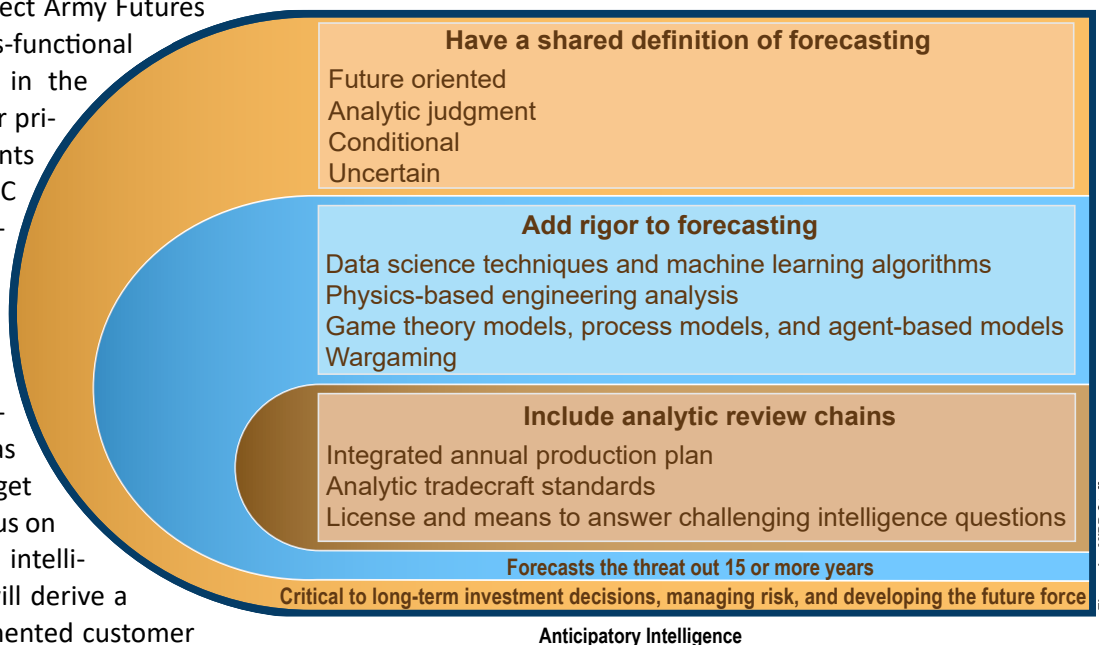


Figure by MIPB Staff

What is a Forecast? For an intelligence professional, to forecast is to provide a future-oriented judgment that is inherently conditional and uncertain. In unpacking this definition, we see four components:

- ◆ **Future orientation** conveys a need to understand a prospective state of the world, but customer and analyst must share a common understanding of the precise type of requirement. Does the customer require a point estimate of future threat capability? The distribution and likelihood of plausible future scenarios? An examination of potentially dangerous wild cards?
- ◆ **Forecasts are analytic judgments;** this means that they are inherently inferential. Waiting for collection to provide the “answer” to a forecasting question is futile and reflects a fundamental misunderstanding of the requirement. Collection is, of course, a critical part of the intelligence process, but a forecast is more than a summary of collected information. The only way to substantiate a forecast is through sound reasoning.
- ◆ **Forecasts are conditional** in that they are built on a foundation of knowledge about the past or present as well as assumptions held constant for the sake of logical argumentation. It is the analyst’s responsibility to make conditions explicit, and it is the customer’s prerogative to question them.
- ◆ **Uncertainty is unavoidable** in forecasts. By virtue of their very ambition, they grapple with the unknowable. Instead of avoiding uncertain judgments, analysts should objectively assess and directly convey uncertainty in their forecasts in order to allow customers to weigh risk appropriately.

How Can Analysts Add Rigor to Forecasts? While traditional intelligence community tradecraft offers a plethora of structured analytic techniques valuable for adding rigor to forecasting, two nontraditional approaches also lend themselves to this challenge, each under a different set of conditions.

For questions that require identifying trends, patterns, or outliers in large amounts of structured or unstructured information, data science techniques and, increasingly, machine learning algorithms, can uncover hidden insights. Notably, these techniques support inductive data exploration, hypothesis testing, probabilistic predictions, and reasoning beyond singular, or small numbers of, observations.

For questions that require making analytic judgments when information is scarce, formal methods provide critical analytic leverage. As with data science approaches, these

methods can be computationally intensive, but they contrast with data science in that they derive conclusions from assumed or established predicates instead of inducing them from large numbers of observations. Methods that fall under this broad category include physics-based engineering analysis, game theory models, process models, agent-based models, wargaming, and a variety of other simulation environments. For example, the discipline of modeling and simulation puts foundational MI data in motion. The Defense Intelligence Enterprise has made a concerted effort to develop and maintain a robust capability to afford customers the ability to conduct high-fidelity, red-on-blue, many-on-many modeling and simulation scenarios for operational planning and modernization design tradeoff studies. As the Army modernizes and develops concepts for executing multi-domain operations, modeling and simulation affords a cost-effective and efficient manner with which to explore various future operational environment conditions and related excursions.

Sound application of these methods, and other novel analytic approaches, will require a broadening of traditional analytic tradecraft training to ensure analysts, analytic review chains, and leaders understand their value and limitations and can communicate the results of their analysis clearly and accurately.

The Art of Review. Senior analysts and others in analytic review chains add value in all steps of the intelligence process, but they primarily focus on the *plan and direct* step and the *produce* and *disseminate* steps. Senior analysts affect the *plan and direct* step by helping to develop an integrated annual production plan in support of the Army Program of Analysis, in addition to supporting rigorous analytic design at the individual production requirement level. The *produce* and *disseminate* steps require senior analysts to review and evaluate intelligence production for analytic quality and to ensure analysis is timely, relevant, and delivered to customers in the right format.

To meet these challenges in an increasingly complex and fast-paced environment, senior analysts and others in review chains would benefit from a shift in perspective with respect to analytic tradecraft standards. Rather than senior analysts viewing intelligence community analytic standards through a lens of *adherence to ends*, we suggest that they adopt a view of the standards as a *license, and a means*, to answer the most challenging intelligence questions.

For example, the community standards should be properly understood as giving analysts permission to make inherently uncertain far-term threat forecasts, as opposed to precluding them. Importantly, senior analysts should

understand, and be able to communicate to customers, the distinction between a highly uncertain, but properly substantiated, judgment and an unwarranted speculation. In good news for Army modernization, analytic tradecraft standards viewed liberally provide the intelligence analyst both license and means to achieve the highly uncertain, but properly substantiated, judgment for answering intelligence questions, while avoiding unwarranted speculation.

Foundational Intelligence

In the Defense Intelligence Agency's (DIA) 2018 *Strategic Approach*, foundational MI is described as "the comprehensive understanding of foreign military capabilities, infrastructure, and materiel."³ This simple, descriptive phrase conveys that foundational MI is a fundamental element for understanding the current threat and a necessary basis for forecasting the threat component of the future operational environment.

Machine-assisted Analytic Rapid-repository System

With the plethora of foundational MI data available across the Defense Intelligence Enterprise, discoverability and accessibility by the Army and other customers is a growing concern. To address this, DIA has launched the Machine-assisted Analytic Rapid-repository System, also known as MARS. MARS incorporates five major foundational MI categories: infrastructure, order of battle, intelligence mission data, cyberspace, and space/counterspace. While MARS will certainly host foundational MI data, it is not simply a "grand foundational MI database" that will subsume all current and future foundational MI datasets. Rather, it will be an interoperable, cloud-enabled environment with dynamic linkages to foundational MI throughout the Defense Intelligence Enterprise. As of this writing, the initial capability offering for the infrastructure portion of MARS is being piloted, and the initial capability offerings for order of battle and intelligence mission data are beginning to take shape. MARS is intended to provide users with the ability to scale intelligence and information, dynamically bring together content, and continuously adapt to new missions. As envisioned, MARS will be a fundamentally important resource for the Army to address the current threat environment and will enable accurate forecasting for the future operational environment.

When describing how MARS will change the way intelligence data is processed and accessed, DIA Director LTG Robert P. Ashley Jr., stated, "MARS is our moon shot...It's those kinds of innovations that we're looking at that allow us to be able to have better situational awareness, have richer information, to be more current, to be agile and dynamic—that is not static databases and that we are constantly updating."⁴

Hybrid Intelligence. Army and Department of Defense intelligence consumers also require intelligence products that forecast future adversary capabilities within the foundational construct. Currently, three intelligence product types address this need for "hybrid intelligence" that builds on foundational MI:

- ◆ Threat modules.
- ◆ Joint correlation of forces assessment.
- ◆ Critical intelligence parameters.

Individual threat modules available in the Defense Intelligence Threat Library combine foundational data on existing systems with projected data for future systems. Likewise, the Joint Correlation of Forces Assessment database contains more than 30 years of order of battle information. Critical intelligence parameters are intended to inform the acquisition community when an adversary has breached a threshold on a particular threat-sensitive performance parameter for a U.S. capability. Including analysis of an adversary's progress along the way will greatly improve the effectiveness of the critical intelligence parameters process. Updates to all three forms of hybrid intelligence occur on a 1- or 2-year cycle.

To make efficient use of analytic resources and to set up our analytic processes for success in answering additional anticipatory questions about the future threat, we make three recommendations:

- ◆ Disseminate foundational MI in integrated databases that enable near-real-time dissemination of analysis of current foundational data to facilitate common access to current data.
- ◆ Leverage enterprise-wide solutions such as MARS (when and where) to enhance both infrastructure and operational efficiencies.
- ◆ Treat parameterized anticipatory data in the same way as current foundational MI to create automated, dynamic availability of data to the acquisition, modeling and simulation, and wargaming communities.

Conclusion

The challenge for NGIC and its intelligence community mission partners is to deliver timely, relevant, integrated intelligence to meet the Army's modernization needs while at the same time fulfilling requirements to support current operations and readiness. A wide range of extant



products can be tailored to improve all-source output in this regard, including foundational MI data, modeling and simulation, hybrid products, and anticipatory forecasts developed through the Army Program of Analysis. Ultimately, all-source assessments that sufficiently address the adversarial aspect of the future operational environment represent the critical analysis upon which the Army will generate threat-based performance as a successful outcome of multifaceted modernization efforts. We have described effective forecasting methodologies that the Army should incorporate into products that serve the Army's force development and acquisition programs. If these ideals can be realized, then the modernized force will be better prepared to prevail in future conflicts. ✨

Endnotes

1. Department of the Army, Field Manual 2-0, *Intelligence* (Washington, DC: U.S. Government Publishing Office [GPO], 6 July 2018), ix (common access card login required).
2. Department of the Army, Army Doctrine Publication 2-0, *Intelligence* (Washington, DC: U.S. GPO, 31 July 2019), 3-2.
3. Defense Intelligence Agency, *Strategic Approach* (September 2018), 11, https://www.dia.mil/Portals/27/Documents/About/DIA_Strategic_Approach.pdf.
4. Robert K. Ackerman, "DIA Aims for MARS as its Moon Shot," *SIGNAL Magazine*, August 15, 2019, <https://www.afcea.org/content/dia-aims-mars-its-moon-shot>.



Dr. Elyssa Dunfee is the senior intelligence officer for scientific and technical intelligence analysis at the National Ground Intelligence Center (NGIC). She has 10 years of experience in research, analysis, and policy related to foreign affairs in the federal government and private sector. Previously, she was a senior analyst with the Army, served in the Department of State and Department of Homeland Security as a U.S. Presidential Management Fellow, and was an associate with Booz Allen Hamilton. Dr. Dunfee holds a bachelor's degree in anthropology and a doctorate in foreign affairs from the University of Virginia with a concentration in comparative politics.

Mr. Ralph Edwards is Chief Analyst for NGIC. In 1990, he joined the Foreign Science and Technology Center, later NGIC, where he has served in many capacities. These roles include Chief of the Weapons of Mass Destruction Division, Director for Mission Integration, lead for the Interagency and Foreign Partners section of the Office of Intelligence Integration, commander's advisor for intelligence integration, and Chief of the Emerging and Disruptive Technologies Division. While at NGIC, he spent 2 years on a joint-duty assignment with the Defense Intelligence Agency (DIA). For 20 years, he also served in various capacities with the National Intelligence Committee's Weapons and Space Systems Intelligence Committee. He is an electrical engineer with a bachelor of science degree from the University of Tennessee and a master of science degree from Virginia Tech.

Dr. Chris Beiter is Chief Scientist for NGIC and serves as the senior advisor for the Army on scientific and technical intelligence. He has served in various capacities at NGIC, including senior intelligence officer for Science and Technology, Mission Management Division Chief, senior intelligence officer for Integration, senior intelligence officer for Weapons and Systems, Afghanistan Mission Manager, and Division Chief in the Weapons of Mass Destruction and Military Technologies Divisions. He also served in a joint-duty assignment at DIA. He holds a bachelor of science in mechanical engineering from the University of Notre Dame. He also holds a master of science and a doctorate in aerospace engineering from the Georgia Institute of Technology.

GREAT SKILL Program

Military Intelligence Excepted Career Program

Our Mission

The GSP identifies, selects, trains, assigns, and retains personnel conducting sensitive and complex classified operations in one of five distinct disciplines for the Army, DOD, and National Agencies.

Who are we looking for?

Those best suited for this line of work do not fit the mold of the "average Soldier." Best qualified applicants display a strong sense of individual responsibility, unquestionable character, good interpersonal skills, professional and personal maturity, and cognitive flexibility. **Applicants must undergo a rigorous selection and assessment process that includes psychological examinations, personal interviews, a CI-scope polygraph and an extensive background investigation.**

Basic Prerequisites:

- ◆ Active Duty Army.
- ◆ 25 years or older.
- ◆ Hold a TS/SCI clearance.

For a full list of prerequisites, please visit our website (SIPRNET <http://gsd.daiis.mi.army.smil.mil>) or contact an Accessions Manager at gs.recruiting@us.army.mil or call (301) 833-9561/9562/9563/9564.



Training Today's Army for Tomorrow's Threats



by Ms. Jennifer Dunn

Introduction

The U.S. Army has spent the past 4 years grappling with its role in confronting adversaries in joint multi-domain operations. In the future, the U.S. military will face a battlespace in which adversaries will contest it across all domains—it will no longer be assured freedom of action in the air, land, maritime, space, and cyberspace domains. The U.S. Army Training and Doctrine Command (TRADOC) is helping the Army prepare for this environment through the training, education, and development of both today's and tomorrow's force.

The TRADOC G-2 is the Army's proponent for developing and approving operational environments for training and opposing force (OPFOR) doctrine; its charter is the continuous analysis of peer, near-peer, and other potential threats. This analysis ensures that Army training, now and in the future, is relevant and representative of the kinds of actions our adversaries will take to challenge us in multi-domain operations. The fruits of TRADOC G-2's continuous analysis are two series of doctrinal publications. The first, the TC 7-100 series, includes training circulars designed to provide the U.S. Army training community with a challenging, realistic adversary for training events. The second, the ATP 7-100 series, includes four manuals designed to provide the Army with official unclassified assessments of real-world threats' tactics, applicable for both training environments and real-world threat analysis.

TC 7-100 Series

TC 7-100, *Hybrid Threat*

TC 7-100.2, *Opposing Force Tactics*

TC 7-100.3, *Irregular Opposing Forces*

TC 7-100.4, *Hybrid Threat Force Structure Organizational Guide*

TC 7-101, *Exercise Design*

TC 7-102, *Operational Environment and Army Learning*

TC 7-100 Series: Threat Best Practices for OPFOR Doctrine

The TC 7-100 series comprises six publications, produced to inform U.S. Army training exercises by facilitating exercise design and Army learning (TC 7-101 and TC 7-102) and by providing instructions on how the Army OPFOR should operate in a training environment in which the "enemy" is the U.S. Army (TC 7-100, TC 7-100.2, TC 7-100.3, and TC 7-100.4). These training circulars are the Army's official doctrinal support material for threat representation in training events. These manuals, in particular TC 7-100.2, *Opposing Force Tactics*, and TC 7-100.3, *Irregular Opposing Forces*, herein referred to as OPFOR doctrine, provide Army OPFOR practitioners with details on how a composite model threat actor would execute tactics and techniques if the United States were the enemy.

WHICH SOURCE SHOULD INFORM OPFOR TACTICS FOR AN EXERCISE?		
TRAINING CIRCULAR 7-100 Series		ARMY TECHNIQUES PUBLICATION 7-100 Series
The training circular series presents the Army with an assessment of how a <u>composite model threat actor</u> would execute tactics and techniques if the United States were the enemy.		The Army techniques publication series presents the Army with an assessment of how <u>specific threat actors</u> would execute tactics and techniques if the United States were the enemy.
Derived from merging practices from threats around the globe, creating a composite adversary	SOURCE WHERE THE INFORMATION COMES FROM	Derived from unclassified open-source intelligence on specific actors, replicating an explicit adversary
Use when directed to be representative of best practices of any combination of threat actors or when the use of a specific threat is not needed	UTILITY WHEN EACH SHOULD BE USED	Use when directed to add techniques and procedures from a specific threat actor and requiring the incorporation of the whole training package for effect
Composite model that represents best practices of real-world threats to create the toughest conditions	DESIGN THE DIFFERENCE BETWEEN THE MODELS	Distinct model that represents best practices of specific actors to create tailored and particular conditions
Designed to challenge task proficiency, requiring increased rigor and agility to succeed against an optimized adversary	TRAINING SELECTION INFORMED BY TRAINING TASKS	Designed to challenge adversary-focused readiness, requiring threat familiarity and precision to succeed against the actions of an identified adversary
Best suited for decisive action exercises in order to yield maximum task proficiency	IMPLEMENTATION USING THE RIGHT TOOL FOR THE JOB	Best suited for regionally focused or mission-readiness exercises in order to develop specific capabilities

OPFOR Source Comparison

OPFOR doctrine, while not directly labeled or tied to any specific threat actor, is informed by threat analysis. These books were created through an intensive review of the tactics of state and non-state actors from around the globe for the sole purpose of identifying the *best practices* of those actors’ tactics. It is important to understand this concept: The OPFOR doctrine composite model is *not* a threat model made up by intelligence specialists in the TRADOC G-2, but rather a model that is representative of the world’s best tactical practices—an exemplar of the most dangerous adversary the United States could face in a tactical fight.

The TRADOC G-2 created this composite model for two reasons:

- ◆ To capture the types of actions executed by actors around the world that represent best tactical practices.
- ◆ To provide the U.S. Army an OPFOR capable of challenging every task a U.S. Army brigade may have to conduct.

Finding one single actor in the real world that has the equipment and organization and executes tactics in a way that can adequately challenge the task proficiency of a brigade has historically not been possible. For this reason, training

the application of those tactics and techniques in a conflict with the U.S. Army.

The TRADOC G-2 is undertaking an initiative to produce threat tactics doctrine in order to deliver this information to the Army. This doctrine, the ATP 7-100 series, will provide the Army with official unclassified assessments of projected tactics from four countries. The series comprises ATP 7-100.1, *Russian Tactics*; ATP 7-100.2, *North Korean Tactics*; ATP 7-100.3, *Chinese Tactics*; and ATP 7-100.4, *Iranian Tactics*.

These four tactical assessments contain similar information:

- ◆ Introductions to the actors’ national strategies.
- ◆ Descriptions of how they perceive their place on the international (and/or regional) stage.
- ◆ Overviews of their entire military force.
- ◆ Details on their ground forces’ organizations.
- ◆ In-depth reviews of the tactical actions their ground forces are likely to employ in conflict with the United States.

events that focus on task proficiency should reference the OPFOR doctrine manuals because the composite model, as an *optimized adversary*, best yields maximum task proficiency.

**ATP 7-100 Series:
Threat Tactics
Doctrine**

While the Army needs an OPFOR doctrine that is representative of the most challenging adversary it could expect to encounter, it also needs to have unclassified assessments of how specific threat actors would execute tactics and techniques. These assessments would provide the Army with an understanding of the nuanced differences between the actor application of tactics and techniques, in particular

While some of the material is also in other U.S. Government publications, these manuals are unique in the level of detail they provide. For example, they include information that explores *how* these actors would likely approach specific types of tactical actions if confronted with U.S. Army formations enabled by joint multi-domain operations capabilities as an enemy.

Due to the actor-specific focus of these Army techniques publications, these documents are not well suited for use in decisive action training events that need to challenge task proficiency, unlike the training circular series of OPFOR doctrine. Rather, these manuals serve as source material of specific actor tactics and techniques that can be used to challenge U.S. Army adversary-focused readiness. They are best suited for mission rehearsal exercises or other training events in which the success of U.S. forces is dependent upon familiarity with a specific threat. The intent of the Army techniques publications series of threat doctrine is to provide familiarity with a specific threat's tactics and techniques, the sum of which may not challenge all U.S. tasks.

The Army techniques publication series also serves another function for the U.S. Army. As the Army's official unclassified doctrinal source of the tactics of countries like North Korea, China, Russia, and Iran, this material serves as a foundational baseline assessment for each actor. These assessments are based on the most up-to-date information available. Subject matter experts within the Department of Defense and intelligence communities have vetted them, ensuring their veracity and applicability to the greater Army training and intelligence community. Additionally, the material in the Army techniques publications serves as a starting point for the concept and capabilities development community. The Army techniques publications, in conjunction with the TRADOC G-2's battlefield development plans, have informed TRADOC's and Army Futures Command's simulations and tests that will drive changes to the Army's future force as it prepares for joint multi-domain operations.¹

What's Next?

Unlike the existing training circular series, the Army techniques publication series is in production. The first one,

ATP 7-100.2, *North Korean Tactics*, is in the final stage of review with publication anticipated in early 2021. The next Army techniques publication will be ATP 7-100.3, *Chinese Tactics*, with an expected publication by mid-2021. Release of the publications describing Russian and Iranian tactics will not occur until late 2021. In the meantime, the Combined Arms Doctrine Directorate will conduct a worldwide staffing of these two publications. Those interested in participating in their review should contact the element of their command that distributes Army doctrine staffing.

Many of the manuals in the training circular series of doctrine are nearing their 10-year anniversary. The TRADOC G-2 has been collecting material over the past several years and will continue to collect material throughout the production of the Army techniques publications with the intent to inform updates to the training circular series of manuals. Right now, an update is planned for TC 7-101, *Exercise Design*, and TC 7-102, *Operational Environment and Army Learning*. TC 7-101 will likely transition to an Army field manual as part of the update. Additionally, in fiscal year 2021, the TRADOC G-2 will undertake an update to the OPFOR doctrine to ensure the Army's OPFOR training materials still provide the most robust and most dangerous enemy the Army could encounter in a tactical fight.

For the Army to remain ahead of its adversaries, training against a robust and realistic threat for task proficiency is essential. It is also essential for the Army, especially for the regionally aligned elements, to thoroughly understand the adversary they are most likely to encounter in future conflicts. Collectively, the training circulars and Army techniques publications series of doctrine provide the Army the most up-to-date realistic unclassified threat material needed to enable success in future conflicts against any enemy. 🌟

Endnote

1. The U.S. Army Training and Doctrine Command (TRADOC) G-2 battlefield development plans are classified analytic assessments of Russian and Chinese systems warfare. They were produced to support TRADOC's concept and capabilities development in light of joint multi-domain operations.

Ms. Jennifer Dunn is a career U.S. Army Civilian intelligence specialist assigned to the U.S. Army Training and Doctrine Command (TRADOC) G-2. As a branch chief in the Operational Environment Integration Directorate, she specializes in threat and operational environment representation for Army training, education and leader development, and fielded force integration programs. Operational Environment Integration, as an organization in the analysis and control element of the TRADOC G-2, is responsible for developing TRADOC's understanding of the future operational environment and ensuring the TRADOC community of interest is prepared for today's, and tomorrow's, threats.

China's Sustained Success in Sub-Saharan Africa: Letting China Pick Up the Check



by Chief Warrant Officer 4 Charles Davis

Author's Note: Thoughts and assessments in this work are those of the author and are not meant to reflect the official position of the Warrant Officer Career College or the Army.

Introduction

China's Belt and Road Initiative, also known as One Belt, One Road, is a massive infrastructure, transportation, and energy project that could eventually stretch from East Asia to Europe and Africa. So far, approximately 60 countries either have signed on to the Belt and Road Initiative or have expressed an interest in doing so, including several African nations.¹ Although the initiative will lead to an era of trade and growth, it comes at the risk of increased Chinese political and economic influence, as well as the potential for "debt-trap diplomacy" for economically deprived countries, many of which are in sub-Saharan Africa.

As part of the Belt and Road Initiative, China opened its first overseas military base in the sub-Saharan African nation of Djibouti in 2017, and is likely planning to establish similar military facilities in other countries that share common strategic interests. In the African continent, these locations could include Kenya, Tanzania, and Angola.²

According to a 2019 executive briefing to the United States International Trade Commission, China's foreign direct investment in sub-Saharan Africa has increased significantly each year since 2010.³ Some say this is cause for concern; others argue it is an opportunity to let China pick up the check—in other words, to let China pay for infrastructure projects that also reflect the interests of the United States and its allies.

China's Overseas Military Base

Djibouti is a small East African coastline country that now represents China's portal to the continent. Djibouti is located on the western shore of the Bab el-Mandeb Strait. This strait separates the Red Sea and Indian Ocean, providing maritime links between Europe and the Middle East. Djibouti also serves as a key operational hub for United States Africa Command (AFRICOM). The U.S. base, Camp Lemonnier, is under lease until 2034 at a cost of \$1.4 billion.⁵ While China avoided labeling its facility in Djibouti a military base, calling it a logistics support base, Rush Doshi, a specialist in Chinese military and diplomacy at The Brookings

Institution, thinks that China selected the location because a number of other nations had representation there, making it "less provocative" than selecting a new site.⁶

Analysts at The Brookings Institution believe that China will "continue to forgo formal military alliances and full-fledged bases, and instead seek to develop partnerships that allow it access to its expanding interests."⁷ In a congressional hearing on China's strategic aims in Africa, Yun Sun of the Stimson Center highlighted the United States

The Silk Road

The Belt and Road Initiative is reminiscent of the ancient Silk Road and is therefore also known as the New Silk Road. The original Silk Road existed during the westward expansion of China's Han Dynasty (206 BCE to 220 CE), which built trade networks extending more than 4,000 miles to Europe. The Chinese used the networks to trade silk, spices, and other goods.

Chinese President Xi Jinping announced the expansion initiative in 2013, which comprised what he called the overland "Silk Road Economic Belt" and the "Maritime Silk Road." At first, they were collectively referred to as the One Belt, One Road initiative but eventually became the Belt and Road Initiative. Although the goal was to revive the ancient trade routes of the historic Silk Road, the project quickly grew beyond the geographic "belt-road" concept to become a massive global initiative that would also encompass many of the developing countries of Africa.⁴

"tendency to underestimate the Chinese ideological push as they are dismissed as ineffective." He went on to say, "At this stage, what is important here is the Chinese intent to export its model and experience rather than its effectiveness for Africans to receive and emulate. China is still exploring the most effective way to promote its political influence and soft power within African countries."⁸ Given that Chinese policy and diplomacy derive from a *reactive culture*, it is no

wonder the People's Liberation Army would assume an indirect and passive role as a tool of China's national power. Tying military partnerships to the Belt and Road Initiative will be less intrusive, and less worrisome, to the local population and will be more economically beneficial than simply establishing a military presence.

A "Reactive" Culture, According to the Lewis Model

As Richard Lewis describes in his book *When Cultures Collide: Leading Across Cultures*, a reactive culture is one that prioritizes courtesy and respect, listening quietly and calmly to their interlocutors and reacting carefully to the other side's proposals. It rarely initiates action or discussion, preferring to listen to and establish the other's position first, then react to it and formulate their own.⁹

Chinese Projects in Africa

Local perceptions are extremely important given that China continues to increase its foreign direct investment and has imported a workforce of almost a quarter million Chinese citizens to support these initiatives.¹⁰ The Belt and Road Initiative in Africa has provided China opportunities in 39 countries and propelled it to the top in trading on the continent. These economically deprived countries are welcoming the financial benefits of doing business with China without considering the implications of this "debt-trap diplomacy" and a growing Chinese national presence in their countries.

More than 10,000 Chinese businesses are now operating in Africa, and large settlements of Chinese entrepreneurs in places such as Nigeria and Senegal have followed them.¹¹ Beijing clings to authoritarian capitalism, in which the Chinese government owns many large firms and determines which sectors receive subsidies and market protection, because the system affords tight social and political control and allows Beijing to redirect capital toward geo-strategic aims.¹² This control of Chinese capital expansion allows the government to direct the focus and location in line with national interests.

Guinea is a prime example of Chinese capital expansion. The small west coast nation claims the largest stores of bauxite ore, having produced 55 million metric tons in 2018. Recent agreements with China secured Guinea \$3 billion in infrastructure projects while Chinese firms secured a 25-year mining right worth 1 billion tonnes of bauxite.¹³ However, protests over poor wages and work conditions plague these mining companies, which are used to a population base that is not entitled to a voice or platform in which to air their concerns.

Close bilateral ties between China and most of its African partners remain centered around China's growing demand

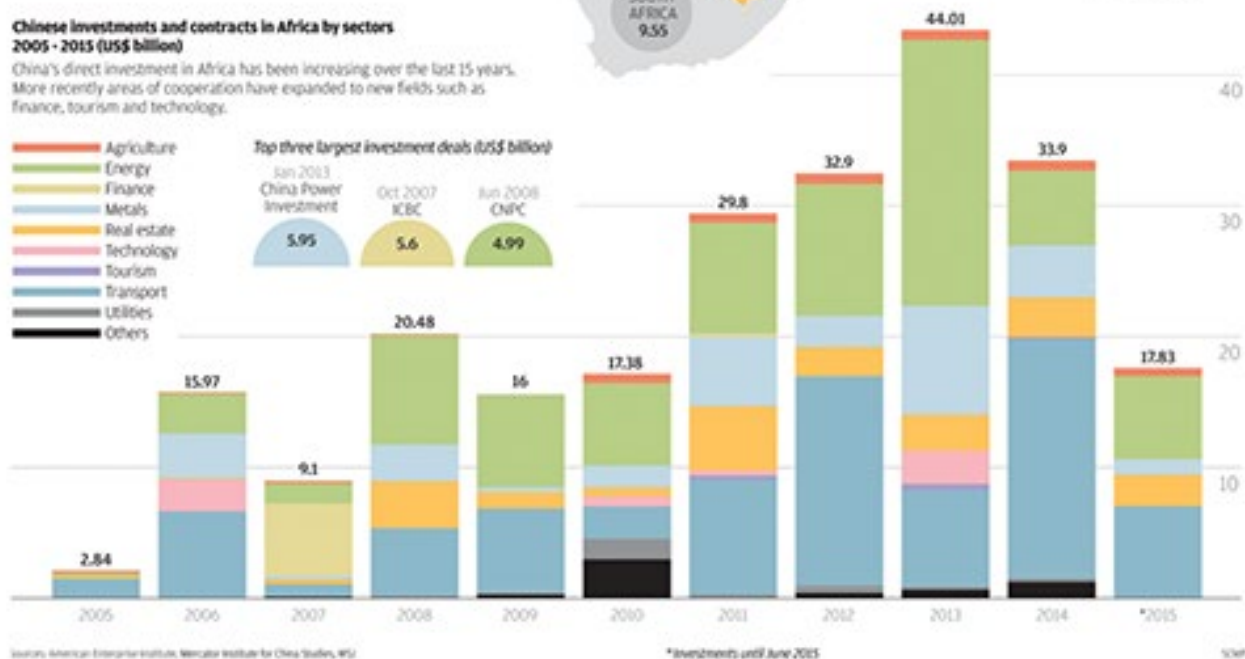
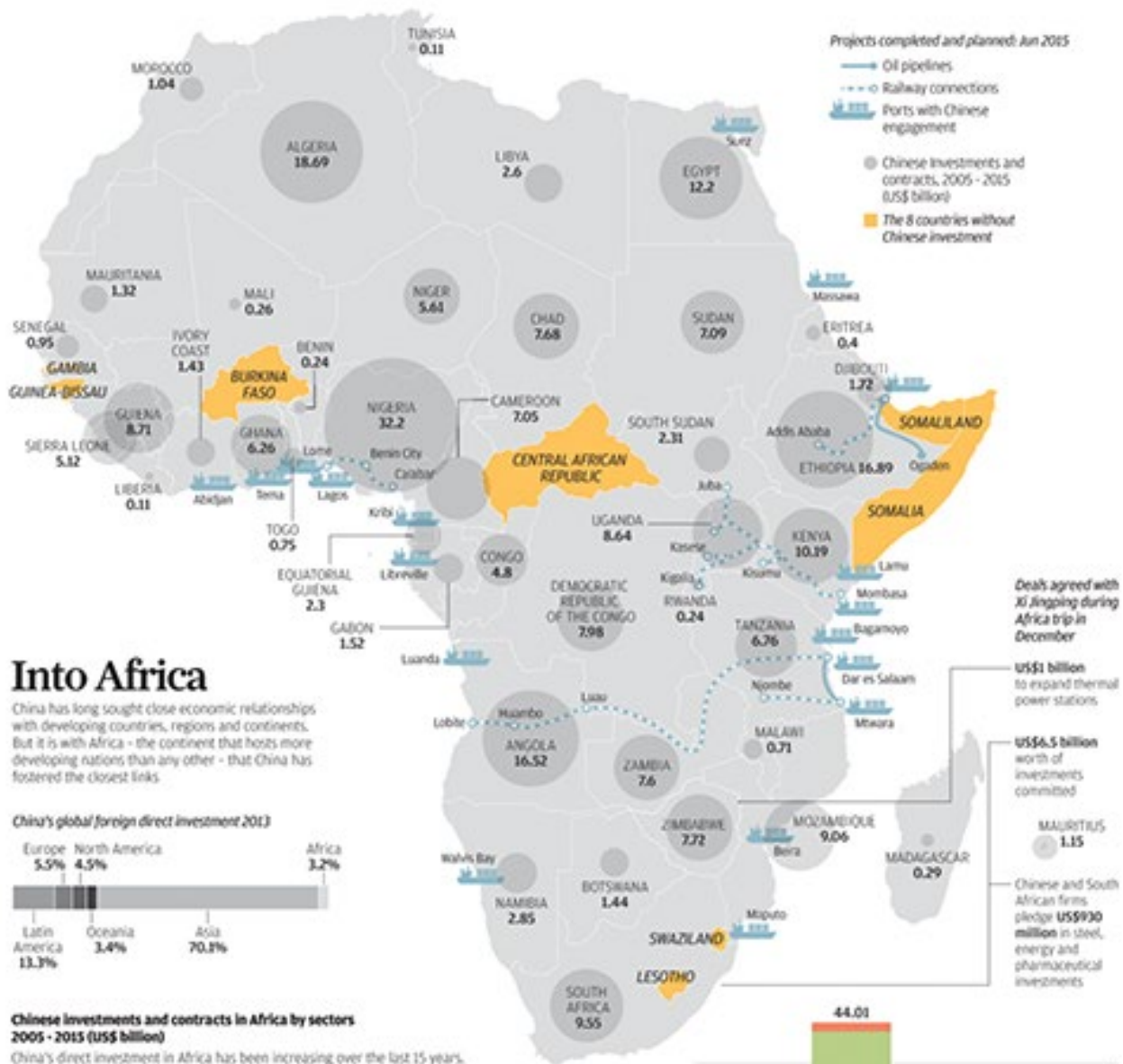
for commodities—particularly mineral resources such as oil, metals, and precious stones—and has become subject to increasing scrutiny.¹⁴ This observation is reinforced in the Department of Defense's *Annual Report to Congress*, which states the following: "In 2019, China imported approximately 10.1 million barrels per day of crude oil, which met approximately 77 percent of its needs. Also in 2019, China met 43 percent of its natural gas demand with imports, which the [International Energy Agency] IEA projects will grow to 46 percent by 2035. Most of China's oil and natural gas imports come primarily from the Persian Gulf, Africa, Russia, and Central Asia."¹⁵ Trade with South Sudan is a strong example of China's reliance on Africa for these import requirements. In 2016, South Sudanese oil exports (99 percent of recorded exports in 2016) were sent to China.¹⁶

In 2017, the top recipients of Chinese outward foreign direct investment were Ghana, Kenya, South Africa, Tanzania, Democratic Republic of Congo, and Uganda. As part of this investment, Ghana gave China 5 percent of its bauxite in exchange for \$10 billion in infrastructure projects.¹⁷ Ghana's bauxite reserves are estimated at \$460 billion, so China stands to gain \$23 billion on its investment.¹⁸ During the 2018 Forum on China-Africa Cooperation in Beijing, 50 African presidents and heads of government lauded the transforming effect China was having across the continent. "Africa is not a zero-sum game. Our growing ties with China do not come at anyone's expense. Indeed, the gains are enjoyed by everyone who does business on our continent."¹⁹ Interestingly, Judd Devermont, the director of the Africa Program at the Center for Strategic and International Studies, noted that nine African leaders attending the United Nations General Council the previous year stated they would prefer to do business with the United States, but the United States is not there the way China is.²⁰

Local Anti-Chinese Sentiment

Past industrial policies left Chinese officials with a stark choice of either boosting Chinese construction abroad or shutting down domestic coal and steel plants, which in turn would cause political and social unrest. The Belt and Road Initiative provides an opportunity for the former by allowing Chinese state-led firms to maintain high production levels amid slowing Chinese economic growth.²¹ Furthermore, the Belt and Road Initiative has presented migration opportunities for a strained population in the homeland. Not only do they provide domestic resource opportunities, but they also produce labor export initiatives.

The massive influx of funds and workers from China has led to increased anti-Chinese sentiment. Beijing has yet to find ways to defend itself against accusations that its



people exist in parallel societies in the host countries, independent of indigenous values and norms.²² One reason may be in the way contracts are awarded and money is distributed. The former Minister of Information and Broadcasting in Zambia stated, “Chinese loans often don’t even go to Zambian accounts. They choose the contractor from China, the contractor is paid in China, but it reflects in our books as a loan from China.”²³ If one considers the 10,000 private Chinese companies and businesses throughout Africa are really an extension of the People’s Republic of China, then China is making a loan to itself and having another country pay it back.

Negative sentiment is also prevalent in countries with populations that make their living on the water. The African Association of Environmental and Resource Economists indicate Ghanaian fishermen can earn only about 5 percent of the income of Chinese fishermen. Ghanaians’ own catch from the sea can meet only 41 to 42 percent of domestic needs for their country.²⁴ This may be largely due to the roughly 500 Chinese fishing vessels operating off the western coastline of Africa. These operations are reportedly catching more than 300,000 tons of fish each year. Much of the Chinese operation is conducted farther off shore than can be accomplished by the local fishing vessels, leaving locals unable to support domestic needs.



A DF4D diesel electric locomotive owned by the China Road and Bridge Corporation is parked on a bridge construction site of the Nairobi-Malaba Standard Gauge Railway Project in Kenya.

The Military Perspective

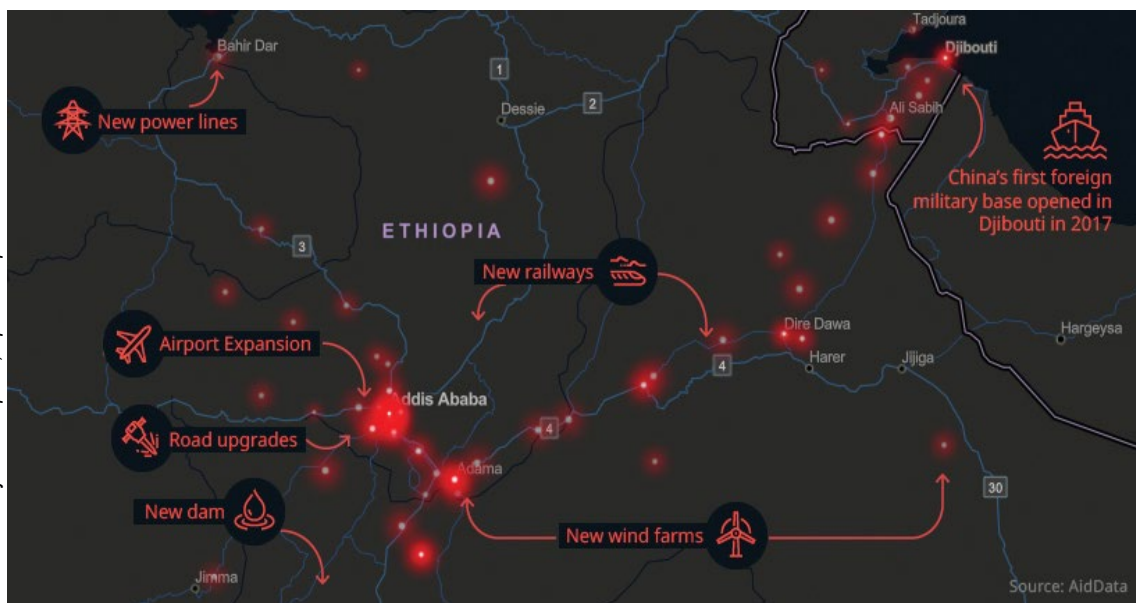
A number of U.S. analysts argue that the Belt and Road Initiative is a conduit for greater military presence and cooperation across sub-Saharan Africa. Certainly, China wants to protect its investments, and there is the issue of a surging Chinese national presence across the continent, so they would want to protect their citizens as well. This almost sounds like an action from Russia’s next generation warfare, and it is possible China is playing the long game of seeding economic relationships while developing cultural ties in or-

der to exploit that presence with a necessary security effort. However, Africa does not need to create security concerns; they already exist and are likely the reason China hosted the China-Africa Peace and Security Forum in July 2019.

Dr. Cobus van Staden, a senior researcher in China-Africa relations at the South African Institute of International Affairs in Johannesburg, South Africa, believes African leaders desire greater cooperation in training and intelligence with China. To African countries, security relations with China provide unprecedented opportunities to strengthen their capacity-building efforts as a way of ending the recurring cycles of violence and insecurity.²⁵ From 2014 to 2018, China provided military support, through equipment sales to 26 African countries. The deals included CSK-131 armored vehicles for the Central African Republic, Harbin Y-12 military transport aircraft for Mali, and Red Arrow-9A antitank missiles to Rwanda.²⁶ In the bigger picture, China’s arms deals in Africa totaled one fifth of its annual sales and made up 24 percent of sub-Saharan Africa’s total purchases. However, Deputy Director for Intelligence at AFRICOM, BG Gregory Hadfield, stated, “It is important to remember that outside of selling arms for their own economic benefit, China and Russia are not doing much to help counter extremist groups to rob Africans of their future.”²⁷ Compared to the investments China has been making in Africa, the United States is reducing its footprint in the region—or is it?

In November 2019, the U.S. Agency for International Development distributed a funding opportunity called the East Africa Private Sector Engagement for the Prosper Africa Initiative. The focus areas were trade facilitation, co-investments, enabling the environment, and leveraging existing resources. Fifteen federal agencies support Prosper Africa, and the goal is to substantially increase two-way trade and investment between the United States and Africa.²⁸ The 13th U.S.-Africa Business Summit was to take place in Morocco in June 2020 but was postponed because of the coronavirus disease 2019 (COVID-19) pandemic. Additionally, the 1st Security Force Assistance Brigade (SFAB) has been identified to relieve the 101st Airborne Division of its Africa mission.²⁹ SFABs are specialized units with the core mission to conduct training, advising, assisting, enabling, and accompanying operations with allied and partner nations.

Nevertheless, U.S. efforts may be a day late and a dollar short when it comes to making real headway. In February 2020, former Secretary of State Michael Pompeo made his first trip to sub-Saharan Africa. He landed at an airport funded by China and traveled on Ethiopian highways built by China to reach the African Union Conference Center that China paid \$200 million to construct.³⁰ It is hard not to see China’s progress, and maybe we should learn a



Ethiopia is one example of Chinese investment transforming the sub-Saharan infrastructure.

lesson already taught to us in the Middle East and Afghanistan. China and Russia let us commit a significant amount of United States wealth to stabilizing these countries, just to come in and reap the benefits. If China is investing so heavily, let it stabilize and protect its interests. As our adversaries have done repeatedly, U.S. capitalism can step into a thriving region for a change.

China's Voting Power at the United Nations

Letting China absorb the cost of growth and security would be a great idea, if not for the voting power at the United Nations that China is securing through these strong economic connections. One of the variables used to assess a country in support of the command or military decision-making process is economics. When reviewing the economic situation in a country, analysts consider import and export partnerships. Analysts understand the relative dependence countries can develop based on these trade relationships and in many cases can assess what position they will take on world issues at the United Nations. As demonstrated in the voting patterns from 1992 to 2017, there is a significant relationship between China lending to African nations and the voting patterns of those nations in the General Assembly. Since China joined the United Nations in 1971, North Korea has voted most similarly with China, and the United States has voted most dissimilarly. Djibouti, where China established a military base, is also high on the list.³¹

Are Some Loans in Jeopardy?

The financial future of some Chinese-funded projects is uncertain because of downturns resulting from the COVID-19 pandemic and heavy debt. One such example is Kenya's \$3.2 billion railway line, completed in 2017 using Chinese funds. Massive projects like this may require several financially

overburdened developing nations to renegotiate their loans, placing them in a dependent and precarious position with regard to China.³²

Conclusion

The ambitious scale of China's Belt and Road Initiative, including its activities in sub-Saharan Africa, has caused much debate. Some analysts believe China has purely geopolitical and economic motives, while others see it as an

opportunity to have China pay for infrastructure projects that also reflect the interests of the United States and its allies. However, letting China pick up the check comes with risk—increased Chinese presence and power in the sub-Saharan region and a greater influence in the United Nations General Assembly. Soft power diplomacy will likely be the most effective tool for both China and the United States when deciding the next step in Africa. 🌟

Endnotes

1. Andrew Chatzky and James McBride, "China's Massive Belt and Road Initiative," Council on Foreign Relations website, January 28, 2020, <https://www.cfr.org/backgrounders/chinas-massive-belt-and-road-initiative>.
2. Department of Defense, *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2020* (Washington, DC, 2020), x, <https://media.defense.gov/2020/Sep/01/2002488689/-1/-1/2020-DOD-CHINA-MILITARY-POWER-REPORT-FINAL.PDF>.
3. Arona Butcher, Wen Jin Yuan, and Ujjwall Uppuluri, "China's Outward Foreign Direct Investment In Sub-Saharan Africa," USITC website, April 2019, https://www.usitc.gov/publications/332/executive_briefings/2019-05_chinaof_dissa.pdf.
4. Chatzky and McBride, "Belt and Road Initiative"; David Dollar, "Understanding China's Belt and Road infrastructure projects in Africa," The Brookings Institution, September 2019, <https://www.brookings.edu/research/understanding-chinas-belt-and-road-infrastructure-projects-in-africa/>; and "Belt and Road Initiative," Belt and Road Initiative website, accessed 3 December 2020, <https://www.beltroad-initiative.com/belt-and-road/>.
5. Ali Mohammed, "US losing influence to China in key African port," *Columbus Dispatch*, 29 October 2019, <https://www.dispatch.com/opinion/20191029/column-us-losing-influence-to-china-in-key-african-port>.
6. John Grady, "U.S. Base in Djibouti Key to American Interests in Africa," U.S. Naval Institute website, April 19, 2019, <https://news.usni.org/2019/04/19/panel-u-s-base-in-djibouti-key-to-american-interests-in-africa>.

7. Leah Dreyfuss and Mara Karlin, *All That Xi Wants: China Attempts to Ace Bases Overseas* (Washington, DC: The Brookings Institution, September 2019), https://www.brookings.edu/wp-content/uploads/2019/09/FP_20190930_china_basing_karlin_dreyfuss.pdf.
8. *Hearing on China's Strategic Aims in Africa: Hearing Before the U.S.-China Economic and Security Review Commission*, 116th Cong., 2nd Sess. 26 (May 8, 2020) (statement of Yun Sun, Senior Fellow and Co-Director of East Asia Program, Stimson Center).
9. Richard D. Lewis, *When Cultures Collide: Leading Across Cultures*, 3rd ed. (Boston: Nicholas Brealey Publishing, 2006), xix, 32.
10. Caleb Slayton, "Africa: The First U.S. Casualty of the New Information Warfare Against China," *War on the Rocks*, February 3, 2020, <https://warontherocks.com/2020/02/africa-the-first-u-s-casualty-of-the-new-information-warfare-against-china/>.
11. Wenyuan Wu, "How Africa is Breaking China's neo-Colonial Shackles," *The Interpreter*, Lowy Institute, 30 October 2019, <https://www.lowyinstitute.org/the-interpreter/how-africa-breaking-china-s-neo-colonial-shackles>.
12. Sagatom Saha, "The Future of Chinese Foreign Economic Policy Will Challenge U.S. Interests, Part 1: The Belt-and-Road Initiative and the Middle Income Trap," *China Brief* 20, no. 2 (January 29, 2020), <https://jamestown.org/program/the-future-of-chinese-foreign-economic-policy-will-challenge-u-s-interests-part-1-the-belt-and-road-initiative-and-the-middle-income-trap/>.
13. Anthony Kleven, "Belt and Road: colonialism with Chinese characteristics," *The Interpreter*, Lowy Institute, 6 May 2019, <https://www.lowyinstitute.org/the-interpreter/belt-and-road-colonialism-chinese-characteristics>.
14. Carlos Casanova and Ruben Nizard, "China-Africa: Will the Marriage of Convenience Last?" *Coface Economic Publications*, November 7, 2017, <https://www.coface.com/News-Publications/Publications/China-Africa-Will-the-marriage-of-convenience-last>.
15. Department of Defense, *Annual Report to Congress*, 133.
16. Casanova and Nizard, "China-Africa."
17. Kwasi Gyamfi Asiedu, "A \$10 billion China deal to mine bauxite in Ghana is facing fierce environmental pushback," *Quartz Africa*, June 5, 2018, <https://qz.com/africa/1296808/a-10-billion-china-deal-to-mine-bauxite-in-ghana-is-facing-fierce-environmental-push-back/>.
18. Emmanuel K. Dogbevi, "Bauxite reserves can earn Ghana \$460b – Vice President," June 26, 2017, *Ghana Business News*, <https://www.ghanabusinessnews.com/2017/06/26/bauxite-reserves-can-earn-ghana-460b-vice-president/>.
19. Abdi Latif Dahir, "'Satisfied' and 'inspired': All the ways African leaders praised their alliance with China," *Quartz Africa*, 5 September 2018, <https://qz.com/africa/1379457/china-africa-summit-african-leaders-praise-relations-with-beijing/>.
20. Olivier Caslin, "Afrique-États-Unis: rencontre avec Cyril Sartor, le «Monsieur Afrique» de Trump," *Jeune Afrique*, 12 June 2018, <https://www.jeuneafrique.com/mag/564959/politique/afrique-etats-unis-rencontre-avec-cyril-sartor-le-monsieur-afrique-de-trump/>, quoted in Center for Strategic and International Studies, *Statement before the Senate Armed Services Committee Subcommittee on Emerging Threats and Capabilities, "Implications of China's Presence and Investment in Africa," A Testimony by Judd Devermont Director, Africa Program Center for Strategic and International Studies (CSIS)* (Washington, DC: December 12, 2018), 7, https://www.armed-services.senate.gov/imo/media/doc/Devermont_12-12-18.pdf.
21. Saha, "Chinese Foreign Economic Policy."
22. Wu, "Breaking China's neo-Colonial Shackles."
23. "Resistance growing to Chinese presence in Zambia," *Deutsche Welle*, accessed 2 December 2020, <https://www.dw.com/en/resistance-growing-to-chinese-presence-in-zambia/a-47275927>.
24. China House Student Fellows, "Chinese and International Public Perceptions of China's Fishing Fleets in West Africa," *China-Africa Project*, November 8, 2019, <https://chinaafricaproject.com/student-xchange/chinese-and-international-public-perceptions-of-chinas-fishing-fleets-in-west-africa/>.
25. Abdou Rahim Lema, "China in Africa's Peace and Security Landscape," *The Diplomat*, December 12, 2019, <https://thediplomat.com/2019/12/china-in-africas-peace-and-security-landscape/>.
26. Sarah Zheng, "Beijing security forum shows how Chinese military takes belt and road route to Africa," *South China Morning Post*, 13 July 2019, <https://www.scmp.com/news/china/diplomacy/article/3018414/beijing-security-forum-shows-how-chinese-military-takes-belt>.
27. Diana Stancy Correll, "How AFRICOM plans to counter Russian, Chinese influence in Africa," *Military Times*, 20 January 2020, <https://www.militarytimes.com/news/your-military/2020/01/20/how-africom-plans-to-counter-russian-chinese-influence-in-africa/>.
28. U.S. Agency for International Development, *East Africa Private Sector Engagement for the Prosper Africa Initiative Annual Program Statement (APS)*, n.d., https://www.usaid.gov/sites/default/files/documents/1860/APS_EA_Prosp_Fact_Sheet_FINAL.pdf.
29. Kyle Rempfer, "Pentagon realignment will send 1st SFAB to Africa," *Army Times*, February 12, 2020, <https://www.armytimes.com/news/your-army/2020/02/12/pentagon-realignment-will-send-1st-sfab-to-africa/>.
30. "African Union opens Chinese-funded HQ in Ethiopia," *BBC News*, 28 January 2012, <https://www.bbc.com/news/world-africa-16770932>.
31. Yiqin Fu, "Data Analysis: Who Votes with China, and Who Votes with the US and Europe at the UN?" *GitHub Pages* (blog), June 10, 2018, <https://yiqinfu.github.io/posts/united-nations-general-assembly/>.
32. Duncan Miriri, "Kenya should renegotiate Chinese rail loan, parliamentary panel says," *Reuters*, September 24, 2020, <https://www.reuters.com/article/kenya-railway-china/kenya-should-renegotiate-chinese-rail-loan-parliamentary-panel-says-idUSL5N2GL377>.

CW4 Charles Davis serves on the faculty of the Warrant Officer Career College. He currently instructs International Strategic Studies at all levels of warrant officer education. CW4 Davis is a graduate of the U.S. Army War College Strategic Broadening Program and holds a master's degree with honors in intelligence studies from American Military University. CW4 Davis is also a recipient of the Military Intelligence Corp Knowlton Award.

Freely Associated States

by Mr. Geoffrey Goudge, Major Christopher Neal, and Major Mark Swiney

Introduction

U.S. relations with the freely associated states (FAS) in Oceania are mutually beneficial agreements that the United States must continue to maintain. The FAS relationship provides the United States with free and open sea-lanes, broader access to the Pacific region, and strategic power projection in this critical region. Realizing this, China is attempting to dismantle United States partnerships through economic means to engage with and coerce its Pacific neighbors. United States allies in the region recognize the

growing influence of China in the Pacific and have expanded their involvement with the FAS to counter growing Chinese influence.¹ The United States must employ shrewd diplomatic and economic engagement efforts to ensure the ability to maintain its relationship with the FAS. The success of these efforts could have far-reaching military implications. The engagements will help the United States to assure its partners and allies of its commitment to the region while building a broad coalition to stem the rising tide of Chinese influence in the area.²



Map of the Freely Associated States³

National Security Strategy/National Defense Strategy

The 2017 National Security Strategy portrays a struggle taking place throughout the Pacific region between free and authoritarian views of the world. It also represents the need for freedom of the seas and relationships with partner nations that support forward U.S. military presence capable of deterring and defeating adversaries in the Pacific region.⁴ In the near term, China seeks hegemony within its area and displacement of the United States as the preeminent global power in the long term.⁵ Relationships with U.S. partners in the region are central to this contest. The uniquely positioned FAS support U.S. interests through longstanding, mutually beneficial agreements. The United States must maintain these critical relationships to ensure free and open seas as well as influence, access, and strategic power projection in the Pacific region.⁶

Who Are the Freely Associated States

The FAS have three member nations—the Federated States of Micronesia, the Republic of the Marshall Islands, and the Republic of Palau—and share a unique relationship with the United States through agreements known as Compacts of Free Association (COFAs). Each deal is a mutually beneficial partnership between the United States and each FAS member that provides stability, security, and exclusive military access in exchange for developmental support and funding. The economic aspects of these Compacts are set to expire in the 2023/2024 timeframe.⁷

China's Regional Influence

China has rapidly increased its diplomatic and economic investment to expand its influence in the Pacific region; as a result, it is increasingly becoming a more dominant power in the region.⁸ Through greater diplomatic and economic engagement, China employs predatory lending practices to exert influence on vulnerable Pacific nations.⁹ Recently, China directed its efforts toward weakening United States ties with the island nations of Oceania. Countries of Oceania provide access to the area through their positioning in critical sea lines of communication. These islands maintain vital strategic access and reach in this region for the United States as well as for China. In effect, both countries view this as a zero-sum contest for influence, access, and strategic reach.¹⁰ While they view the Pacific region as an open ground for competition, neither nation must see the relationship purely as a zero-sum game in which a participant's gain or loss of utility is correctly balanced by the losses or benefits of the utility of the other participants. The two countries have strongly intertwined economic ties. Each country must consider that any economic successes, fail-

ures, and interruptions will have positive and negative effects for both economies as the United States works to counteract the increasing impact of Chinese influence in the Pacific.¹¹

Approach

Using the problem/solution approach, this article will provide an analysis of the current situation in the Pacific region with regard to growing Chinese influence and maintaining United States influence and presence. This article will present a case for maintaining and extending the current COFAs with the FAS and several recommendations that will reassure our partners and allies that the United States remains committed to this vital region.¹² Understanding China's use of diplomatic and economic instruments of power throughout the world is foundational to understand Chinese intentions in the Pacific region. Analysis of the Chinese engagement with the FAS and attempts to make diplomatic and economic inroads align with China's intent to further its influence and strategic power projection throughout the world and the Pacific region. In effect, the Chinese seek to create a vital buffer zone of authority that is counter to the existing state of United States regional dominance. China's current diplomatic and economic practices to coopt vulnerable Pacific Islands and reduce United States influence have increased in recent years.¹³ Analysis of the past, current, and potential future successes of the mutually beneficial agreements with the United States is pivotal in developing a long-term strategy for the future. The United States can employ several actions to strengthen its position in the Pacific region by maintaining and extending the FAS program to deepen United States ties in the area and to counter Chinese attempts to expand their influence and hegemony in the Pacific region.



U.S. Secretary of State Michael R. Pompeo holds a joint press availability with Micronesia President David Panuelo, Marshall Islands President Hilda Heine, and Palau Vice President Raynold B. Oilouch, in Kolonia, Federated States of Micronesia, on August 5, 2019.

State Department Photo by Ron Przystucha

U.S. Partnership with Freely Associated States

The United States provides FAS access to many U.S. domestic programs. This includes—

- ◆ Hazard mitigation under the Federal Emergency Management Agency.
- ◆ Representation to the International Frequency Registration Board of the International Telecommunication Union.
- ◆ Disaster response and recovery.
- ◆ Some U.S. Department of Education programs, including the Pell Grant.
- ◆ Services provided by the National Weather Service, U.S. Postal Service, Federal Aviation Administration, and Federal Communications Commission.¹⁴

Additionally, COFAs allow citizens of FAS to live and work in the United States, and U.S. citizens and their spouses to live and work in the FAS.¹⁵ The aligned agreement permits military operations within the COFAs and grants land to operate bases while denying encroachment of other foreign militaries in the region without U.S. permission. In turn, the United States becomes responsible for protecting its affiliate countries and for administering all international defense treaties and affairs, though it may not declare war on their behalf.¹⁶ Further, the U.S. military maintains the responsibility and authority for defense and security matters relating to the FAS. Citizens of the FAS may serve in the U.S. armed forces, and there are high levels of military enlistment by FAS citizens. FAS citizens also retain the right to enter, study, and work in the United States without a visa for an unlimited period.¹⁷

The FAS Compacts renewed in 2003 for a 20-year term. The Compacts include \$3.5 billion in funding and provide the island governments with funding for immigrant expenses and infrastructure repairs, among other financial assistance. The Compacts also offer necessary financial support in fiscal years 2004 through 2023 via the Department of the Interior. The Compacts require the Federated States of Micronesia and the Republic of the Marshall Islands to target funding in six sectors of development: education, health, environment, public-sector capacity building, private-sector development, and infrastructure. Education, health, and projects directly affecting health and safety are priorities.¹⁸ Palau is the exception. Palau's association with the United States requires an official evaluation of terms on the 15th, 30th, and 40th years of the Compact's effective date. The first review occurred in 2010, which resulted in the signing of the Palau Compact Review Agreement. The agreement included additional economic assistance through 2024, which is the next

anticipated Compact review. The Compacts are unique to U.S. support strategies and are not intended for full FAS financial support, but rather they are a way for the islands to improve their essential government services and infrastructure. The economic aid allows the nations to reform fiscal policies and evaluate their business processes.

The Compacts with the FAS guarantees the United States exclusive military access to these countries and their surrounding waterways. The agreements also permit access to the Kwajalein military facility. Along with the potential for future basing options, the FAS Compact allows a long-term military interest within the area. The Compact is a strategic influence because of the multiple islands within the region that cover a large area and parallel vital sea-lanes. The FAS are located between Hawaii and Guam. Their location is critical because of the defense relationship within the Pacific region, creating an arc from South Korea through Thailand and on to Australia.¹⁹ The FAS also create a prepositional location for forward operations to the Pacific, if needed, for future U.S. operations.

Expanding Chinese Influence

The FAS are at an international crossroads that span all the instruments of power and demand a whole-of-government approach from the United States to assure continued presence and influence in the region. The United States must engage in diplomacy to counter the expansionist and destabilizing efforts of China. Information will shape not only the strategic but also the operational environment. Military presence and engagement will increase influence and assure allies in the region, and will further complicate the decision space of China. Economic strategies will continue to build and expand upon the bonds the United States has cultivated to varying degrees of success since the end of World War I. The analysis herein highlights the current situation as being below the level of armed conflict and focusing on the diplomatic and economic instruments of power as the most prudent to counter Chinese aggression.

China's Belt and Road Initiative has taken on the status of a national strategy, focusing the economic power of the nation's state-backed financial institutions and industries toward Forward Direct Investment and "in the geo-strategically vital region of the Freely Associated States...China is increasingly competing with the United States for influence."²⁰ The FAS face a precarious set of decisions that will have long-term effects not only for their development and sovereignty but also for the stability of the region and beyond. The FAS form a strategic center of gravity for the region, and it is surmised that "Beijing seeks to incorporate the FAS into its signature Belt and Road Initiative (BRI) by

boosting investment and economic assistance.”²¹ By forcing inroads into the financial markets of the FAS, China is creating a strategic pressure point that has shifted the focus to the Indo-Pacific area of responsibility. To that end, “during 2012–2017, the total value of overseas mergers and acquisitions (M&A) cases undertaken by Chinese firms rose from U.S. \$43.4 billion to U.S. \$119.62 billion.”²² As the renewal date for the COFAs nears, the FAS are at a crossroads and must decide whether to remain aligned with the United States and Western ideals or to shift to a pro-China footing that will restructure the region. The COFAs agreed upon by the United States and the FAS collectively have been beneficial; however, they also open a choke point for Chinese intervention.

States that offset the power base of China and are beneficial to United States policy and interests.

- ◆ **Motivations of Chinese Aid.** Chinese aid was “motivated from the start by ideology and it’s still influencing its decision today.”²⁴ If the United States focuses on free and open trade markets, which is not the case with China, a war of ideals that moves the FAS further away from a pro-United States footing is profoundly concerning.
- ◆ **Lack of Oversight.** There is no oversight of the actions of the Chinese Communist Party, which gives the Chinese uncontested freedom to bribe political and business leaders in the region with no downside to their efforts.



Plan of the Silk Road with its maritime branch on display at Shenzhen City Planning Exhibition Hall in January 2017. The Silk Road and its maritime branch are one part of the Belt and Road Initiative.

The issue currently facing the region is that the Federated States of Micronesia is the only associated state that “recognises China over Taiwan, participates in BRI, and was accorded a state visit to Beijing. This visit had a lasting positive effect on [the Federated States of Micronesia’s] FSM’s perception of China.”²³ This use of soft power on a long-term U.S. partner is a subtle yet bold gambit aimed at dividing the partner nations and limiting freedom of action for the United States. In his 2019 *Pacific Inquiry* article, Wai Yi Ma highlights several points that require counter moves from the United States in terms of Chinese activities:

- ◆ **Recognition of the One China Policy.** Taiwan is a stable democracy in the region with strong ties to the United

- ◆ **Controversy around Chinese Aid.** “Chinese aid is controversial because the traditional aid providers claimed that Chinese aid is undermining their painstaking work on reform supported by good governance and accountability.”²⁵ The United States, for better or worse, has some semblance of moral authority and a history of supporting stable democratic governments. However, if the perception of Chinese aid is that it is free flowing with no strings attached to moral obligations, corruption may become more prevalent and affect the relations of the area of responsibility.

- ◆ **Chinese Aid Is Difficult to Track.** “China is not a member of the Organization for Economic Cooperation and Development...as an aid provider; therefore, it is difficult to track Chinese aid.”²⁶

China’s revisionist actions may undermine free-market institutions that came about as a result of post-war efforts. The leap forward into an association with the FAS would serve to address the Chinese fears of encirclement and lack of reach in the region diplomatically, economically, and militarily. If China were able to construct bases and develop a forward presence for aircraft and naval assets, it would present the United States with the inverse of what United States containment is attempting to produce. The Organization for Economic Cooperation and Development is doing more

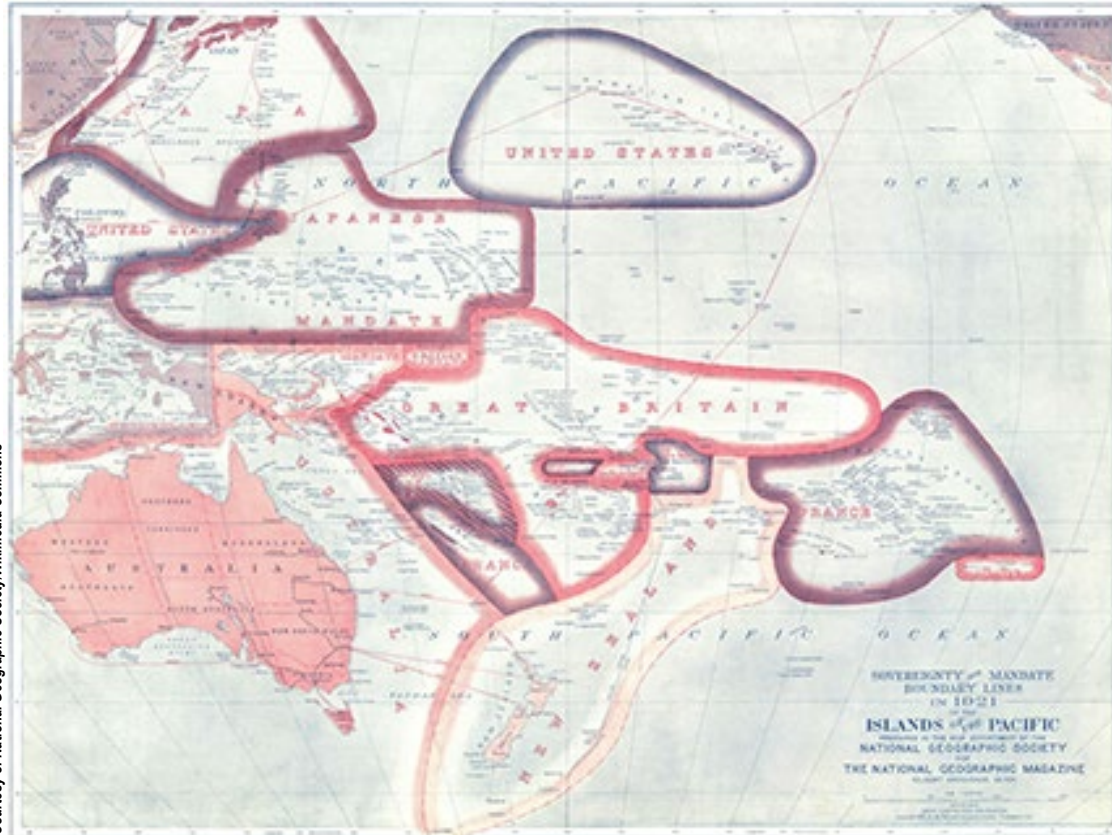
than addressing fishing rights and providing seemingly endless streams of aid packages. This is brinkmanship that will shape the political and economic landscape or will allow the reshaping of the region to a contentious hot spot that, when added to the complexities the United States faces around the globe, will only stretch even further the capabilities and capacity of the United States.

United Nations and the Trust Territory, which placed the responsibility for the defense of the FAS nations with the United States. With the desired end state always being self-governance, the United States embarked on a lackluster course that drew extensive criticism and required numerous course corrections over the years. Ultimately, COFAs outlined and strengthened the bonds of all parties concerned.

However, those articles will soon expire. If they are not renewed, the United States will lose a strategic asset to a global power competitor that has its eyes set on regional and global expansion to the detriment of United States, its ideals, and economic interests.

Recommendations

The United States should support/renew the FAS Compacts in 2023 (2024 for Palau) and continue funding and support to counter Chinese attempts to seize influence from the United States.²⁸ The United States must also recommit to its alliances



Sovereignty and mandate boundary lines of the islands of the Pacific as outlined in the Japanese Mandate and depicted on a 1921 National Geographic map of the area.

History often repeats itself through similar variations on themes played out on the world stage. The history of FAS is a perfect example of this construct. President Woodrow Wilson and the often ineffective League of Nations noted the strategic importance of the FAS and saw to provide some governance to the region. The South Seas Mandate placed the FAS nations under the control of Japan at the end of World War I. “The many islands and atolls provided airfields and deepwater lagoon anchorages that contributed to sea and air control, making them valuable for both power projection eastward, to Midway and Hawaii, and southward to Indonesia and Australia.”²⁷ U.S. forces employed island-hopping tactics during the World War II Pacific campaign to counter fortifications like those developed on the FAS islands. The attempts to contain the expansionist goals of Japan were akin to the current situation with China, with the level of armed conflict being the only difference. The end of World War II brought about the formation of the

in the Pacific through both diplomatic and economic engagement. The status of these commitments could have lasting military implications.²⁹ Continuing U.S. support to the FAS now and in the future is critical to U.S. interests, influence, strategic power projection, and geographic positioning in the region. The FAS nations are also peaceful, stable democracies. Extending the COFA agreements beyond their expiration will send a powerful signal of reassurance to U.S. allies and partners in the Pacific. Additionally, the COFAs should be used as a template to further United States negotiations in the region and to ensure that other island nations remain within the United States sphere of influence and do not succumb to Chinese control.

While China’s spending in the FAS increased, the United States currently outspends China in the FAS by a ratio of 10 to 1. Allies and partners—Australia, Japan, and Taiwan—are collectively contributing substantial sums of economic aid by a ratio of 3 to 1. China may increase spending to fill

the gap and gain influence if the COFAs expire or a reduction of United States assistance is implemented.³⁰ Economic aid can serve as both carrot and stick to motivate partners to support U.S. interests in the region. Simply put, “money talks” and equals influence. In other words, the United States must work to continue its economic assistance and diplomatic engagement with the FAS as part of a broader strategy to maintain its position with the FAS and the Pacific region.

*The United States must also leverage relationships with allies to ensure Compacts remain in place long term.*³¹ The United States must develop a broad coalition to enlist the aid of its established allies and partners in the region.³² There are many opportunities to work together on shared security concerns. The 2017 National Security Strategy depicts the intent of the United States to work with allies in the region to ensure better insulation from fluctuations and disasters for fragile island nations.³³ China seeks to undermine United States influence and alliances wherever possible in the Pacific. It is critical to reestablish U.S. commitment to the system of alliances the United States developed in the post-World War II and Cold War eras.³⁴ Allies such as Australia, New Zealand, Japan, and Taiwan realize the importance and role of the FAS in maintaining the balance of power in the region to keep free and open seas and to reduce growing Chinese influence. However, each country engages with the region differently and in line with its interests. Many United States allies are wary of Chinese efforts to establish military bases in Oceania and seek more profound engagement efforts to help buffer against continuing Chinese expansion.

Australia is highly active and focused on the broader Oceania region, and historically has been the largest donor to the area. Australia is primarily concerned with the effects of instability spilling over to its borders but has limited involvement with the FAS. The United States and Australia are also working to establish a new joint naval base on Papua New Guinea’s Manus Island as an attempt to counterbalance China’s growing influence in the region. New Zealand’s interests are similar to Australia’s and they have called for greater United States engagement in the Pacific region. New Zealand’s stated interests are to “improve the prosperity, stability, and resiliency of the region and its people.” Taiwan’s interests are to further education in the region and continue engagement with the island nations that still diplomatically recognize Taipei over Beijing. Oceania is home to 6 of Taiwan’s 17 remaining political allies. China has actively worked to get more countries to drop their recognition of the legitimacy of Taiwan in the international space, and these efforts are another reliable driver of its economic involvement in the region. Taiwan has attempted to compete against the much larger resources of China by offering more inclusive packages that benefit the broader region. Japan maintains close ties with the island nations of Oceania despite its colonial history in the region. It also advocates for the rule of law and climate protections. Japan is a significant donor to the FAS and recognizes China’s growing influence. Nations of Oceania perceive Japan as a positive, steady-ing influence with a strategy of mutual respect. While each country has differing motivations for its relations with nations of Oceania and the FAS, the United States needs to recognize these varied interests and work with its allies in a concerted effort that will ensure continued long-term cooperation with the FAS.³⁵

The United States can diplomatically engage with China and the Pacific region to shape the future of the region. The United States must increase diplomatic engagement with the broader region, including China, on a host of issues. Despite current friction between the United States and China, significant economic ties exist between the two powers. A stable, prosperous Pacific region is in the best interests of both countries. The United States must commit diplomatic resources and continually engage with China. While it may not yield profound breakthroughs, it will help to mitigate inevitable friction and disagreements between the two nations. Where possible, the two powers should work together to solve



U.S. Army National Guard photo by SGT Michael Tietjen

Soldiers from Charlie Company, 1st Battalion, 69th Infantry Regiment, New York Army National Guard, acting as an opposing force defend their positions during the final battle of Exercise Talisman Saber at the Shoalwater Bay Training Area, Queensland, Australia, on July 19, 2017.

regional problems. Opportunities abound to address non-traditional security challenges like humanitarian crises, natural disasters, human trafficking, and narcotics. Efforts such as these will help to paint U.S. commitment in the region as earnest, long-term sustainability, and not just posturing to improve military access and positioning in the region.³⁶

Many United States regional partners are hesitant to choose a side because of their economic ties with China and its growing power in the region and the need to remain engaged with their much larger neighbor.³⁷ Given this geographic reality, the United States should continue diplomatic engagement in the region with larger countries, such as India, and with regional nations' organizations like the Association of Southeast Asian Nations or the Pacific Islands Forum.³⁸ The United States increased its relationship with India, becoming its largest arms supplier to counterbalance China's ascendant regional power. Involvement with groups of nations is essential in building coalitions with disputes against China.³⁹ The United States should also consider re-entering the Trans-Pacific Partnership. Enhancing relations through these organizations and agreements gives the United States a seat at the table to shape the rules of the game for economic influence in the region. Continuing engagement and working to strengthen countervailing coalitions and financial organizations would push back against Chinese mercantilist practices and allow these coalitions to come to fair, widely beneficial agreements for all players in the region. Without United States backing, many of these smaller nations lack enough economic power to avoid bullying by China in favor of their interests.⁴⁰

Conclusion

The United States requires a mutually beneficial relationship with the FAS to maintain strategic reach, open sea lines of communication, and the ability to project power. Chinese investment within the Pacific region will continue to be a vital concern because of China's encroaching influence on the FAS and United States partnerships. The United States must continue diplomatic, economic, and military strategies to prevent China from shaping the territory and to empower the FAS against the expanding Chinese influence in the region. Achieving a secure United States and FAS alliance is accomplished by invigorating FAS Compacts, engaging diplomatically with China and the Pacific region, and leveraging relationships with allies to ensure a strategic advantage within the Pacific region. ✨



Endnotes

1. Derek Grossman, Michael S. Chase, Gerard Finin, Wallace Gregson, Jeffrey W. Hornung, Logan Ma, Jordan R. Reimer, and Alice Shih, *America's Pacific Island Allies: The Freely Associated States and Chinese Influence* (Santa Monica: RAND Corporation, 2019), ix-xi.
2. Ely Ratner, "Rebalancing to Asia with an Insecure China," *Washington Quarterly* 36, no. 2 (May 2013): 21-22, <https://doi.org/10.1080/0163660X.2013.791080>.
3. Grossman et al., *America's Pacific Island Allies*, 2.
4. The White House, *National Security Strategy of the United States of America* (December 2017), 45-47, <https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf>.
5. Office of the Secretary of Defense, *Summary of the 2018 National Defense Strategy of The United States of America*, n.d., 2, <https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf>.
6. Grossman et al., *America's Pacific Island Allies*, x-xi.
7. Ibid.
8. Ibid., iii.
9. Office of the Secretary of Defense, *National Defense Strategy*, 1.
10. Grossman et al., *America's Pacific Island Allies*, iii.
11. Stephen W. Hartman and Peter Whooley, "Are China and the United States in a Competitive Zero-Sum Economic Game?" *International Trade Journal* 30, no. 5 (July 2016): 435-439, <https://doi.org/10.1080/08853908.2016.1203380>.
12. John T. Ackerman, Matthew C. Stafford, and Thomas Williams, updated by Kathleen A. Mahoney-Norris, *Six Research Frameworks* (Maxwell AFB, AL: Air Command and Staff College, 2010), 6-7.
13. Grossman et al., *America's Pacific Island Allies*, 61-63.
14. 99th Cong., Pub. L. No. 99-658, 100 Stat. 3673, *Compact of Free Association between the United States and the Government of Palau*, Title 1 (1986).
15. Ibid., Section 141.
16. Carolyn Bennett Patterson, "In the Far Pacific: At the Birth of Nations," *National Geographic* 170, no. 4 (October 1986): 498.
17. Grossman et al., *America's Pacific Island Allies*, x-xi.
18. *United States' Interests in the Freely Associated States: Statement before the Senate Comm. on Energy and Natural Resources to Examine the United States' Interests in the Freely Associated States* (July 23, 2019) (statement of Douglas Domenech, Assistant Secretary, Insular and International Affairs, Department of the Interior), U.S. Department of the Interior website, last modified 23 July 2019, <https://www.doi.gov/ocl/freely-associated-states>.
19. *U.S. and the Freely Associated States: Testimony before the House of Resources Comm. and the House International Relations Comm., Subcomm. on Asia and the Pacific* (October 1, 1998) (statement of Stanley O. Roth, Assistant Secretary for East Asian and Pacific Affairs, U.S. Department of State), Mount Holyoke College website, <https://www.mtholyoke.edu/acad/intrel/roth2.htm>.
20. Derek Grossman and Michael S. Chase, "Maintaining the U.S. Edge in the Freely Associated States," East Asia Forum, 2 September 2019,

<https://www.eastasiaforum.org/2019/09/02/maintaining-the-us-edge-in-the-freely-associated-states/>.

21. Ibid.

22. Ping Lin, Boqiang Lin, Mengting Lin, and Chen Lin, "Empirical Study of Factors Influencing Performance of Chinese Enterprises in Overseas Mergers and Acquisitions in Context of Belt and Road Initiative—A Perspective Based on Political Connections," *Emerging Markets Finance & Trade* 56, no. 7 (2020): 1564-1580.

23. Grossman and Chase, "Maintaining the U.S. Edge."

24. Wai Yi Ma, "Bilateral Aid to a Small Island Developing State: The Case of the Federated States of Micronesia," *Pacific Inquiry* 10, no. 1 (Fall 2019).

25. Ibid.

26. Ibid.

27. Grossman et al., *America's Pacific Island Allies*, 12.

28. Ibid., xvii.

29. Andrew Rhodes, "The Second Island Cloud: A Deeper and Broader Concept for American Presence in the Pacific Islands," *Joint Force Quarterly* 95 (4th Quarter 2019): 52.

30. Grossman et al., *America's Pacific Island Allies*, 60.

31. Ibid., xvii.

32. Michael Mandelbaum, "The New Containment: Handling Russia, China, and Iran," *Foreign Affairs* 98, no. 2 (March/April 2019): 127.

33. The White House. *National Security Strategy*, 47.

34. Mira Rapp-Hooper, "Saving America's Alliances: The United States Still Needs the System That Put It on Top," *Foreign Affairs* 99, no. 2 (March/April 2020): 136.

35. Clair Apodaca, "Foreign Aid as Foreign Policy Tool," *Oxford Research Encyclopedias*, 26 April 2017, <https://doi.org/10.1093/acrefore/9780190228637.013.332>.

36. Ratner, "Rebalancing to Asia," 30-33.

37. Ibid., 33-34.

38. "Pacific Islands regional organisations," Australian Government: Department of Foreign Affairs and Trade website, accessed 12 November 2020, <https://www.dfat.gov.au/international-relations/regional-architecture/pacific-islands/pacific-islands-regional-organisation>.

39. Iulia Monica Oehler-Şincai, "United States' 'Pivot' Towards Asia-Pacific: Rationale, Goals and Implications for the Relationship with China," *Knowledge Horizons-Economics* 8, no. 1 (2016): 28-30.

40. Christopher F. Corr, "It's Time For The US To Re-Engage With The TPP," *Law360* (26 March 2018): 1-3, <https://www.whitecase.com/publications/article/its-time-us-re-engage-tpp>.

Mr. Geoffrey Goudge, Department of the Air Force Civilian, serves as a logistics planner at U.S. Strategic Command, Omaha, NE. He entered the civil service through the PALACE Acquire program. Mr. Goudge holds a bachelor of science in geography from Northwest Missouri State University, a master of business administration from the University of Oklahoma, and a master of military operational art and science from Air Command and Staff College. Before his current assignment, Mr. Goudge served as a readiness analyst at U.S. Strategic Command.

Maj. Christopher Neal, U.S. Air Force, serves as the nuclear command and control strike advisor trainer at U.S. Strategic Command, Omaha, NE. He was commissioned through the Reserve Officer Training Corps at Oklahoma State University. Maj. Neal holds a bachelor of science in marketing from Oklahoma State University and a master of science in administration from Central Michigan University. Before his current assignment, Maj. Neal served as Assistant Director of Operations, 320th Missile Squadron, F. E. Warren Air Force Base Cheyenne, WY.

MAJ Mark Swiney serves as the Joint Task Force-North J-3 Air, Fort Bliss, TX. His previous duty assignment was as the 111th Military Intelligence Brigade Deputy Commanding Officer at Fort Huachuca, AZ. He served as an aviation warrant officer before commissioning through Officer Candidate School. MAJ Swiney holds a bachelor of science in business administration and a master of aeronautics from Embry-Riddle University. His primary position is as an all-source intelligence aviator and signals intelligence officer.

Fort Huachuca Museum



Check out the Fort Huachuca Museum website at:
<https://history.army.mil/museums/TRADOC/fortHuachuca/index.html>



Fighting the Division Intelligence Enterprise in Large-Scale Ground Combat Operations

by Lieutenant Colonel James Leidenberg



Introduction

In the face of emerging global threats, peer and near-peer adversaries are pushing the bounds of competition and threatening our allies and partners with increasing capabilities. U.S. Army divisions are designed to be the lethal warfighting force able to execute Army and joint force operations to win decisively against these threats. In counter-insurgency operations, brigade combat teams (BCTs) were the front line of defense and bore the weight of planning and executing operations, fires, and maneuver. The self-reliance and independence of BCTs became the hallmark of decentralized mission command to overwhelm militant and insurgent threats. Today's challenges require divisions and corps to have a more central role in responding to threats. This article will discuss how to train and prepare the division intelligence enterprise to meet the challenges that the Army faces as it shifts its warfighting focus from the BCT to the division's readiness.

Role of Division Intelligence

Division intelligence teams gain and maintain contact with the enemy to focus the lethal and nonlethal targeting efforts that enable BCTs to close with and destroy the enemy. Lethality in large-scale ground combat operations requires precision and speed. At the point of the spear is the division intelligence enterprise to gain and maintain contact with the enemy. The primary role of intelligence leaders is to direct the intelligence process providing lethality-driven intelligence to win decisively. *Lethality-driven intelligence* is the timely, accurate, precise, and predictive intelligence that enables maneuver commanders to position forces and capabilities at the right location, at the right time, and in the right posture to close with and destroy the enemy. Lethality is measured in terms of the *potential* for something (a formation or a system) to effectively deliver and cause the desired lethal effects. It is assessed by two relative conditions:

- ◆ *Preparedness (readiness)* to deliver lethal effects.
- ◆ *Posture in terms of proximity (ability to make contact)* as expressed over time and distance from the object receiving the lethal effect.

All steps of the intelligence process must operate optimally with integrated and resilient architecture to provide lethality-driven intelligence. Intelligence leaders drive the speed, focus, and precision of the intelligence enterprise by executing intelligence support to the warfighter to meet the commander's needs so that they understand the enemy and terrain across time, space, and distance. Division intelligence leaders must master—

- ◆ Doctrine and the fundamentals of warfighting (understand and apply knowledge of all warfighting functions and lead the intelligence preparation of the battlefield [IPB] process).
- ◆ Targeting requirements and process for the lethal precision needed to win through the decide-detect-deliver-assess methodology.
- ◆ Collection management with an understanding of mission management and requirements management.
- ◆ The intelligence architecture.

Training Focus Areas for the Division

As technology and knowledge have become more prolific and accessible in even the world's most remote corners, our competitive advantages are challenged across all domains. The strategic environment is in a state of continuous competition. To prevail in providing the understanding needed to win decisively, we must retrain the intelligence enterprise to dominate when contested. Our technology is only as strong as our processes and systems that generate the understanding. We must be able to adapt to fight for understanding even when technology is no longer able to power our assessments. 1st Cavalry Division's approach relies on three training areas to ensure the division intelligence enterprise is ready. A robust and resilient intelligence architecture must underpin these areas to ensure continuous communication at echelon:

- ◆ Training Focus Area 1: Deploy ready to connect to the enterprise.
- ◆ Training Focus Area 2: Master the planning basics.
- ◆ Training Focus Area 3: Synchronize information collection operations.

Focus Area 1: Deploy ready to connect to the enterprise

- ◆ Train accountability and equipment tracking
- ◆ Build relationships
- ◆ Train realistically

Focus Area 2: Master the planning basics

- ◆ Military decision-making process
- ◆ Intelligence preparation of the battlefield
- ◆ Predictive analysis through an event template
- ◆ Common intelligence picture across echelon
- ◆ Targeting methodology

Focus Area 3: Synchronize information collection operations

- ◆ Concept of intelligence support
- ◆ Intelligence architecture

Training Focus Area 1: Deploy Ready to Connect to the Enterprise

The division must be ready to connect to the national to tactical intelligence enterprise. Readiness for a division begins with the ability to leverage the full intelligence community ahead of conflict. In large-scale ground combat operations, Army intelligence units at every echelon must arrive connected to the enterprise to enable maneuver and fires to rapidly deploy to fight and win decisively. The First Team gained direct experience of the challenges awaiting their arrival in a new theater while executing a real-world deployment exercise to Europe as part of DEFENDER-Europe 20. For rapid deployments, divisions must coordinate with the U.S. Army Intelligence and Security Command's military intelligence brigade-theater ahead of movement to prepare architecture connections in sanctuary, thereby enabling a rapid connection upon their arrival in the theater. Division intelligence teams must be "ready now." This requires a warm start of intelligence systems and architecture to provide enough time to react to uncertain conditions. Intelligence teams can quickly provide initial assessments to commanders to make informed and sound decisions. Intelligence systems and processes must be integrated with higher, lateral, and subordinate units and connected to the entire intelligence enterprise. Intelligence Soldiers must be well trained and certified at every echelon to the high levels of proficiency required for executing mission-essential tasks. This proficiency must be trained and validated across echelons at every opportunity. The unique requirements of the intelligence warfighting function require an enterprise

approach. Interconnectivity, dependencies, and standardization are key to effectively and efficiently delivering our core product—timely, accurate, precise, and predictive lethality-driven intelligence to enable fires and maneuver.

Three general lessons emerged from deploying the entire division's intelligence team. These lessons apply to future readiness in large-scale ground combat operations:

Train Accountability and Equipment Tracking at Every Opportunity. In preparation for movement to the field or even when doing inventories, leverage opportunities to train accounting for and deploying intelligence systems as single end items. When they arrive at the training location, track the time required to establish the system. This rigor enables intelligence leaders to know their systems at the division and below level and to measure the effectiveness and readiness to establish the system in tactical conditions. This also enables an evaluation of preconfiguration and preparedness for systems to rapidly support operations. Validate details such as the container and loadout timeline and the pack-out plan. Also, prepare the strategic lift support paperwork as an opportunity to ensure current measurements are available for short-notice strategic movements. Each request for equipment movement will come with a litany of additional requirements.

Build Relationships in the Training Environment. Train by connecting into the theater and corps intelligence teams during field training exercises and command post exercises to build the processes and relationships needed for an intelligence picture that is nested with higher. Likewise, when the division trains, it builds processes to support subordinate brigade intelligence development in events such as the Military Intelligence Training Strategy certification. When notified for deployment, division intelligence teams will leverage these connections to the national, theater, and tactical intelligence enterprise to support force projection and expeditionary capacity as detailed in FM 3-0, *Operations*.¹ The intelligence enterprise is powered through relationships. In deploying, theater and national intelligence teams can answer the commander's critical intelligence requirements during the force projection process. Once established in the theater, the deploying unit's (the division or its subordinate units) organic intelligence assets are distributed across the area of operations to answer the intelligence needs. In sum, preparedness to connect at every echelon to the larger intelligence enterprise is foundational for intelligence readiness. Well-established relationships are important to achieve this preparedness.

Train Realistically to Achieve Synchronization. Time matters in a contested environment. In training, it is important

to ensure that all movement is tactical and synchronized so that systems are able to connect quickly to the enterprise. Align movement timelines for arrival and setup to synchronize the arrival of key personnel with equipment. Leaders must know when, how, and how much bandwidth should be requested for intelligence operations. Intelligence leaders must maintain awareness of the timeline for mission requirements, like risk reduction exercises, to ensure the arrival and availability of the required equipment and Soldiers to maintain and set up that equipment. Understand the timeline for agricultural cleaning, strategic lift requirements for classified and mission-critical systems, and line haul requirements for low-density equipment so that those moving do not damage or break it in transit to its final destination. Load plans and accountability of all subcomponents associated with each system are vital not only to the single end item shipment but also to mission accomplishment. A single cord missing in a contested environment can have significant operational impacts. Sustained deployment readiness training ahead of exercises and mobilization is critical to the successful mobilization and employment of intelligence equipment.

terrain through common understanding. The products and production are not as important as the analytics behind the products. Cyclical analytical evaluations, iterative feedback for key processes (information collection and targeting), and assessments of the overall effectiveness of fighting products are the primary driver for future requirements in the next iteration of the intelligence process. Learning is continuous and makes the division increasingly lethal through contact.

Military Decision-Making Process. At the division level, the G-2 must support the intelligence planner in the G-5 with continuous updates for the planner's intelligence running estimate. The planner leverages a comprehensive running estimate with key products, references, and a playbook of enemy actions to provide realistic estimates of future enemy actions beyond the scope of the event template. Honing lethality requires deliberate planning. Synchronization is achieved through the military decision-making process (MDMP). MDMP is an "iterative planning methodology to understand the situation and mission, develop a course of action, and produce an operation plan or order."² The intelligence plans officer must have a thorough understanding of all the warfighting functions to integrate intelligence during planning.

Intelligence Preparation of the Battlefield. FM 2-0, *Intelligence*, describes "a number of challenges in order to successfully conduct large-scale combat operations. Foremost among those challenges are peer threats, who are highly adaptive, technologically advanced, and operate at a tempo and depth that greatly complicates Army forces' ability to respond to threat actions throughout the range of military operations."³ The command and staff rely on intelligence products and tools to support their analysis and decision making. FM 2-0 outlines products

from IPB needed throughout the MDMP steps that are tailored to support commander's requirements and the operation. ATP 2-01.3, *Intelligence Preparation of the Battlefield*, provides detailed information on the preparation of these products.

Against near-peer threats, gaining an understanding to synchronize and position forces properly requires multi-echelon intelligence analysis and support. Information gained provides an understanding of potential enemy

Photo by SSG Kelsey Miller, 1st Cavalry Division Sustainment Brigade



Troopers from the 1st Cavalry Division conducted a simulated tactical command post exercise during Warfighter 21-01 in order to ensure the integration and readiness of the division staff, as well as test the command post systems and processes for operations in October 2020.

Training Area 2: Master the Planning Basics

The division intelligence teams must master the planning and targeting requirements to bring lethality. Lethality-driven intelligence products and processes focus on enabling the commander to synchronize desired effects at every echelon at a time and place of our choosing in order to dominate our enemies and win decisively. Production of all "fighting products" is nested at every echelon to focus the entire division on the critical aspects of the enemy and

locations and conditions necessary to create a convergence of effects across multiple domains at these locations during important windows of time. In certain situations, stimulation of the enemy through operations maximizes the commander's decision space by providing a greater understanding at echelon at critical times of the friendly commander's choosing.

Deep maneuver enables the shaping and success of future operations; however, it also introduces increased risk to the force and risk to the mission. Based on how the division fights, the focus of stimulation and collection is the deep fight. Deep operations assume high levels of risk when employing simultaneous air or ground maneuver forces. Therefore, a dedicated and deliberate process must be established for air planning and reconnaissance. These distinct efforts require dedicated teams to develop and synchronize the enabling resources required for a division-level operation. Two missions in large-scale ground combat operations that are leveraged to gain intelligence, or to stimulate the enemy to gain intelligence, are deliberate attacks out of contact and reconnaissance in force.

Intelligence Support to Aviation Out of Contact Planning.

The division artillery and air cavalry brigade (ACB) can contribute immeasurably early in the division fight to gain intelligence needed for follow-on operations. As a maneuver and targeting force, the ACB is an integral part of the division's daily scheme of maneuver while shaping for or supporting the main effort during each phase of the operation. The ACB is also critical to the scheme of intelligence support and scheme of fires because the ACB provides a significant amount of the division's intelligence and fires, respectively. In the deep area, the ACB conducts deliberate attacks or nightly air assaults in a high-threat environment based on intelligence gained through the integration of intelligence from across the entire enterprise.

The ACB S-2 and division artillery S-2 teams are fully incorporated into the larger division intelligence enterprise through the analysis and control element (ACE) for parallel planning and analysis rather than separate planning efforts. For air mission planning, integration enables effects, joint suppression of enemy air defense, sequence, timing, and a shared understanding of the division commander's intent for the plan. Intelligence support and analysis priorities are coordinated between the division G-2 and ACB and division artillery S-2s. The ACB S-2 refines the air and air defense assessments, and the division artillery S-2 conducts an artillerization of the fires aspects of IPB for the entire division. The ACB S-2 must be connected with the ACB's aviation mission survivability officer (AMSO) and maintain the enemy integrated air defense (IAD) situation template with input from the ACE. Linkage with the AMSO is critical in order to maximize the special training, knowledge of friendly aviation tactics, and unique systems the AMSO uses to overcome enemy IAD capabilities. The IAD situation template must be updated continuously and reassessed to meet the need for time-sensitive out-of-contact attack to degrade antiaccess and area denial. The rapid suppression of the enemy air defense plan mitigates risk to friendly aviation assets. Because of the fast pace of operations in large-scale ground combat and limited time to exploit opportunities, the intelligence teams at each echelon must be engaged in their core competencies and nested with higher and subordinate organizations.

Support to Reconnaissance (Division Cavalry) in Force and Movement to Contact Planning.

The IPB effort establishes a baseline understanding of the terrain and enemy early in the planning process. When the commander determines ahead of or during planning that the scheme of fires or maneuver requires a ground-based division cavalry squadron, the division staff develops a task organization to meet the

commander's intent. If the intent is for an aggressive reconnaissance, planners will allocate a variety of enablers to help the division cavalry perform its role based on the given mission (reconnaissance in force, movement to contact, etc.).

Intelligence assets allocated to the division cavalry provide redundant collection beyond the coordinated fire line and short of the fire support coordination line. These intelligence assets support and integrate with the allocated direct support artillery, direct support attack aviation (with manned and unmanned teaming capability), engineer mobility, and air defense artillery. Given the intent of adversaries to deny



Photo provided by 1st Air Cavalry Brigade

The strength of the pack! Air Cavalry Troopers train and deploy to conduct expeditionary aviation operations in support of unified land operations, combined arms maneuver, and wide area security to ensure the success of the 1st Cavalry Division.

situational understanding, the fight for intelligence requires a task organization of enablers suitable for aggressive reconnaissance. Interdependent capabilities are allocated to the division cavalry to enable it to conduct forceful, aggressive reconnaissance with limited support from the division until a seam or gap is identified that the division and corps can exploit. The division artillery S-2 supports early artilleryization of the enemy counterreconnaissance and fires enterprise alongside the division cavalry S-2. The ACE provides intelligence updates to the templated versus confirmed enemy situation template. The event template of radars and artillery positions affecting the division cavalry are included in discussions of division cavalry operations. This provides reactive counterfire and employs information operations and cyberspace electromagnetic activities to mitigate risk from the enemy’s holistic indirect fire network for increased survivability.

Leveraging the Event Template to Refine Predictive Analysis. Do not get drawn into the “current fight” at the expense of gaining an understanding of the next one by establishing processes to deliberately review and update IPB and running estimates. To accomplish this, work to create shared knowledge among the functional elements within the intelligence team. Predictive analysis is gained by getting input and feedback from everyone in the intelligence process—the collection management team, targeting team, single-source intelligence discipline leads, and current operations, plans, and fusion. These teams provide input back into the IPB process to integrate intelligence gained into forward-thinking predictive analysis and collaborative outputs used to update the event template. The updated event template leads to further assessments, refined requirements, and gaps, all of which will require additional collection. Ultimately, enabling predictive analysis depends upon an accurate information collection plan and the effectiveness of the event template and event matrix.

The Common Intelligence Picture. Every echelon provides updates to the common intelligence picture. They should not be created independently. A common architecture underpinned with common systems and processes enables First Team intelligence to maxi-

mize lethality by taking full advantage of all the intellectual and analytic capacity of the division with minimal duplication of effort. This is challenging with multinational partners but not impossible. The division relies on corps to provide brigade-level fidelity of the enemy and terrain. Likewise, the division refines that assessment into battalion-level fidelity. Brigades refine the assessment into company-level fidelity. Battalions refine the assessment for platoons. These refinements are provided to both subordinates and higher headquarters. Higher headquarters reviews the subordinate unit refinements, assesses any divergences, and integrates its refinements into the intelligence estimate. The refinements should be maintained and distributed on the Distributed Common Ground System (DCGS) architecture and published in the Command Post Computing Environment. The primary, alternate, contingency, and emergency (PACE) plan enables resilient mechanisms to have daily points of contact to send updates of the intelligence estimate. Regardless of the mode and medium of reporting, reports are sent using tactical transmission protocols (proper radio etiquette) based on the line format published in Annex B for the operation.

A special cross-staff, cross-domain assessment in IPB is the electronic preparation of the battlefield conducted by the ACE, signals intelligence, cyberspace electromagnetic activities, and G-6 teams. The division and subordinate headquarters conduct electronic preparation of the battlefield to integrate an understanding of electromagnetic activity in the electromagnetic spectrum. The staff conducts electromagnetic spectrum emissions assessments from all war-fighting functions across multiple domains. The electronic preparation of the battlefield depicts emissions for friendly, neutral, and enemy in the operational environment into

Receive guidance on—	• Commander’s intent • High-payoff targets • Attack criteria • Rules of engagement	• Lead time between decision points and target areas of interest • Combat assessment requirements
Develop—	• Modified combined obstacle overlay • Situation and event templates	• High-value targets • Information collection plan
Explain—	Threat courses of action, as part of war gaming, based on friendly courses of action: • Refine the event template • Assist in developing the high-payoff target list, target selection standard matrix, and attack guidance matrix	
Produce—	Collection management tools	
Collect—	Information for target nomination, validation, and combat assessment	
Disseminate—	• High-payoff target-related information and intelligence to the fires cell or appropriate location immediately • Pertinent information and battle damage assessment in accordance with standard operating procedures or other instructions	

Intelligence Support to Targeting⁴

a single electromagnetic spectrum common operational picture. The output of the electronic preparation of the battlefield is a predictive assessment of expected enemy electromagnetic spectrum presence based on the IPB event template. This emissions event template enables the cross-staff integration of efforts in the electromagnetic pulse in numerous processes and activities such as information collection and targeting within headquarters and with higher, subordinate, supporting, and supported units.

Intelligence Support to Targeting. Intelligence support to targeting is the culmination of the entire intelligence cycle. Time (of response to information) is the unit of measure to assess the lethality of intelligence. In large-scale ground combat operations, seconds matter. Winning decisively is to destroy the enemy before the enemy has the option to do the same. All things being equal, the time it takes to generate intelligence strongly correlates to the lethality generated. This statement is true at each echelon. It is imperative to fight aggressively for intelligence.

Training Focus Area 3: Synchronize Information Collection Operations

The third training focus area is how the intelligence teams operationalize the information collection processes as an integrated function for planning, targeting, and operations. Information collection planning to make contact with the enemy or key terrain at the right time and place involves the integration of all assets of supported units, coordination between external and internal elements, and synchronization with operations and targeting. Fully nesting information collection takes significant practice and training. Intelligence leaders must execute a focused application of collection requirements management to support operations and targeting in dynamic conditions. Division intelligence efforts support the targeting of critical points to leverage deep maneuver planned in the division's overall scheme of maneuver. The division's information collection maximizes collection opportunities to collect and target exposed enemy positions.

Concept of Intelligence Support. During training and exercises, the division command nodes and subordinate units must train, certify, and validate their role in executing the concept of intelligence support to integrate and synchronize efforts with the scheme of fires and maneuver. The overall concept of intelligence support involves maximizing the use of multiple command post nodes and subordinate headquarters to develop and assess specific intelligence areas of

focus based on planning horizons and assets. The intent is to maximize an in-depth look in areas with specialty, as well as capitalizing on existing requirements. Responsibilities for each group are as follows:

- ◆ The division ACE is responsible for the overall intelligence picture, integration with corps and lateral divisions, and primary analytical input for all single-source intelligence.
- ◆ The division tactical command post is responsible for conducting intelligence analysis within the close fight, ensuring targeting and collection is aligned with operations in the next 72 hours, and maintaining a battlefield visualization for the deputy commanding general for maneuver.
- ◆ The support area command post intelligence fusion cell is responsible for conducting threat assessments within the rear area, integrating with the maneuver enhancement brigade intelligence cell, and maintaining a battlefield visualization for the deputy commanding general for support.
- ◆ The division artillery headquarters is responsible for determining and visualizing the enemy artillery picture. This includes the enemy's most lethal artillery assets or groupings, counterfire analysis, cross-boundary enemy fires, and potential locations of brigade artillery groups, divisional artillery groups, and integrated fires command assets.
- ◆ The ACB headquarters is responsible for assessing the composite surface to air threat, to include identifying enemy air mobility corridors and enemy air threats, and providing battle damage assessment for friendly air attack missions.



Over several days 1st Armored Brigade Combat Team, 1st Cavalry Division leaders, through the military decision-making process, planned and rehearsed for Combined Resolve, a live-fire exercise as part of their Atlantic Resolve rotation across Europe, which is to improve the interoperability between U.S. forces and their North Atlantic Treaty Organization allies and partners.

U.S. Army National Guard photo by SFC Robert Jordan, 382nd Public Affairs Det.

These shared roles and assessments, visualizations, and products are synchronized during the twice-daily G-2/S-2 synchronization meetings.

Intelligence Architecture Underpinning Information Collection. Division command posts require agile, resilient, and redundant architecture to increase survivability and mobility. Intelligence leaders must know how to employ adaptive physical hardware, virtual software and data management, and conceptual processes' design techniques to build capacity and agility at each echelon to be more mobile, survivable, and redundant. This complex array of connections is the core of the intelligence enterprise and requires deliberate training and design to know how to leverage national to tactical intelligence capabilities that can support tactical operations down to the battalion level. To establish an effective intelligence architecture, it is important to understand some key aspects and limitations of all intelligence architectures.

All intelligence leaders have a role in increasing their professional knowledge of the DCGS-Army (DCGS-A) family of systems and integrated capabilities. Leaders must understand the interoperability of the Mission Command System and DCGS-A systems and maintain the relevant training and toolsets to transition between transport layers to properly employ PACE from the upper-tactical internet to the lower-tactical internet. They must also capture knowledge of the dissemination of data through services in standard operating procedures for the leader's respective element. While not part of the intelligence architecture, it is important for intelligence leaders to understand the way units communicate using the different transport layers to understand how to design that architecture. Key transport layers include the Warfighter Information Network-Tactical/Army Data Network, Modular Communications Node-Advanced Enclave, Trojan Network, and Installation as a Docking Station. The division intelligence architecture is integrated with the national to tactical intelligence dissemination architecture to ensure global connectivity using available broad-

cast and network services to deliver intelligence supporting targeting, threat warning, and situational awareness.

Closing Thoughts

How we fight the intelligence enterprise relies on trained and validated processes to maintain intelligence operations and processes across the entire division. Unlike the last 20 years of warfighting, large-scale ground combat operations require greater multi-echelon systems and processes synchronized across time and space. Achieving the delivery of timely, accurate, predictive, and precise intelligence occurs only through the synchronization of intelligence operations at each echelon with the reconnaissance, maneuver, and fires planning efforts.

We cannot train on the fight we want; rather, we must prepare for the fight we do not want. The enemies of this Nation will not fight fair or hold back capabilities just because we do not have the training and resources in our formations to counter. In fact, we must drill with absolute rigor in training to get leaders to explore novel ways to counter emerging enemy capabilities—current and projected. The past offers clues to the complexity of future conflict against peer and near-peer threats, but we cannot rely on the past to give comfort that we are ready to refight these battles. The nature of conflict is changing. In the fight against these threats, intelligence leaders must navigate challenges facing the intelligence enterprise from national to tactical in ways not required since the Cold War. 🌟

Endnotes

1. Department of the Army, Field Manual (FM) 3-0, *Operations* (Washington, DC: U.S. Government Publishing Office [GPO], 6 October 2017). Change 1 was issued on 6 December 2017.
2. Department of the Army, Army Doctrine Publication 5-0, *The Operations Process* (Washington, DC: U.S. GPO, 31 July 2019), 2-17.
3. Department of the Army, FM 2-0, *Intelligence* (Washington, DC: U.S. GPO, 6 July 2018), 1-20 (common access card login required).
4. Ibid., 2-11.

LTC James Leidenberg is the division G-2 for 1st Cavalry Division at Fort Hood, TX. He previously served as the 504th Expeditionary-Military Intelligence Brigade S-3; 163rd Military Intelligence Battalion executive officer; 532nd Military Intelligence Battalion S-2; 1st Brigade Combat Team, 101st Airborne Division S-2; military intelligence company commander; and 1st Squadron, 32nd Cavalry Regiment S-2. His previous assignments include joint staff, Army staff, two deployments to Afghanistan, two deployments to Iraq, and 2 years assigned to Korea. LTC Leidenberg is a 2004 graduate of the U.S. Military Academy and received a master's degree in policy management from Georgetown University in 2011.





M2A2 Bradley Infantry Fighting Vehicle crews assigned to 3rd Battalion, 67th Armored Regiment, 2nd Armored Brigade Combat Team, 3rd Infantry Division, conduct a river crossing with Polish Army Soldiers assigned to the 2nd and 5th Polish Engineer Brigade Battalion during exercise DEFENDER-Europe 20/Allied Spirit at Drawsko Pomorskie Training Area, Poland, June 10, 2020.

Setting the Theater: Intelligence and Interoperability in DEFENDER-Europe 20

by Major Chad Lorenz

Introduction

Key lessons captured during DEFENDER-Europe 20 can significantly enhance the U.S. Army's efforts to train, build capability, and ensure readiness across the European theater. Phase I of the exercise culminated on 19 June 2020 at the Drawsko Pomorskie Training Area in Poland. The bilateral exercise included United States and Polish Soldiers operating under the control of the 1st Cavalry Division (Forward) and featured both airborne operations and a United States-Polish division-size river crossing. Designed as a deployment and tactical exercise to build strategic readiness in support of the U.S. National Defense Strategy and North Atlantic Treaty Organization (NATO) deterrence objectives, DEFENDER-Europe 20 was downscaled because of the coronavirus

disease 2019 (COVID-19) pandemic, yet the modified exercise design afforded participants the opportunity to test several important interoperability initiatives. Lessons in three areas stand out as especially significant from an intelligence interoperability perspective:

- ◆ Friendly collection and information operations.
- ◆ Transition to the Mission Partner Environment (MPE) information sharing capability.
- ◆ Provisioning of the U.S. Army Intelligence and Security Command (INSCOM) Cloud Initiative (ICI) web interface.

Background

In context, interoperability training opportunities are invaluable in a theater where the Army has a reduced force

posture in comparison to historical Cold War levels. In 1989, approximately 214,000 Soldiers covered a concentrated 175-mile frontage associated with the Fulda Gap. The Fulda Gap included several open passes northeast of Frankfurt, Germany, which was a likely invasion route for Soviet Bloc forces. Today, with the Warsaw Pact dissolved, 33,000 Soldiers supporting Operation Atlantic Resolve face a revanchist Russia across a much wider frontage spanning from Estonia to Bulgaria. To capably defend this terrain, Atlantic Resolve forces depend on allies and partners. In particular, across the Atlantic Resolve nations, this includes a multinational corps, three multinational divisions, and the Enhanced Forward Presence battlegroups in the Baltics and Poland. Additionally, Polish land forces include the Polish 11th, 12th, and 16th Divisions, all of which would play a vital role in stemming aggression in the event of a future military conflict.

Through dozens of exercises conducted annually, U.S. Army Europe hones its interoperability competencies with these elements as well as many other contributing military bodies. DEFENDER-Europe 20 was designed originally as an opportunity to do this at scale. Through the initial mobilization for the exercise, the Army tested force projection capability, coordinating large-scale movements from across multiple airbases and ports for onward movement to training areas in Germany and Poland. When the tactical portion of the exercise was changed to a modified division-level live exercise concept, the 1st Cavalry Division focused on drawing out key interoperability lessons realized in conjunction with elements from the Polish 12th Mechanized Division and the Polish 6th Airborne Brigade.

Friendly Collection and Information Operations

The first key lesson learned pertains to the unique capabilities and authorities our allies and partners possess. Successfully leveraging these competencies can significantly enhance friendly collection and information operations. The Polish 12th Mechanized Division brought two notable tactical capabilities to DEFENDER-Europe 20, both especially suited for European theater operations. The Drawsko Pomorskie Training Area featured dense foliage and numerous water obstacles, and the exercise took place during Poland's wet season. Polish personnel carriers (Rosomaks and BMPs) were equipped to ford large bodies of water and were able to conduct reconnaissance in portions of the training area that Bradley Fighting Vehicles could not access. Polish elements also employed a maneuverable quadcopter unmanned aircraft system that was able to fly underneath low ceilings and in conditions prohibitive to Shadow and Raven operations. The 2nd Brigade Combat

Team, 3rd Infantry Division, which was the participating regionally aligned forces brigade combat team, received both capabilities through scenario cross-organizational decisions and proved especially adept at developing ground and aerial collection plans that leveraged them effectively.

The Polish also offered unique collection capabilities and authorities that they employed to protect the integrity of the DEFENDER-Europe 20 exercise in the face of real-world adversary propaganda efforts. Polish open-source intelligence cells constantly monitored the information environment in the period leading up to and during the exercise. Adversary messaging attempted to frame Poland and the United States as irresponsible for continuing the exercise in a COVID-19–threatened environment. When these narratives were published, early Polish open-source intelligence detections enabled timely and robust whole-of-government Polish messaging responses. Subsequently, other participating partners capitalized on this Polish competency to enhance similar narratives.

Overall, successfully incorporating Polish capabilities during DEFENDER-Europe 20 required deliberate arrangements planned and executed by the participating units. For example, the division (forward) G-2 officer in charge met with all unit S-2s during the military decision-making process to develop primary, alternate, contingency, and emergency communication plans and to discuss simulated intelligence collection constructs. During the exercise, the Polish airborne reconnaissance element provided an intelligence liaison officer to the division command post; and the 2nd Brigade Combat Team, 3rd Infantry Division's S-2 embedded an intelligence liaison officer in the Polish 2nd Mechanized Brigade, 12th Mechanized Division's command post with the Polish S-2. These arrangements ensured a common understanding of respective capabilities and the timely sharing of intelligence reporting.

Transition to the Mission Partner Environment

The second key interoperability lesson learned during DEFENDER-Europe 20 pertains to the Department of Defense and U.S. Army transition to the MPE information sharing capability. Incorporation of MPE was a keystone training objective for DEFENDER-Europe 20, with Polish forces accessing the network assisted by a regional signal support team. Network architecture planning enabled both Polish and United States elements to establish MPE network footprints, which capably facilitated the command and control of tactical operations in the Drawsko Pomorskie Training Area. However, although network access was robust, the operational environment information available for initial planning on the MPE network was minimal.

Thus, accessing and sharing items such as specialized maps, advanced terrain analysis, and timely imagery were difficult to accomplish during the exercise.

Capabilities of MPE

MPE will support an estimated 45,000 users with basic human-to-human services, such as chat, email with attachments, web, file-share, and other services, like command and control, weather, logistics, and planning. Specifically, it—

- ◆ Simplifies/standardizes information sharing through virtualization technologies.
- ◆ Eliminates costly and slow mission-specific build-outs.
- ◆ Operates at a variety of classification/releasability levels.
- ◆ Is comprised of [Department of Defense] DoD and mission partner-provided infrastructure, services, and agreed upon procedures.
- ◆ Allows the team to aggregate, reconfigure, and disaggregate as required.
- ◆ Is scalable and can support small enclave to major multi-nation coalition operations.
- ◆ Frees planners to focus on unique mission capability needs by using a shared suite of utility-like services, such as email, chat, voice, or video teleconferencing (VTC).¹

This issue in part hinged on the fact that MPE is not yet a mature network in theater, and therefore the tremendous amount of resources and theater databases currently available on the U.S. network are not yet accessible on MPE. For example, geospatial intelligence analysts and geospatial engineers participating in the exercise did not have access to the many terabytes of map data they would typically use to complete robust intelligence preparation of the battlefield planning. During DEFENDER-Europe 20, a cross domain solution was available at the U.S. Army Europe level. However, the cross domain solution process did not facilitate the transfer of items along a time horizon responsive to the real-time change of mission planning efforts.

Moving forward, in consideration of both future exercises and real-world operations, it is critical that the transfer of information and intelligence databases to MPE be prioritized at every echelon. This will require time and investment. Many products on the U.S. system are already classified at the SECRET//Releasable level and can be transferred to MPE without declassification or disclosure decisions. However, a significant number of other valuable products are overclassified and will require vetting by a foreign disclosure officer. This should happen both proactively, during the product creation phase, and retroactively, in terms of culling existing databases, identifying relevant items suitable for clas-

sification downgrade, and transferring those items to the MPE network. Although these solutions involve time-consuming processes, the availability of theater databases on MPE will allow for true interoperability during both exercises and real-world operations with our allies and partners.

Provisioning of the INSCOM Cloud Initiative Web Interface

The third intelligence interoperability takeaway from the DEFENDER-Europe 20 experience stands out as an area in which a training objective was not fully realized. The 1st Cavalry Division's G-2 and G-6 forward elements worked throughout the duration of the exercise to provision the ICI web interface to both United States and Polish counterparts but ultimately proved unsuccessful with Polish elements.

For context, ICI boasts numerous features that make it an ideal interoperability platform. INSCOM's design for the tool allows it to flexibly ingest data sources from across a range of organizations and sources, and users can view/manipulate that data through simple yet logical display tools. As a web interface, it bears some similarity to the Army's Command Post Computing Environment interface, but many features are tailored for intelligence consumers. Access to ICI is also generically afforded to other allies and partners because availability is not hamstrung by cumbersome licensing or software agreements.

At U.S. division and brigade echelons during DEFENDER-Europe 20, ICI worked as a key combat multiplier for intelligence and targeting operations. Using ICI as a common intelligence picture display, the 1st Cavalry Division G-2 was able to overlay operational graphics and develop separate user groups in ICI to ensure disciplined management of threat icons at echelon, in the brigade, division close, and division deep areas. Enemy icons were built and published in the Distributed Common Ground System-Army, and the 66th Military Intelligence Brigade's cross domain solution allowed those icons to appear on both the SECRET Internet Protocol Router and the MPE networks at multiple geographically distanced headquarters, including 1st Cavalry Division's main command post participating from Fort Hood, Texas. The exercise moving target indicator and full-motion video feeds were both readily available to all users with access to ICI. ICI also stood out as the only source of exercise intelligence on the MPE network. The G-2 targeting officer and collection manager used this intelligence to tip and cue simulated intelligence, surveillance, and reconnaissance assets such as Gray Eagle to confirm target locations and differentiate high-payoff targets from other less lucrative collects.

Ultimately, ICI was the only mechanism available to comprehensively share and manage situational awareness with Polish intelligence counterparts. However, despite significant troubleshooting, the Polish were unable to access ICI successfully during the 9-day live portion of the exercise. U.S. theater network technicians required additional approvals to add ICI to the common services hub within the demilitarized zone on the U.S.-owned portion of MPE. As such, Polish network technicians were not able to access ICI on MPE in the same way the United States units could.

NATO network interoperability, including access on MPE, is governed through the Federated Mission Networking initiative. According to NATO, the Federated Mission Networking was built to enable the “rapid instantiation of mission networks by federating NATO organizations, NATO Nations and Mission Partner capabilities, thereby enhancing interoperability and information sharing.”² NATO accomplishes

this through publishing spirals of the capability, or sets of network interoperability standards. Moving forward, key capabilities such as ICI will become even more necessary to enable interoperability as multinational collaboration opportunities increase. In this environment, intelligence leaders must understand network certification and access requirements in order to ensure intelligence equities are adequately postured for multinational operations.

Conclusion

Overall, a modified DEFENDER-Europe 20 exercise allowed valuable perspective regarding intelligence interoperability initiatives. Future exercises, including the upcoming



U.S. Army photo by SGT Andres Chandler

A U.S. Army first lieutenant assigned to Company C, 3rd Battalion, 67th Armored Regiment, calls out the description, distance, and direction of enemy opposing forces for his infantry dismounted fire team to lay suppressing sectors of fire during exercise DEFENDER-Europe 20/Allied Spirit at Buchierz Range, Drawsko Pomorskie Training Area, Poland, June 10, 2020.

DEFENDER-Europe 21, offer additional opportunities to expand on the lessons learned and test additional initiatives. Meanwhile, leaders retain the responsibility to codify best practices, ensuring they are reinforced at echelon both in interoperability standard operating procedures and in governing documents such as the Federated Mission Networking spirals. If successful, U.S. forces will operate confidently in the face of adversary aggression, knowing the theater is set and allies and partners are poised to effectively leverage individual competencies toward the realization of multiplicative effects. ✪

Endnotes

1. “DoD’s Mission Partner Environment – Information System (MPE-IS),” Chief Information Officer, U.S. Department of Defense website, accessed 26 August 2020, <https://dodcio.defense.gov/In-the-News/MPE/>; Department of Defense, Department of Defense Instruction 8110.01, *Mission Partner Environment (MPE) Information Sharing Capability Implementation for the DoD* (Washington, DC: U.S. Government Publishing Office, 25 November 2014), <https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/811001p.pdf>.
2. “Federated Mission Networking,” NATO Allied Command Transformation website, accessed 26 August 2020, <https://www.act.nato.int/activities/fmn>.

MAJ Chad Lorenz is the S-2 for 1st Armored Brigade Combat Team (ABCT), 1st Cavalry Division, forward deployed to Europe as the regionally aligned forces ABCT. He most recently served as the 1st Cavalry Division (Forward) G-2 in support of U.S. Army Europe and the Operation Atlantic Resolve mission. His previous assignments include three tours in Afghanistan and two rotations in the U.S. European Command area of responsibility. MAJ Lorenz is a 2007 graduate of the U.S. Military Academy and received his graduate degree in policy management from Georgetown University in 2017.





Interested in an Intelligence Career with a Fort Bragg Special Missions Unit?

TRUST ▲ ADAPTABILITY ▲ COMMITMENT



THE Mission

Entrusted with the Nation's most critical tasks, we stay at the leading edge of operations that immediately impact global security.



National Crisis Response

Some problems require immediate action and application of unique skills where failure is not an option.



High Value Targeting

We specialize in capturing and eliminating the most influential threats to our Nation and the World.



Combat Development

Staying at the forefront of the modern combat environment requires continuous development of cutting edge tools and weapons, by individuals who operate at the highest levels.



Assignments for:

35A, 35D, 35F, 35G, 35L
35M, 35N, 35P, 35S, 35T
35X, 35Y, 18F

Apply in 4 Easy Steps

Step 1

Email your SRB/ORB to:

army.sof1-recruiter@mail.mil

and request an online application



Step 2

Complete and Submit an online application consisting of:

- Application
- All OER/NCOERs
- Commander Evaluation
- All 1059s
- Updated ORB/SRB
- Security Clearance (SF 86)



Step 3

Attend an assessment



Step 4

Those selected will PCS to Fort Bragg to begin training or start work in their new position



"THE RELENTLESS PURSUIT OF EXCELLENCE"

CALL (910) 643-0699

COVID-19 Surveillance: Hidden Risks and Benefits for Identity Intelligence



by Ms. Christine Kaiser, Mr. Gregory Smith, and Mr. Kasey Diedrich

The views expressed in this article are those of the authors and do not necessarily reflect the official policy or position of the Departments of the Army or Defense, or the U.S. Government. This article does not imply nor should the reader infer the policies and regulations covering intelligence oversight have changed. Intelligence activities must comply with and adhere to applicable law and policies pertaining to the collection of publicly available information and U.S. person data. These include, but are not limited to, Executive Order 12333, the Foreign Intelligence Surveillance Act, DoD Manual 5240.01, and AR 381-10.

Identity intelligence is “the analysis and fusion of human signatures with other information concerning individuals, entities, groups, networks, or populations of interest to identify intent, actions, and activities for validation during the assessment.”

—Identity Intelligence Concept of Operation

Introduction

Just as Galileo’s first crude telescopes resolved the light of distant celestial bodies, a new generation of tools is enabling the world to distinguish previously uncollectible and indiscernible human signatures. By fusing diverse data sets and taking advantage of rapidly improving new technologies, identity intelligence (I2) promises to offer ever-clearer insights into the human mosaic, including in public, private, military, and civilian sectors. However, the advent of artificial intelligence-enabled biometrics, big data, increased computing power, and worldwide crises, such as the coronavirus disease 2019 (COVID-19) pandemic, is driving exponential growth in personal data production, data capture ability, and data fusion using machine-aided ana-

lytic systems. Worldwide COVID-19 is forcing human activity to accelerate online, generating increased personal and professional digital interaction from which useful patterns can be discerned. In the competition phase of multi-domain operations, the troves of I2 data generated from our digital footprints can highlight patterns of movement, military planning, and key individuals, providing immense value to friends or foes with mature I2 capabilities. Conversely, I2 with foreign datasets can assist U.S. commanders in understanding and better identifying the human aspect of the operational environment across all physical domains (air, land, maritime, space, and cyberspace) and within the information environment. As the Army transitions away from counterinsurgency-centric operations and postures

for future large-scale ground combat operations against peer/near-peer nation states, the military force that can access foreign I2 data and best use I2 tools will have a distinct advantage in more fully understanding the operational environment, and thus be able to more effectively employ capabilities on the battlefield.

Background

An article in the January–March 2020 *Military Intelligence Professional Bulletin*, titled “Identity Intelligence Contributes to Multi-Domain Operations,” examined how I2 can support multi-domain operations across all of its phases, including competition, armed conflict, and return to competition.¹ We continue the I2 theme in this article by highlighting the increasing global availability of and interest in I2 data, which is a fusion of biometric, biographical, and behavioral attributes that can provide powerful analytic insights at micro- and macroscales. In all multi-domain operations phases, I2 can support the identification of persons of military interest, and their intent, by distinguishing individuals from each other; discovering new threats; linking individuals and threats to other people, places, things, actions, and activities; and properly characterizing individuals, entities, groups, networks, and populations of interest. In the conflict phase, I2 can support commander and staff decision making by answering priority intelligence requirements and providing intelligence to support kinetic and non-kinetic targeting. The use of I2 enables targeting in future large-scale ground combat operations by increasing commanders’ situational understanding/situational awareness and helping to prevent peer/near-peer threats from gaining positions of advantage.²

The exponential growth of foreign data as countries step up surveillance efforts within their borders could prove a boon to the United States and allies in answering commanders’ priority intelligence requirements. However, adversaries, unconstrained by U.S. privacy and civil liberties laws, will take full advantage of U.S. persons’ publicly available information and seek ways to seize non-public I2 data to answer their own intelligence requirements.

Biometric Data

Biometric data include metrics relating to human features—such as fingerprints, iris scans, facial photos, and voice prints—that could be used to distinguish individuals. Biographical data include name, address, gender, marital status, and birthdate. Behavioral attributes identify people by the ways in which they interact with the world or a device. Examples include how individuals perform the following: walk, known as gait recognition; hold and interact with a device; operate a computer mouse; or type on a keyboard.

U.S. Privacy and Civil Liberties Laws

U.S. agencies engaged in domestic security investigations operate under, and are restricted by, clear legal frameworks pertaining to collecting publicly available information. These include, but are not limited to, Executive Order 12333, the Foreign Intelligence Surveillance Act, Department of Defense (DoD) Manual 5240.01 and various other DoD instructions, and AR 381-10 (*U.S. Army Intelligence Activities*). These legal frameworks ensure that the intelligence community collects, retains, or disseminates information concerning U.S. persons only in accordance with procedures established by the head of the intelligence community element concerned or by the head of a department containing such element and approved by the Attorney General after consultation with the Director of National Intelligence. Collection following these legal frameworks respects U.S. citizens’ privacy rights and civil liberties.

Old Idea, New Tools

The idea of gathering large amounts of seemingly innocuous data tied to an identity is not a new concept. As a marketing tool, such efforts have distilled general and individual consumer tastes and preferences for decades. What is rapidly changing is where and how the gathering of artificial intelligence-enabled biometric data is occurring in a world that is increasingly harnessing big data. Also changing is how those data are aggregated with biographical data to become a powerful I2 tool for operational use. Devices such as smartphones have enabled tremendous new and expanded data mining opportunities, even in the most remote villages of the world. Although smartphones provide convenience and services to users, they also serve as tracking devices for marketing firms that can use Global Positioning System location technology to profitably trace users’ locations and behaviors for their public and private clients.³

Although a privacy-conscious smartphone user in some countries may be able to somewhat minimize his digital footprint, a growing Internet of Things ecosystem has multiplied the sensors that can be used to generate I2 data whether or not users opt in. For instance, many foreign governments are implementing smart cities that enable technology to improve a city’s governance, planning, management, and liveability through the gathering of real-world, real-time data from a variety of collection devices. Smart cities are enabled by our digitized world, in which increasingly powerful computer technology, fifth-generation cellular communications, artificial intelligence-enhanced facial-recognition cameras, and inexpensive internet-connected sensors of all kinds are linked. According to one smart city vendor website, by the end of 2020, trillions of gigabytes of data will be generated daily.⁴ These data are touted as having the ability to provide insights to help local governments predict where, when,

and how city assets (for example, transportation, power generation, and mobility) behave and thereby enable cities to plan for growth, maintenance, and infrastructure development. Smart cities also emphasize public safety—they are increasingly implementing the wide-scale use of artificial intelligence-enabled facial-recognition cameras and vehicle license plate readers to identify law offenders and persons of interest in real time.⁵

get and forcibly intern whole populations of ethnic minorities in the formerly restive state of Xinjiang.⁷

COVID-19 Outcomes: Privacy Concerns versus Public Health Justifications

Although the COVID-19 pandemic is an epidemiological threat, it serves as a new and powerful driver to increase the depth and scope of these surveillance systems to identify,

assess, and track individuals and larger human patterns. Because of COVID-19 and increasing global health concerns, foreign governments in crisis are attempting to use every physical and digital means available to identify and perform contact tracing of infected individuals. Countries such as Singapore, China, Taiwan, and South Korea are attempting to control the epidemic by using mass surveillance of mobile phones, credit cards, rail, and flight data and by using closed-circuit television camera footage to track those afflicted with the virus, ultimately to prevent them from coming into contact with healthy populations.⁸ More generally, public health officials are also using this technology

to observe, by monitoring overall population movements and travel patterns, whether populations are adhering to social distancing guidelines to slow the spread of the pandemic.⁹ For example, one analytic suite of tools, which Italy implemented into one of its smart cities for urban planning, displays anonymized and aggregated location data from connected vehicles' sensors, navigation systems, mobile phone applications, and governmental agency data. At the regional, provincial, and municipal levels, the software generates the daily percentage variation in the number and



Illustration public domain courtesy of Pixels.com

Cities around the world are rolling out systems designed to gather and analyze data for the public good.

Such smart city efficiency improvements have provided foreign countries with new capabilities to build surveillance systems into their deepest infrastructures, enabling them to use device and social media data to provide citizens with or deny citizens of state-sanctioned benefits. China, for example, mandates that citizens use government-sanctioned mobile phone applications to show their “social credit scores” to vendors and government officials when seeking services. Russia attempts to alter the behavior of certain domestic and foreign audiences through targeted social media influence campaigns.⁶ Increasing computational power, in conjunction with the expanding efficiencies of artificial intelligence, enables the fusion and machine-driven analysis of diverse data sources.

Imagine a world in which aggregated I2 databases exist to fuse one’s biographical, behavioral, and biometric data (for example, identified images of one’s face from official documents, one’s voice prints from their phone, social media activities, travel patterns, and even a quantified signature of one’s way of walking as seen from public cameras) to locate, identify, and characterize individuals at the whim of governments. This pervasive I2 could be realized in a not too distant future in foreign countries that have the resources and the desire. China has used these tools very effectively to tar-



Photo illustration by the National Ground Intelligence Center

In the future, smartphones, smart city camera systems, social media, and contact tracing will work together to make surveillance increasingly effective in public areas.

distance of trips compared with January 2020 (the COVID-19 outbreak onset) and the proportion of incoming and outgoing daily and weekly trips according to origin or destination.¹⁰

Foreign governments that have not previously purchased smart city surveillance systems are very likely seeing the advantages of those systems because of the crisis.¹¹ Chinese companies, which lead this market, will likely take advantage of the current climate to aggressively market their surveillance systems to previously uninterested or unconvinced customers, or to augment and expand existing installed systems.¹² China has successfully employed facial-recognition technology to control the activity of its citizens within its own smart cities, and now in response to the pandemic, its major technology companies are expanding their mass digital surveillance networks to include people's health data.¹³ Vendors will argue that smart city technologies provide the intelligence-gathering and analysis tools critically needed to manage people in urban areas facing COVID-19 and future pandemics. Governments with weak democratic institutions that buy in, armed with emergency powers and increased financial resources to tackle the crisis, will have little incentive to restrict these systems once this particular crisis is over—especially in a world that has been traumatized and now fears the next pandemic.

Although many foreign countries that have historically protected personal privacy are doing their best to anonymize and compartmentalize the COVID-19 contact tracing information for health professionals only, in other countries, significant I2 data are readily accessible by nonmedical government personnel and thus enable data sharing for agile government responses.¹⁴ Other types of biometric and biographical data, taken from mobile devices, are available for purchase by savvy buyers, including foreign governments using emergency powers (regardless of legalities).¹⁵ Governments will almost certainly also purchase sophisticated and available tools to gain sharper insights from these I2 data to target, trace, and isolate individuals and those with whom they have come in contact.¹⁶

Looking Ahead: Growing Capabilities and Novel Uses

Massive amounts of I2 data are being generated globally, and the COVID-19 pandemic is loosening restrictions in many foreign countries, enabling the aggregation of data

Disclosed Information	Germany	Hong Kong	New York	Singapore	South Korea	U.K.
Age and gender	*	*	*	*	*	
Geographical breakdown of patients	*	*	*			
Home address (area)		*		*	*	
How case confirmed					*	
Identified contact persons		*			*	
Links to previous cases	*	*		*		
Nationality if case is imported				*	*	
Prior places visited				*	*	
Travel history		*	*	*	*	*
Treatment location		*		*	*	*
Workplace address				*	*	

Personal data governments have released about COVID-19 patients.

Table by author, Ms. Christine Kaiser

and overlooking the legal frameworks meant to protect privacy. A more sympathetic legal framework driven by public health concerns and coupled with the availability of aggregation tools, training, and maintenance (such as those that smart cities offer) will enhance public sector I2 in the future. Even though privacy concerns limit the collection, usage, and dissemination of data in Western democracies such as the United States, the overall global collection and aggregation of these data are unlikely to cease with the de-escalation of COVID-19 concerns once governments realize how powerful state-level I2 tools are to gain knowledge and insight for managing and potentially even avoiding state-level crises.

From a military perspective, the same technology tools offering the ability to track human patterns broadly or individuals more specifically for epidemiological control could also determine the military-related indications and warnings of adversarial action. As data explodes and governments increasingly harness I2 capabilities to aggregate and make sense of human activity, these digital footprints become an attractive target for adversarial states. The ability to remotely collect identity information—including biographical, biometric, behavioral, and relevant publicly available data about an individual through digital means—can provide the ability to target key players during the competition phase. Competitive defense organizations with these I2 tools, in a digital age, could monitor troop movements, identify and follow message traffic between troops and their families, and analyze foreign military actions and patterns. Those who can obtain, through whatever means, global I2 data

troves that countries are increasingly building will have powerfully enhanced abilities to understand who the enemy are, where they are, and what they are planning well before the eruption of open conflict.

During the competition phase of multi-domain operations, the deep fight can be taken to the stateside homeland, where our data are locally generated but become borderless in the cloud because of the internet. In today's digital realm, everyone is connected to the internet to shop, bank, socialize, and work, often using mobile phones that signal exact locations and patterns and that are linked to identities. An adversary that could access these digital footprints could recognize Army reservists getting ready to leave their homes for deployment, conducting revealing travel patterns that serve as indicators. Once deployed, Soldiers will not take their mobile phone with them to observation posts or on patrol; however, as off-duty Soldiers access and post to social media to stay in touch with family, plenty of I2 data valuable to an adversary will continue to be generated. Foreign governments conducting surveillance, data collection, and I2 analysis, initially in response to COVID-19, may have new clarity within their borders to identify patterns of interest from a military intelligence perspective (for example, activity of Soldiers and/or assets in country).

Key Takeaways

In the near future, joint operating environment priorities will potentially undergo shifts due to deployments in regions with highly sophisticated personally identifying data collection, aggregation, and pattern analysis capabilities. These places may have newly enhanced abilities to understand who we are, where we are, and what we are planning, thus posing a threat to cover and to conventional military operations.¹⁷ The I2 data and analysis will help reveal unexpected patterns of movement and behavioral anomalies at individual or group levels that may have been the most effective way to conceal activity previously. In addition, the potential availability of such data in the cyber domain may enable intelligence organizations—both friend and foe—to better understand the operational environment.

Military intelligence officers and military decision makers need to recognize the rapidly developing permissive collection environment that the COVID-19 pandemic has accelerated. This new reality is driving nations to use I2 technology to access and consolidate individuals' data into huge repositories for identity analysis. These new I2 capabilities have implications for the DoD because I2 can be used to inform policy and strategy development, conduct operational planning and assessments, and target individual identities at the

point of encounter. Under this new environment, operational decision makers should reevaluate how the U.S. military conducts planning, training, and collection long before the opening of hostilities. 

Epigraph

Headquarters, Department of the Army G-2, *Identity Intelligence Concept of Operation* (Draft) (Washington, DC, 2020).

Endnotes

1. Peter Baber, Pamela Baker, and Mark Dotson, "Identity Intelligence Contributes to Multi-Domain Operations," *Military Intelligence Professional Bulletin* 46, no. 1 (January–March 2020): 24–28.
2. Headquarters, Department of the Army G-2, *Identity Intelligence Concept of Operation*.
3. Matthew Johnston, "Smartphones Are Changing Advertising & Marketing," Investopedia, March 26, 2020, <https://www.investopedia.com/articles/personal-finance/062315/how-smartphones-are-changing-advertising-marketing.asp>.
4. "Build on data for smart cities: What is a smart city?" Autodesk, accessed April 21, 2020, <https://www.autodesk.com/solutions/architecture-engineering-construction/smart-cities>.
5. Kashyap Vyas, "In What Ways Data Collection in Smart Cities Is Threatening?" Interesting Engineering, January 28, 2019, <https://interestingengineering.com/in-what-ways-data-collection-in-smart-cities-is-threatening>.
6. Stephan De Spiegeleire, Matthijs Maas, and Tim Sweijs, *Artificial Intelligence and the Future of Defense* (The Hague: The Hague Centre for Strategic Studies, 1 January 2017), [https://www.hcss.nl/sites/default/files/files/reports/Artificial Intelligence and the Future of Defense.pdf](https://www.hcss.nl/sites/default/files/files/reports/Artificial%20Intelligence%20and%20the%20Future%20of%20Defense.pdf).
7. Chris Buckley and Paul Mozur, "How China Uses High-Tech Surveillance to Subdue Minorities," *New York Times*, May 22, 2019, <https://www.nytimes.com/2019/05/22/world/asia/china-surveillance-xinjiang.html>.
8. Nicholas Wright, "Coronavirus and the Future of Surveillance," *Foreign Affairs*, April 6, 2020, <https://www.foreignaffairs.com/articles/2020-04-06/coronavirus-and-future-surveillance>; Shirin Ghaffary, "What the US can learn from other countries using phones to track Covid-19," Vox, April 22, 2020, <https://www.vox.com/recode/2020/4/18/21224178/covid-19-tech-tracking-phones-china-singapore-taiwan-korea-google-apple-contact-tracing-digital>; and Veronica Combs, "How smart city tech is being used to control the coronavirus outbreak," TechRepublic, March 30, 2020, <https://www.techrepublic.com/article/how-smart-city-tech-is-being-used-to-control-the-coronavirus-outbreak/>.
9. Yasheng Huang, Meicen Sun, and Yuze SuiHuang, "How Digital Contact Tracing Slowed Covid-19 in East Asia," *Harvard Business Review*, April 15, 2020, <https://hbr.org/2020/04/how-digital-contact-tracing-slowed-covid-19-in-east-asia>; and Isobel Asher Hamilton, "Compulsory selfies and contact-tracing: Authorities everywhere are using smartphones to track the coronavirus, and it's part of a massive increase in global surveillance," *Business Insider*, April 14, 2020, <https://www.businessinsider.com/countries-tracking-citizens-phones-coronavirus-2020-3>.

10. Sue Weekes, "Analytics tool launched to track mobility flows across Italy," Smart Cities World, 14 April 2020, <https://www.smartcitiesworld.net/news/analytics-tool-launched-to-track-mobility-flows-across-italy-5194>.

11. Simon Chandler, "How Smart Cities Are Protecting Against Coronavirus But Threatening Privacy," Forbes, April 13, 2020, <https://www.forbes.com/sites/simonchandler/2020/04/13/how-smart-cities-are-protecting-against-coronavirus-but-threatening-privacy/#2088e6a41cc3>.

12. Naomi Xu Elegant and Clay Chandler, "When red is unlucky: What we can learn from China's color-coded apps for tracking the coronavirus outbreak," Fortune, April 20, 2020, <https://fortune.com/2020/04/20/china-coronavirus-tracking-apps-color-codes-covid-19-alibaba-tencent-baidu/>; and Combs,

"How smart city tech is being used."

13. Ghaffary, "What the US can learn."

14. Wright, "Coronavirus and the Future of Surveillance."

15. Chandler, "How Smart Cities Are Protecting."

16. Ibid.

17. Der Spiegeleire, Maas, and Sweijs, *Artificial Intelligence*.

Ms. Christine Kaiser serves as an intelligence specialist in the Identity Intelligence Division with the Department of Defense (DoD). She has 20 years of experience as an all-source intelligence analyst, contract analyst, and Army Civilian intelligence specialist; 13 of those years are within the identity intelligence enterprise. She holds a bachelor of science in criminal justice and homeland security.

Mr. Gregory Smith is an analyst for identity intelligence with the DoD. He previously worked with the Federal Bureau of Investigation as an analyst on the National Name Check and Domain Intelligence programs. He holds a bachelor's degree in foreign affairs from the University of Virginia and a master of science from Colorado State University.

Mr. Kasey Diedrich serves in the Identity Intelligence Division with the DoD. He has 8 years of analysis and production experience, specifically within the identity intelligence enterprise.



What is Foundry

The Foundry Intelligence Training Program is a critical enabler to Army global readiness. It provides commanders the necessary resources (funding, facilities and subject matter experts) to prepare military intelligence Soldiers, Civilians, and units to conduct intelligence operations and activities at the tactical, operational, and strategic levels.

Foundry Training Types

Foundry enhances individual and collective intelligence training for the Active and Reserve Components through –

- a. Resident (TDY) or at a Foundry Site
- b. Live Environment Training
- c. Mobile Training Teams



Funding

Headquarters, Department of the Army, Office of the Deputy Chief of Staff for Intelligence, may allocate Foundry resources that support unit METL, Army Service component command's intelligence warfighter function training requirements and advanced intelligence training provided by the intelligence community.

Schedules

Foundry Courses can be scheduled through the Army Training Requirements and Resources System (ATRRS). ATRRS allows units to submit training requests online and view calendars of all available, requested, and scheduled intelligence training. ATRRS also displays training objectives, prerequisites, class size, and course administrative requirements. ATRRS URL: <https://www.atrrs.army.mil>.

Points of Contact

DA G-2 TRAINING POINT OF CONTACT
Foundry Program Manager: 703-695-1268
INSCOM FOUNDRY POINT OF CONTACT
Foundry Program Administrator: 703-706-1890
INSCOM ATRRS: 703-706-2227

Modernization of Army Counterintelligence and Human Intelligence Collection Management

by Ms. Erin Masly

Photo by Louis Hansel on Unsplash



Chess involves a struggle of wills, and it contains what has been termed the essentials of fighting—to strike, to move, and to protect.¹

Introduction

Picture it—commanders sending their infantry Soldiers to fight without weapons; the launching of aircraft with no identified target; and combat engineers wandering the countryside, unsure of where to build a necessary bridge for their advancing forces. Does that sound like a modern, efficient military force? Any good Soldier recognizes that the tactical force needs to know the objective and have the means to meet that objective. It is obvious that infantrymen need their rifles. But what about Soldiers whose mission is information? What weapons do intelligence Soldiers have, and are those Soldiers being properly equipped with those weapons?

Collection management is a vital function within the intelligence process at all echelons throughout the intelligence community. Like the conductor of a symphony orchestra, collection managers direct and manage a myriad of information requirements, collection requirements, and taskings to direct intelligence collection from the national to tactical levels. Just as an infantryman needs a rifle, intelligence collectors need an understanding of information requirements and identified targets for collection, and a plan on how to collect the necessary intelligence. Collection management is a military intelligence (MI) Soldier's weapon system.

“Collection management is the process of converting intelligence-related information requirements into collection requirements, establishing priorities, tasking or coordinating with appropriate collection sources or agencies, monitoring results, and retasking, as required.”² In basic terms, *collection requirements management* determines the collection requirements, while *collection operations management* determines the best approach to obtain the necessary information.³ Collection management provides a critical link between collection and analysis, supporting defined and focused operations for national, Service-level, and regionally focused objectives.

Army collection management for counterintelligence (CI) and human intelligence (HUMINT) has been instrumental in directing intelligence collection against counterterrorism and counterinsurgency missions over the past two decades. Robust collection management will continue to be vital in supporting the execution of the Army's vision to field a force by 2028 capable of deploying, fighting, and winning in a multi-domain, high-intensity conflict while simultaneously deterring others and maintaining the ability to conduct irregular warfare.⁴ Modernization of Army CI and HUMINT collection management will be necessary to support the vision's objectives to man, organize, train, equip, and lead the Army toward this capability.

Modernization in a Changing Environment

The 2018 National Defense Strategy spells out U.S. strategy to compete, deter, and win in the emerging security environment of peer and near-peer great power competition. The National Defense Strategy acknowledges the erosion of the U.S. military's competitive advantage and the increasing complexity of the security environment, requiring a more resilient and rapidly innovative joint force.⁵ In response to this need, the Army's modernization strategy highlights six modernization priorities that focus on driving the Army to create a more modernized force capable of conducting multi-domain operations as part of the joint force. These priorities are—

- ◆ Long range precision fires.
- ◆ Next generation combat vehicles.
- ◆ Future vertical lift.
- ◆ Network.
- ◆ Air and missile defense.
- ◆ Soldier lethality.⁶

The Army G-2X is reforming CI and refocusing HUMINT to meet this shift toward great power competition and Army modernization.⁷ Army CI reform will posture the force to better protect current technological development and future strategic capabilities. Service-level HUMINT capabilities will be focused and aligned more effectively against peer adversaries while increasing regionally focused theater collection capability to support combatant commands and Army Service component command priorities. In direct conflict with technologically advanced adversaries such as China and Russia, our systems and networks will be the first capabilities targeted and possibly compromised, leaving traditional human-based collection as the most reliable and available intelligence collection capability.

CI modernization requires efficient and agile processes to identify, disrupt, and mitigate foreign intelligence entities and insider threats across all phases of conflict in all domains. The future environment in which Army CI will operate is likely to be crowded and complex, dealing with dense urban areas, antiaccess and area denial challenges, and the impacts of technological change. This environment will likely see empowered elements and proxies and will require working in a degraded, intermittent, and low bandwidth communication environment while facing peer and near-peer foes with the potential of large-scale combat operations. Delivery of intelligence to the warfighter must occur with speed, precision, and accuracy.

Modernization of Army HUMINT means transitioning from the experience of deployed counterinsurgency operations in support of targeting to using Army HUMINT full spectrum capabilities throughout each phase and domain across the continuum of conflict to support modernization, set the theater, shape battlespace understanding, and enable commanders' decision making. HUMINT is critical to increasing lethality of the force and opening windows of opportunity across all domains by providing commanders with detailed knowledge of threat strengths, weaknesses, intentions, organizations, equipment, and tactics.



A U.S. Army Soldier and Afghan Border Policeman exchange greetings after assignment providing security to the same area at the Spin Boldak, Afghanistan district center for a district leaders' shura, on February 11, 2013.

Addressing Human-Based Intelligence

Human-based intelligence collection is the oldest form of intelligence. Information sharing between individuals, within communities, and among allied groups is at the base of human interaction. Some of the earliest writings on statecraft identify intelligence as a key component in maintaining the security of a state. In the era before the development of the modern technology that supports intelligence collection today, collection was undoubtedly human-based. From Sun Tzu's declaration in *The Art of War* that "one who knows the enemy and knows himself will not be endangered in a hundred engagements,"⁸ to George Washington's Culper Ring, human-based intelligence has been at the forefront of maintaining strategic advantage for thousands of years.

In a rapidly advancing, technologically focused battlefield, CI and HUMINT operations are unique in that the Soldier is the collection platform. Agents and collectors often perform their functions independently in one-on-one engagements, necessitating a level of understanding and independence in lieu of direct technological support. In order to be effective, CI agents must be aware of key U.S. technologies, research and development efforts, and priority critical infrastructure and locations in order to counter foreign

The Culper Ring

The Culper Ring was an American spy network operating during the War of American Independence that provided George Washington with information on British troop movements. This network operated successfully in and around New York City for 5 years, during which time no spy was ever unmasked. The name “Culper” was suggested by George Washington, taken from Culpeper County, Virginia.



Memoir of Colonel Benjamin Tallmadge. Sons of the Revolution, New York, 1904

Benjamin Tallmadge as a dragoon, by John Trumbull, c. 1783.

Informants used fake names and a numerical codebook consisting of 763 numbers representing words, names, and places to communicate their information. Developed by Major Benjamin Tallmadge, the Culper Code was essential in protecting the vital communications and identities of this important intelligence-gathering group.⁹

Word	Number	Word	Number	Word	Number	Word	Number
they	629	uncommon	676	Gen. Smith	718	Alphabet	
liberty	630	unfriendly	677	Dr. H. Lord	719		
thing	631	unfortunate	678	German d.	720		
though	632			Allen John	721		
times	633			Culper barn	722		
to	634			Culper farm	723		
troops	635	wind	679				
thoroughly	636	war	680				
therefore	637	was	681	Indian Rev	724		
timber	638	we	682	C. Brimston	725		
tory	639	will	683	Livingston	726		
transport	640	with	684				
trial	641	what	685				
traitor	642	wound	686	New York	727		
transcript	643	went	687	Long Island	728		
		want	688	Albany	729		

Pages from the Culper Code Book

intelligence entity threats. Likewise, HUMINT collectors must have an understanding of gaps in information with regard to adversary capabilities and intentions, as well as knowledge of the priorities of those gaps both within and between target areas. This intimate familiarization with collection priorities is a fluid process, requiring responsiveness to shifting focus areas and changing operating environments. Both CI and HUMINT rely on dynamic targeting practices to identify collection opportunities. This targeting is critical to successful CI and HUMINT collection operations, translating analytically identified gaps into targets of opportunity for collection. The ability to provide warning of intentions and identify enemy courses of action, both active and discarded, that are not otherwise easily observable or discernible, distinguishes these intelligence disciplines.

In order to be effective, CI and HUMINT operations require strong collection management at all echelons. Collection management provides a critical link between analysis and collection. This link synchronizes analytical assessments of gaps in knowledge of the adversary with HUMINT collection elements. Collection management also links analysis of critical U.S. technology and capabilities requiring protection with CI agents in the field. Collection managers are critical in providing collection support briefs and collection emphasis messages, and in assisting targeteers to develop targeting packages. Since human-based collection has the capability of doing specifically targeted collection as well as incidental collection, knowledge and understanding of a wide range of collection focus areas are necessary for both the CI agent and the HUMINT collector. Strong collection management support and direction provide this breadth and width of understanding. Additionally, CI and HUMINT have long lead times in the development of operations; therefore, priorities and specific requirements will doubtlessly change over the course of an operation. Collection management is vital to maintain clear and focused collection despite dynamic adjustments to priority areas over the course of time. The time and presence of CI and HUMINT collectors are as inherently limited as the shutter time and bandwidth of technically based intelligence sensors and must be managed actively in a similar fashion to generate efficient and effective collection.

Current Realities of Collection Management within CI and HUMINT

Currently, the Army has no codified collection management career field for CI and HUMINT—no military occupational specialty or additional skill identifier (ASI) covers CI or HUMINT collection management. Below the levels of Headquarters, Department of the Army and U.S. Army

Intelligence and Security Command, often collection management within Army CI and HUMINT units is an additional duty or an ad hoc assignment. Soldiers and U.S. Army Civilians filling these roles often learn on the job, and turnover is high as individuals rotate between duties. No formalized training route exists for CI and HUMINT collection management; likewise, current CI and HUMINT training pipelines do not robustly represent collection management duties and skills.

As CI and HUMINT operations have long lead times, leadership can often attribute preparation of operations as a lack of forward movement. This results in the use of CI and HUMINT forces for garrison duty, or other necessary support functions, but detracts from the intelligence collection mission. Similarly, many individuals often overlook collection management and do not view it as the critical function that it is. Collection elements may engage directly with their analytical cell to ensure a clear understanding of collection requirements and discuss collection opportunities generating notices of intelligence potential. While analyst-collector engagement is essential to support operations, collection management is a key partner in this dialogue to ensure the translation of analytical priorities through the lens of overall focus areas as part of a larger regional and Army strategy. Without effective collection management, collectors risk focusing their efforts on information that is not a priority collection area.



Soldiers with 163rd Military Intelligence (MI) Battalion, 504th MI Brigade, complete an interrogation exercise as part of certifying their MI platforms on Camp Bullis, TX, March 20, 2019.

Modernization of Collection Management

So how does the Army modernize management of the oldest kind of intelligence collection? Changing how CI and HUMINT collection management is viewed and conducted will require adjustments in three key areas: leadership, structure, and training.

The Army Intelligence Plan (TAIP), published by the Army G-2, identifies two lines of effort (LOEs): *CI Reform*, LOE-1; and *Modernization through implementing Multi-Domain Intelligence (MDI)*, LOE-2. Within LOE-1, TAIP indicates that Army CI must be better prepared to counter a “persistent and growing threat of Foreign Intelligence Entities.” This growing threat requires reform that includes changes to the CI force structure.¹⁰ One area that requires improvement is CI and HUMINT collection management.

Leaders across the Army MI Corps must have a greater understanding of collection management functions and capabilities, as well as the value that these functions and capabilities add to the mission. CI and HUMINT collection management must be fully incorporated into individual unit processes and must be regarded as a critical function—one that is worth maintaining regardless of budget considerations, restructuring, staffing levels, or other mission requirements.

MI units need to keep collection management positions as a permanent duty position. Personnel assigned as collection managers should remain in the position for a full assignment. The Army will address the professionalization of the collection management career field, possibly as an ASI within the CI and HUMINT disciplines. Completion of a CI or HUMINT collection management position could be a requirement for consideration for certain assignments or as a developmental position for officers. Some echelon above corps units, realizing the importance of CI and HUMINT collection, create ad hoc collection management cells (or fusion cells/centers) that include CI, HUMINT, and often open-source intelligence capabilities pulled from within their organic force structures. However, there is a potential risk when creating a capability from within—another organic unit capability may become the bill payer. In addition, these created cells take various forms and therefore lack standardization across units.

Collection managers must have access to focused CI and HUMINT collection management training, either as a stand-alone course or as part of the existing training pipeline. Current collection management training focuses on intelligence, surveillance, and reconnaissance (ISR) assets. While CI and HUMINT are in the intelligence category, traditional collection management focuses on electronic systems and platforms, not on intelligence collection using humans. In the latter case, HUMINT and CI collectors *are* the collection platform. Collection managers will benefit from including them in any collection synchronization matrix.

The inclusion of CI and HUMINT personnel in the Army Intelligence Development Program-Intelligence,

Surveillance, and Reconnaissance (AIDP–ISR), and the eligibility of CI and HUMINT Soldiers for advanced/ASI-producing collection management training, would be a partial step toward closing this gap. AIDP–ISR is the Army’s current effort to train and develop certified ISR collection managers who can operate at the tactical, operational, and strategic levels.¹¹ Another initiative that may generate comprehensive results is the establishment of an integrated concept team, led by the U.S. Army Intelligence Center of Excellence, to review gaps in collection management training and processes across the Department of Defense CI and HUMINT enterprise.

Modernizing CI and HUMINT collection management will be a long-term process that will require changing training; adjusting manning practices; and building greater understanding among leaders, agents, and collectors on the value and necessity of having a strong, committed force of collection management professionals. As the Army moves forward to combat the future’s emerging threats, Army CI and HUMINT collection management must, and will, help the MI force move out with clear and focused direction. ✨

Endnotes

1. Emma Young, “Chess! What is it good for?” *The Guardian*, March 3, 2004, <https://www.theguardian.com/science/2004/mar/04/2>. Quote by Swedish researcher, Jan Kuylenstierna, regarding the game of chess as it relates to modern warfare.

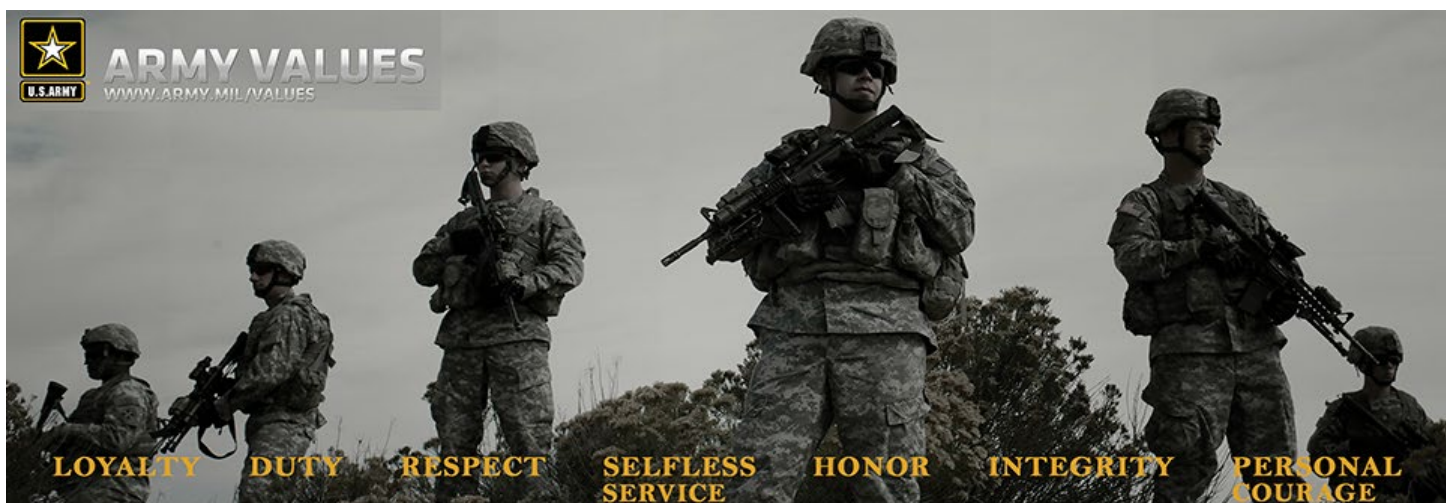
2. Office of the Chairman of the Joint Chiefs of Staff, Joint Publication (JP) 2-0, *Joint Intelligence* (Washington, DC: The Joint Staff, 22 October 2013), I-13.
3. Office of the Chairman of the Joint Chiefs of Staff, JP 2-01, *Joint and National Intelligence Support to Military Operations* (Washington, DC: The Joint Staff, 5 July 2017), III-16.
4. Department of the Army, *The Army Vision* (Washington, DC, June 2018), 1.
5. Office of the Secretary of Defense, *Summary of the 2018 National Defense Strategy of The United States of America*, n.d., <https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf>.
6. Department of the Army, *2019 Army Modernization Strategy: Investing in the Future*, n.d., 6, https://www.army.mil/e2/downloads/rv7/2019_army_modernization_strategy_final.pdf.
7. Marcus O’Neal, “Army G-2X Support to Army Readiness and Modernization Priorities,” *Military Intelligence Professional Bulletin* 46, no. 1 (January–March 2020): 20.
8. Derek M. C. Yuen, *Deciphering Sun Tzu: How to Read The Art of War* (New York: Oxford University Press, 2014), 110–111.
9. “Culper Spy Ring,” Mount Vernon website, accessed 23 November 2020, <https://www.mountvernon.org/library/digitalhistory/digital-encyclopedia/article/culper-spy-ring/>; and Wikipedia, s.v. “Culper Ring,” last modified 12 November 2020, 17:56, https://en.wikipedia.org/wiki/Culper_Ring.
10. Department of the Army, Deputy Chief of Staff, G-2, *The Army Intelligence Plan* (Washington, DC, 2019), 4.
11. Camero Song, “Army Intelligence Development Program-Intelligence Surveillance, and Reconnaissance: Critical to an Army Corps,” *Military Intelligence Professional Bulletin* 44, no. 1 (January–March 2018): 52.

Ms. Erin Masly is a collection manager for the Headquarters, Department of the Army (HQDA) Counterintelligence, Human Intelligence, Disclosure, and Security Directorate, Army G-2. She holds a bachelor of arts in international relations from Boston University. She previously served as program manager of the National Defense University’s Interagency Transformation, Education, and Analysis program and served in assignments at Army Operations Group and 902nd Military Intelligence Group.

Contributors:

CW5 Joseph Lancaster, Human Intelligence Readiness Officer, HQDA G-2X.

CW5 Traci Goodwin, Chief, Counterintelligence Initiatives and Readiness, HQDA G-2X.





Mental Health in the Intelligence Community, Uncovered

by Ms. Pamela J. Miller

Introduction

If your back aches, you go to a chiropractor. If your knee aches, you go to an orthopedic specialist. If your heart aches, you go to a psychotherapist. Our mental health is as important as our physical health! However, many military personnel choose not to seek help from a behavioral health professional for fear of “losing” their security clearance. This is acutely prevalent within the intelligence community.

The Mental Health Myth with Regard to Clearances

The Department of Defense (DoD) Consolidated Adjudications Facility determines a person’s security clearance eligibility once it receives a completed background investigation. Depending on the individual’s assignment, another agency may also need to do its own review because many missions and agencies within the intelligence community require specific levels of access. For example, an Army Soldier assigned to a National Security Agency (NSA) billet will require a background investigation adjudicated for top secret with access to sensitive compartmented information, known as TS/SCI. NSA will also vet the Soldier through its own system. This entire process often takes 6 to 12 months. After waiting so long to obtain these accesses, many Soldiers fear losing them because it would result in their inability to perform the mission.

In the field, Soldiers inevitably hear the story of a coworker who lost access to classified information after seeking help from a behavioral health professional. However, Soldiers are usually circulating an incomplete story because they do not have all the facts. The coworker might have been diagnosed with a mental health disorder that could potentially have had a negative impact on military readiness. Understandably, in this situation the diagnosis also affected the Soldier’s eligibility to access classified information. The reason for the pending discharge was not public knowledge, and the Soldier was not likely to share a mental health diagnosis with his team. Yet the perception was the DoD re-

voked the clearance because the Soldier sought help at a behavioral health clinic, which resulted in his subsequent discharge from the Army. That is not how it works. The DoD considers multiple guidelines and mitigating factors when determining whether to revoke a security clearance.

In truth, less than 1 percent of security clearance revocations are due to psychological conditions alone. In some cases, a Soldier may have been instructed to go to a behavioral health clinic because of a criminal act reported through family advocacy. In this circumstance, peers are probably not aware of the criminal act because of its sensitivity, but they are aware of the visit to the behavioral health clinic and assume that is why the Soldier “lost” his security clearance—thereby reinforcing the stigma of seeking assistance from a behavioral health professional. The timeline of events can also cause the misperception because the suspension of a security clearance often occurs quickly, yet a military discharge due to a mental health disorder could take more than a year.

The Importance of Seeking Help

Electing to seek help from a behavioral health professional indicates a Soldier is taking ownership of his personal situation—being proactive to correct a problem before it gets worse. Some Soldiers try to cope by using drugs or an excessive amount of alcohol, which can have a lasting effect on their career and security clearance. Others spiral out of control into a pattern of self-harm, harm of others, or even suicide.

According to a 2018 study, up to 23 percent of people with mood and/or anxiety disorders self-medicate with drugs or alcohol.¹ Alcohol is the popular choice because it is legal and easily obtainable. However, self-medicating in this way has the potential to lead to *alcohol use disorder*, which will impair the Soldier’s judgment, stability, reliability, or trustworthiness. This is a serious condition. According to the National Institute on Alcohol Abuse and Alcoholism, it is

“characterized by an impaired ability to stop or control alcohol use despite adverse social, occupational, or health consequences. An estimated 15 million people in the United States have [alcohol use disorder].”²

Signs of alcohol use disorder may not become apparent until the Soldier engages in a criminal act, such as driving under the influence, committing assault, or being drunk and disorderly. A security adjudicator will then review the case to decide if the Soldier will retain his security clearance. Had the Soldier gone to a behavioral health professional to get help for his depression, or other problem, rather than self-medicating with alcohol, the only adjudicative concern would have been psychological conditions. Instead, in addition to psychological conditions, concerns include criminal conduct and alcohol abuse. Depending on the severity of the criminal act, the Army may choose not to retain the Soldier, eliminating the need to make a decision about the security clearance.

Some Soldiers use shopping to cope with depression. The concept of excessive shopping may seem innocent enough; however, it can become an addiction. This may also lead to the Soldier being dishonest with her loved ones about the overextended spending, and the Soldier may accumulate serious credit card debt as a result. It is not uncommon for DoD security personnel to notice, through a process called *continuous evaluation*, that a Soldier has multiple delinquent accounts at low dollar limits because she has been keeping purchases a secret from her spouse and not paying the credit card bills. Do not cope alone! Seek help from a behavioral health professional!

What is Continuous Evaluation?

Continuous Evaluation (CE) is an ongoing screening process to review the background of an individual who is assigned to a sensitive position or has access to classified information or material. It exists to ensure that the individual should continue to retain a security clearance or the assignment to sensitive duties. CE leverages a set of automated record checks and business rules to assist in the ongoing assessment of an individual's continued eligibility.³

Identify the Problem Early On

DoD Manual 5200.02, *Procedures for the DoD Personnel Security Program (PSP)*, and AR 380-67, *Personnel Security Program*, identify the requirement to promptly report any information to the security office that suggests a Soldier may have an emotional, mental, or personality condition

that can impair judgment, reliability, or trustworthiness.⁴ Failure to self-report such criteria is a violation and could result in the suspension of access. Once an individual has reported the information to the security manager (or in the case of SCI and Special Access Programs, to the special security officer), these security professionals will refer to the adjudicative guidelines to determine what further action is required. Commanders/directors may remove local access or suspend all access to classified material when a Soldier's behavior casts doubt on his judgment, stability, reliability, or trustworthiness.

This does not mean the DoD will remove or suspend access because a Soldier voluntarily goes to marital, grief, or trauma counseling. In fact, seeking help for these three reasons is highly encouraged. However, certain psychological conditions may result in a temporary suspension until a mental health professional can confirm that the Soldier's condition does not adversely affect his judgment, reliability, or trustworthiness.

Once the mental health professional has determined the diagnosis and prognosis, the security officer sends the information to the DoD Consolidated Adjudications Facility for a final adjudication decision. A Soldier in the intelligence community will likely have multiple access levels requiring reinstatement after a suspension. For example, when the DoD suspends a TS/SCI clearance for a Soldier who has access to NSA, NSA also suspends access. If the DoD Consolidated Adjudications Facility reinstates the TS/SCI, only then will the NSA consider reinstating access as well. Although the process may seem lengthy, it is necessary because the protection of National Security Information is paramount.

Conclusion

We all experience the ups and downs of life, including severe stresses such as grief, trauma, financial difficulty, and divorce. If Soldiers take a proactive approach when dealing with these stressors by seeking help early on, they will mitigate their threat to national security. The identification of a mental health disorder may also help to mitigate other adjudicative concerns, such as financial, criminal, drug misuse, or alcohol abuse. The sooner the disorder is identified, the sooner the Soldier can receive the proper care and treatment to get healthy.

So spread the word: When Soldiers talk to a behavioral health professional, they are taking positive steps to improve their mental health. Their action is a sign of strength, and speaking up is a sign of responsible behavior and a commitment to performance. In most cases, it will not result in “losing” a security clearance. 

Endnotes

1. Sarah Turner, Natalie Mota, James Bolton, and Jitender Sareen, "Self-medication with alcohol or drugs for mood and anxiety disorders: A narrative review of the epidemiological literature," *Depression & Anxiety* 35, no. 9 (September 2018): 851–860, <https://doi.org/10.1002/da.22771>.
2. "Alcohol Use Disorder," National Institute on Alcohol Abuse and Alcoholism website, accessed 21 July 2020, <https://www.niaaa.nih.gov/alcohol-health/overview-alcohol-consumption/alcohol-use-disorders>.
3. "Frequently Asked Questions: What is Continuous Evaluation?" OPM.gov, accessed 21 July 2020, <https://www.opm.gov/faqs/QA.aspx?fid=cb3cafacc1e73-4a6b-bd88-a3adad355390&pid=d4b7d235-34d3-4dba-9c4e-4ad8f4e6e522>.
4. Department of Defense (DoD), DoD Manual 5200.02, *Procedures for the DoD Personnel Security Program (PSP)* (Washington, DC: U.S. Government Publishing Office [GPO], April 3, 2017), 69–70; and Army Regulation 380-67, *Personnel Security Program* (Washington, DC: U.S. GPO, 24 January 2014), 38.

Ms. Pamela Miller is the Chief of Personnel Security for the U.S. Army Intelligence and Security Command. She has 29 years of experience in the security specialty, including 7 years as a lead adjudicator with the U.S. Coast Guard and 9 years as an assistant regional security manager with the U.S. Department of Commerce. She is a retired Security Forces, U.S. Air Force reservist.



Photo by SGT Christopher Lindborg, Army Reserve

One team, one fight! Mental health is just as important for military readiness as physical fitness.

Military OneSource

While Military OneSource does not provide health care services, it does point members of the military family to the resources available to help.

<https://www.militaryonesource.mil/health-wellness/mental-health/>



MILITARY INTELLIGENCE NONCOMMISSIONED OFFICER PERFORMANCE: STRENGTHENING THE CORE

by Mr. Chet Brown, Chief, Lessons Learned Branch

“Sergeant, Paint the Flagpole”

I begin with the punchline of a joke: The [Officer Candidate School] OCS graduate second lieutenant turns to the platoon sergeant and says, “Sergeant, paint the flagpole.” The entire joke, which I will spare you from reading here, is often misused to demonstrate the stereotypical differences in lieutenants from three U.S. Army commissioning sources—U.S. Army Military Academy, Reserve Officer Training Corps, and OCS. What is not immediately apparent from the punchline is the confidence the OCS graduate has in the sergeant’s knowledge and proficiency to accomplish the task. The unstated expectation is that the sergeant will not paint the flagpole alone. The second lieutenant knows the noncommissioned officer (NCO) will assign the task to, and supervise, a team of Soldiers, not only to complete the task but also to complete it to standard. A standard that includes ensuring the Soldiers are properly equipped, the team is properly trained, the task has been rehearsed, and the mission is accomplished in accordance with all appropriate regulations, policies, safety measures, and Soldier welfare considerations. The NCO will ensure a prompt, high-quality result.

Expecting the task to be done correctly by simply putting an NCO in charge exemplifies the adage that the NCO Corps

is the backbone of the Army. This theme appears throughout Army doctrine, including the foreword to TC 7-22.7, *The Noncommissioned Officer Guide*, where the Sergeant Major of the Army Michael Grinston writes, “Throughout the history of the U.S. Army, the NCO has been its backbone.”¹ The adage is also in the preface to TC 7-22.7: “You are ‘The Backbone of the Army.’”²

The Backbone

I hope you’re picking up on the not too subtle message that reading, or at least skimming through, *The Noncommissioned Officer Guide* is worthwhile. All Army professionals, including Army Civilians, should read it to understand the importance of the NCO’s role in preparing to fight, and win, any engagement with any current or emerging near-peer threat. The guide also includes a description of the relationship between officers and NCOs and between Army Civilians and NCOs.³

Here is another quote from the guide: “The NCO corps is the vanguard for leading and training Soldiers at the crew, team, squad, section, and platoon level. Focusing on the basics with tough, realistic combat training, will ensure that in the crucible of ground combat, our Soldiers will be

victorious.”⁴ Also, “NCOs are trainers.”⁵ The NCO’s role in training used to be one of the Army’s seven principles of training; now the role is the first of four principles—*train as you fight*.⁶ NCOs are directly responsible for training individual Soldiers, crews, and small teams.

Don’t Diminish the Role of the NCO in Training

I (over) emphasize doctrine to provide the context necessary to indicate the severity of a report compiled by the Lessons Learned Team at the U.S. Army Intelligence Center of Excellence (USAICoE)—*Observed MI NCO Challenges 2019–2020*. The report cites areas of concern that relate to NCO training. We must apply doctrinal tenets, principles, and intent; otherwise, we risk dismissing these challenges if we assume the actions of others (officers, Army Civilians, or contractors) are sufficiently addressing deficiencies. However, it is fundamentally wrong to diminish the role of the NCO in training, no matter how slight or temporary that role may be.

It has been a long time since I served as an NCO; yet I struggle with a bit of misophonia whenever I hear an NCO seeking to have an “outsider” meet a training objective that the NCO is capable of accomplishing. Every major Army installation or joint base has a variety of differing and various training resources to assist NCOs in serving as their organization’s primary trainer. Too often, these resources are perceived as surrogate trainers or the primary training provider. The same problem occurs with mobile training teams staffed by Army Civilians or contractors, or a mix of both. This isn’t my opinion; it’s what NCOs have told us, the USAICoE Lessons Learned Team, over the past 18 to 24 months.

NCOs Relinquished the Role as the Primary Trainer

As difficult as it is to read or hear, it was easy to understand how the condition developed. An oversimplification of the situation is to state that officers, warrant officers, and advanced individual training (AIT) Soldiers received more emphasis on the combined arms maneuver aspects of intelligence schoolhouse training. While certainly true, additional factors emerged when discussing the military intelligence (MI) NCOs’ challenges.

In the tactical formations, MI NCOs found it difficult to synchronize the training of MI Soldiers distributed among

differing organizations. The locations of MI Soldiers in the current brigade combat team’s (BCT’s) organizational structure added complexity when operating in garrison or the field. Some units are able to overcome these difficulties when the BCT S-2 operates as the senior intelligence officer for the entire MI complement within the BCT formation. That’s a good start. We’re confident a trained, skilled, and able officer will fill every BCT S-2 position. Is the BCT S-2 intelligence master sergeant (military occupational specialty [MOS] 35Z, Intelligence Senior Sergeant) position always filled by an MI master sergeant? How often does the BCT senior intelligence sergeant (an infantry sergeant first class position) serve as the BCT S-2 section senior NCO? What about the differing sections of the BCT S-2 cell or the MI company when combined to form the brigade intelligence support element? Does the senior geospatial intelligence cell NCO hold an MI or engineer MOS? Our NCOs tell us that the current BCT organizational structure does not make it easy for them to train Soldiers.

NCOs also shared that they believed they did not have to concentrate on being, or even seek to become, the unit’s primary trainer because of their (self-admitted) overreliance on high-quality external training resources available from functional training, Foundry, and U.S. Army Forces Command. Why try to do something someone else is able to provide?

The Army’s Principles of Training

- ◆ Train as you fight.
- ◆ Train to standard.
- ◆ Train to sustain.
- ◆ Train to maintain.⁷

Want to Learn a New Word? *Misophonia*

misophonia: a condition in which one or more common sounds (such as the ticking of a clock, the hum of a fluorescent light, or the chewing or breathing of another person) cause an atypical emotional response (such as disgust, distress, panic, or anger) in the affected person hearing the sound.⁸

Tactical and Technical Proficiency Shifts

The NCO hallmark of tactical and technical proficiency has shifted to—

- ◆ Company grade commissioned officers as the tactical experts.
- ◆ Warrant officers as the technical experts.

Combined Arms Maneuver Tactical Proficiency. This NCO challenge may result from an unintended consequence of a best practice. We have watched the improvement in MI commissioned officer training and proficiency in combined arms maneuver as the institution emphasized large-scale ground combat operations.

Over the past several years, the Army revised its training in large-scale ground combat operations for MI enlisted, lieutenants, and captains to provide multiple iterations of practical exercises, producing competent and confident

graduates. We have observed, and NCOs have shared, the problems NCOs face in achieving the same degree of currency and proficiency as their officer and junior Soldiers in conducting intelligence task performance for large-scale ground combat operations. Too often, we have seen MI captains, instead of NCOs, leading teams in building intelligence preparation of the battlefield (IPB) products used in the tactical-level military decision-making process and targeting. I'll describe the impact of this condition later, but first I want to emphasize that every MI NCO we have encountered does not willingly accept the status quo. The overwhelming response is clearly stated. As an MI company staff sergeant confided to us, **"I've failed as an NCO when an officer has to do my job."**

MI Technical Proficiency. MI warrant officers step in to fill the role as the technical experts. Often, this includes performing as the intelligence discipline primary trainer, thereby abandoning the expectation of warrant officers to advise, oversee, and guide NCOs in delivering training. Some warrant officers revealed it is sometimes difficult to avoid reverting to NCO functions when operating under time-compressed deployment schedules. Both warrant officers and NCOs occasionally state the self-fulfilling prophecy of NCOs not having enough time to become proficient in training their subordinates. Yet, NCOs also report they avoid attending Soldier training sessions to prevent exposing their lack of familiarity with intelligence support to combined arms maneuver tasks.

security. Their confidence stems from familiarity and experience gained through multiple combat deployments. NCOs are proficient in information collection for wide area security, targeting, intelligence architectures, and combined operations, as well as simultaneously operating in multiple domains. However, they recognize a disparity in knowledge of, or performance in, near-peer threat order of battle factors.

When NCOs attended institutional AIT, they recall focusing on the most probable and lethal area of operations that did not involve any near-peer threat forces—Iraq and Afghanistan. When, or even if, combined arms maneuver factors were trained to current NCOs during their AIT more than a few years ago, many NCOs do not recall several aspects of that training. For example, the importance of vehicle identification; aggregating and disaggregating of enemy tactical formations; combined arms maneuver tactics, terminology, and indicators; organic information collection/reconnaissance and surveillance capabilities; or tactical intelligence and communications architectures. The NCOs we have encountered at Fort Irwin, California, reveal their surprise at the speed, distances, and lethality (number of simulated casualties) experienced during a National Training Center (NTC) rotation. Many state that the realistic training conditions at NTC are not (cannot be) replicated at home station training. The conditions in previous deployments are much different from the austere NTC tactical environment. They quickly notice the absence of infrastructure (such as

water, electricity, and facilities), readily available MI systems maintenance, sustainment of all types, and various types of contractor support.

Role of the MI NCO versus the Army NCO

The final challenge is that "NCOs conduct the daily operations of the Army."⁹ They are not going to sit around and do nothing while officers, warrant officers, and Soldiers attend to intelligence production tasks for combined arms maneuver. NCOs tell us that

if they are not employed in their respective intelligence discipline or team-leading roles, they will relegate themselves to performing generic NCO command post tasks. These may include ensuring electric power generators are fueled and operating seamlessly; ensuring physical, operations, and information security; coordinating Soldier welfare



U.S. Army photo

Leaders training leaders—every Soldier going through the 7th Army Noncommissioned Officer Academy's Basic Leaders Course training must work together in squads.

Reluctant to Admit a Lack of Expertise

NCOs report their knowledge of large-scale ground combat operations is surpassed by recent graduates of USAICoE institutional training, particularly privates to specialists, warrant officers, and second lieutenants to captains. NCOs are confident in performing intelligence tasks for wide area

considerations (latrines, sleeping areas, subsistence, etc.); and performing other useful but generic tasks. Completing generic tasks is important; however, an insightful sergeant first class said that officers who allow NCOs to be diverted from their critical intelligence roles “deny NCOs the opportunity to grow.” The short-term gain of officers and privates building IPB products to get through an NTC rotation has a long-term effect. At the Army Lessons Learned Forum in January 2020, several general officers discussed trends at the combat training centers. An unidentified general officer made a comment when addressing the number of NCO challenges that each of the combat training centers had reported. He said, “We may be neglecting the very foundation of our Army’s strength.”

Support the Backbone by Strengthening the Core

If you want to help heal an aching back, and avoid future backaches, strengthen your core. This is good advice from my physician’s assistant and gym rat (physical fitness advocate) colleagues. We can apply the same principle to strengthening the Army’s backbone. We can strengthen, and derive strength from, the core—in this case, the core leader competencies.

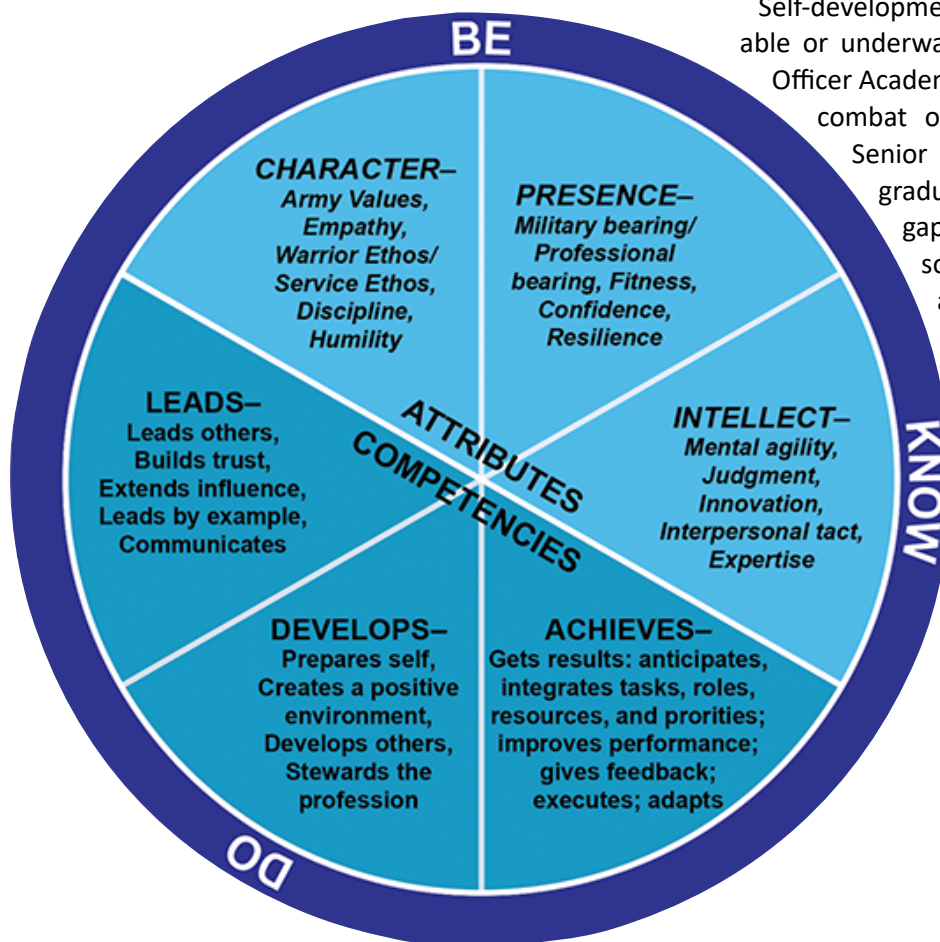
The most difficult yet immediately available solution is *self-development*. We have observed several MI NCOs at combat training center rotations or home station training exercises effectively and successfully lead teams of MI Soldiers in completing intelligence support to large-scale ground combat operations tasks. When asked how, or where, these NCOs had learned so much about large-scale ground combat operations’ combined arms maneuver, each one said it was intensive self-development—a desire to acquire the same level of knowledge and proficiency as their Soldiers in this area. Several NCOs sought guidance from their officers, from other NCOs, or from their own Soldiers. In each case, regardless of the source of instruction, the NCOs identified the importance of not being ashamed to tell their leaders they needed additional training or mentoring.

There is no such thing as tough. There is **trained and untrained**. Now which are you?

—John W. Creasy, portrayed by Denzel Washington in *Man on Fire*.¹¹

Self-development is not the only resolution strategy available or underway. The Fort Huachuca Noncommissioned Officer Academy is emphasizing more large-scale ground combat operations content in its Advanced and Senior Leader Courses. Over time, as students graduate from these courses, the performance gap between enlisted, NCO, and officer personnel will narrow, reverting to a better alignment of knowledge and skills.

The USAICoE Lessons Learned Team is also seeking to increase its contacts and engagements with MI NCOs at combat training centers, at home station training, and throughout the operational environment to provide more rapid and direct feedback to those who train, develop training, and assess the training of NCOs. The USAICoE Lessons Learned Team is working with other elements involved in NCO training at the U.S. Army Training and Doctrine Command, U.S. Army Forces Command, U.S. Army Intelligence and Security Command, and U.S. Army Cyber Center of Excellence to contribute to NCO leader development. Collaboration involves sharing observations, best practices, and the



The Army leadership requirements model¹⁰

commitment to focusing on NCO topics during at least one of the three monthly MI Lessons Learned Forum online sessions per calendar quarter.

Conclusion

The U.S. Army NCO Corps' education, experience, commitment, and competence are unmatched by any other nation's military force. We hope to assist our NCOs in resuming their positions as primary trainers. An NCO trained me to be a Soldier, an NCO, an officer, and an Army Civilian. Now, as a key member of the USAICoE Lessons Learned Team and MI Lessons Learned Forum, I have the opportunity to help repay my debt to the Army's backbone! 

Endnotes

1. Department of the Army, Training Circular (TC) 7-22.7, *The Noncommissioned Officer Guide* (Washington, DC: U.S. Government Publishing Office [GPO], 1 January 2020), foreword.

2. Ibid., v.

3. Ibid., 7-1–7-7.

4. Ibid., foreword.

5. Ibid., vi.

6. Department of the Army, Army Doctrine Publication 7-0, *Training* (Washington, DC: U.S. GPO, 31 July 2019), 3-1.

7. Ibid.

8. Merriam-Webster, s.v. "misophonia (n.)," accessed 14 October 2020, <https://www.merriam-webster.com/dictionary/misophonia>.

9. Department of the Army, TC 7-22.7, *Noncommissioned Officer Guide*, vi.

10. Ibid., 3-3.

11. *Man on Fire*, directed by Tony Scott (Los Angeles, CA: 20th Century Fox, 2004) (emphasis added).

Check out the MI Professional Bulletin website at <https://www.ikn.army.mil/apps/MIPBW>.



To access all of our issues back to 1974, click the archive tab.
A CAC is no longer required.

MI Professional Bulletin

Career Development: Navigating Your Way to a Productive Army Career

by Sergeant First Class Benjamin D. Waite and Sergeant First Class Samantha N. Walls

Introduction

If you are at the beginning of your career, or have been in the Army for a few years, consider the one piece of information you would love to have—a blueprint, maybe, on what steps to take along your career path. *If* you had access to a blueprint of what the Army expects from you, would you use it? The Army has endless opportunities for personal growth and professional achievement. There is just one catch—you must be willing to put in the time and effort and have the desire to achieve more than you ever thought possible.

This article will describe how you can become an expert in your discipline while planning for the next chapter in your Army career. You will learn that you can chart your very own path as you progress in rank, set your own personalized and professional goals, and achieve more by following some simple rules.

The Updated DA PAM 600-25

The Army has expectations for its Soldiers and noncommissioned officers (NCOs). As Soldiers climb the proverbial ladder of success, they must perform specific tasks at each rank for an increased potential for promotion, and these tasks are fundamental to the growth, knowledge, and experience for the next rank. Each task builds on the last and enables the transition from junior enlisted Soldier to NCO. This allows for a well-rounded individual, capable of leading the future force.

The primary publication governing this subject is DA PAM 600-25, *U.S. Army Noncommissioned Officer Professional Development Guide*, available through the Army Publishing Directorate website.¹ Additional chapters outlining each career management field's professional development opportunities are available at milSuite as a supplemental "smartbook." The military intelligence (MI) career management field is addressed in chapter 15, titled "Military Intelligence (Career Management Field 35) Career Progression Plan."² The chapter describes the major duties of each MI military occupational specialty (MOS) and the overarching goals for development, and it provides detailed guidelines pertaining to each skill level.

Educating the Force

Educating the force can be an intimidating task. This is especially true when educating the entire MI Corps on how to get the most out of a career. The Army has countless regulations, pamphlets, and publications that instruct us in all that a Soldier needs to know and do. However, the Army does not have much information on how to navigate your entire career by defining each step of the way. Soldiers and leaders must understand the importance of assignment diversity and its influence on creating a well-rounded Soldier. Leaders not using DA PAM 600-25 to counsel their Soldiers are overlooking a valuable resource to enhance career development in their Soldiers. The Department of the Army (DA) states, "Direct leaders develop others through coaching, counseling, mentoring, and setting the example."³ Many of you reading this article are the direct line leader! How are you giving sound guidance and counsel without using the proper resources designed to facilitate career enhancement? Simply stated, the answer is, you are not.

We must consider this DA pamphlet a blueprint for career development, a guide for counseling, and a resource for knowledge. This DA pamphlet covers each career management field within the Army. Furthermore, it enables non-MI leaders to understand what the MI Soldier's career looks like. As members of the MI Corps, we are responsible for educating our subordinates *and* our non-MI senior leaders on what we bring to the fight. Leaders at all levels need to understand that each Soldier has a different definition of success, and each will take a different path to achieve their goal.

Impacts to the Force and Improving the Force

When embarking on a journey, understanding the overall direction is important, but knowing when and where to turn is essential. Your career is no different. Understanding *what* the expectations are is important, but understanding *why* they are important often results in Soldier buy-in. A Soldier with buy-in is a Soldier who is committed. With a career path established, Soldiers can focus more on ways to improve. This includes seeking out educational opportunities,

being successful at demanding jobs, and attending the necessary schools to enhance MOS Soldier skills. Educating the force is important, and so too is the proper employment of MI Soldiers. Employing Soldiers within their means, which also includes outside their comfort zone, will improve the force. No Soldier can be stagnant throughout a career and hope to make it to the senior enlisted ranks. As Soldiers, we must engage our leadership, branch managers, and career managers to seek guidance. That is why we are here—to help you make the most out of your time in the Army. When our MI Soldiers understand and follow the blueprint for career development, our MI Corps is a more competent and combat-ready force.

Talent Management

Talent management is a self-driven initiative that requires a commitment to the demanding opportunities the Army offers. This is not to say talent management is solely an individual responsibility; leaders across the force must properly manage talent to employ their Soldiers most effectively. Used properly, talent management can improve readiness and combat effectiveness, empower Soldiers, positively influence unit performance, and improve organizational ability. The Army places a high demand on position within the force, and it is imperative that leaders manage their subordinates accordingly. At its core, talent management is about knowing your Soldiers and understanding your organization's mission. If MI leaders are unable to manage talent properly, we will lose that talent to the civilian sector.

Talent management is impossible without the understanding, and incorporation, of knowledge, skills, and behaviors. Knowledge represents experience, mental awareness, and education. Skills are those abilities individual Soldiers have learned from various training opportunities, including prior military, and from other situational experiences. Environmental factors drive behaviors. These factors include cultural experiences, workplace policies, and societal norms. Combining these three factors makes up a Soldier's talent, and knowing how to mold and employ a Soldier is management. Leaders must always remember that the people who make up the force are the Army's greatest asset. By investing in our people, the Army can better develop and employ the force to engage in combat operations around the globe.

Key Leadership, Key Developmental, and Broadening

DA PAM 600-25 clearly defines key leadership, key developmental, and broadening assignments as well as the duties associated with each rank. The MI chapter of the DA PAM 600-25 smartbook states the following:

Key Leadership—Duty positions that consist of traditional and staff leadership positions.

Key Developmental—Operational MOS positions that are required to develop critical technical skills and experience that provide the greatest potential for advancement.

Broadening assignments—Operational or institutional positions in a command or agency where duties can be outside of one's MOS or [career management field] CMF. These assignments offer a purposeful expansion of an NCO's leadership, resulting in agile and adaptive leaders capable of operating in complex environments. Mostly, these assignments are MOS-immaterial and challenge the NCO to increase their knowledge of Army policy and programs, increase skills beyond their CMF by performing the required duties of the assignment, and encourage growth.⁶

Linkage to Concepts and Strategies

Talent management is an implicit component of the ways and means required to support the Army's strategic priorities and an integral part of several key concepts and strategies.⁴ *The Army Strategic Planning Guidance* establishes strategic priorities for the Army Total Force. The first priority is **"Adaptive Army Leaders for a Complex World"** and identifies the required [knowledge, skills, and behaviors] KSBs as "morals, ethics, individual toughness, fighting spirit, intellectual capacity, tactical competence, technical proficiency, and strategic perspective."⁵

Key leadership includes, but is not limited to, team leader, squadron leader, platoon sergeant, and detachment sergeant. These positions are critical in pursuing self-development and aiding the development of subordinates. Key developmental includes, but is not limited to,

Security Force Assistance Brigade, division/corps analysis and control element, or special mission unit. These developmental assignments enable a more challenging workload within a specific MOS. Broadening assignments include, but are not limited to, drill sergeant, recruiter, instructor, and NCO Academy small group leader. It is important that a Soldier be able to step outside his or her specialty and give back to the Army. Volunteering for and being successful in those distinct and demanding assignments will set you apart from your peers. Those assignments are within the three training domains, which will develop the Soldier's training, experience, and education.

Training Domains

The Army has three training domains: operational, institutional, and self-development. Soldier and leader progression

is continuously built upon over the life of a career. Soldiers use the training, education, and experience that they gain through key leadership, key developmental, and broadening assignments to continuously develop themselves in each domain. Through counseling, Army leaders assist their subordinates in prioritizing and balancing their training, experience, and education components. That is why it is imperative for the leader to understand DA PAM 600-25 and how it assists in the counseling process.

Counseling

Regulatory guidance dictates leaders must counsel their Soldiers. This counseling should take place in an environment free from distraction. Whether done with a pen and paper or by digital means, counseling plays a vital role in the development and growth of Soldiers. As stated previously, DA PAM 600-25 serves as a blueprint for leaders conducting professional growth counseling of subordinates of any MOS. The DA pamphlet is a tool to help Soldiers and leaders identify relevant short- and long-term goals that will set them up for success. It outlines the major duties and goals for development for each MOS, and it informs Soldiers which key leadership, key developmental, and broadening assignments they need for each skill level. Additionally, it describes which military training Soldiers require in order to be competitive within their MOS. DA PAM 600-25 also informs Soldiers what they need in terms of self-development. In theory, if the leader follows the guide path in DA PAM 600-25 when conducting professional growth counseling, the subordinate will be successful.

In addition to DA PAM 600-25, another tool is available to assist in the counseling process—the Individual Development Plan (IDP), located on the Army Career Tracker (ACT) website. As a digital tool, the ACT website allows Soldiers and leaders to identify and set goals. This IDP allows Soldiers to view their career map and select a leader(s) and mentor(s) to help guide them in future planning. Consider the IDP a digital version of the DA pamphlet with interactive features Soldiers and leaders can modify as needed to create a focused career plan.

Conclusion

This article provided a baseline understanding of DA PAM 600-25, which offers MI Soldiers and leaders a better understanding of each MI discipline. It emphasized the importance of educating the force and the subsequent impacts on the force. The DA pamphlet, the ACT website, and IDP serve as a blueprint and a resource for career navigation to both MI Soldiers and non-MI leaders. Having knowledge of key leadership, key developmental, and broadening assignments enables Soldiers to seek more diversity, which helps create a well-rounded leader. It is critical that Soldiers understand whom to contact when questions arise concerning career development and assignment selection. Lastly, this DA pamphlet provides leaders a tool for counseling subordinates and educating leaders. An educated leader creates an educated force. 

Endnotes

1. Department of the Army, Department of the Army Pamphlet (DA PAM) 600-25, *U.S. Army Noncommissioned Officer Professional Development Guide* (Washington, DC: U.S. Government Publishing Office [GPO], 11 December 2018), <https://armypubs.army.mil/>.
2. Department of the Army, “Military Intelligence (Career Management Field 35) Career Progression Plan,” chap. 15 at Smartbook DA PAM 600-25, *The Noncommissioned Officer Professional Development Guide* (Washington, DC, 18 August 2020), <https://www.milsuite.mil/book/groups/smartbook-da-pam-600-25>.
3. Department of the Army, Army Doctrine Publication 6-22, *Army Leadership and the Profession* (Washington, DC: U.S. GPO, 31 July 2019), 1-23. Change 1 was issued on 25 November 2019.
4. Department of the Army, Training and Doctrine Command (TRADOC), *Talent Management Concept of Operations for Force 2025 and Beyond* (Fort Leavenworth, KS: TRADOC, September 2015), 33.
5. Department of the Army, *2014 Army Strategic Planning Guidance* (Washington, DC: 2014), 18.
6. Department of the Army, “Military Intelligence (Career Management Field 35) Career Progression Plan,” 8, <https://www.milsuite.mil/book/groups/smartbook-da-pam-600-25>.

SFC Benjamin Waite currently serves as an instructor at the Counterintelligence Special Agent Course (military occupational specialty [MOS] 35L). His previous assignment was as a career manager for MOS 35L with the Office of the Chief, Military Intelligence (OCMI), U.S. Army Intelligence Center of Excellence (USAICoE). Previously, he was the detachment sergeant at 297th Military Intelligence (MI) Battalion.

SFC Samantha Walls serves as a career manager for MOS 35G (Geospatial Intelligence Imagery Analyst) with OCMI, USAICoE. She earned her associate degree in 2014. SFC Walls has served both as a basic combat training drill sergeant with the 165th Infantry Brigade at Fort Jackson, SC, and as an instructor in the 35G10 Course in the 111th MI Brigade at Fort Huachuca, AZ.



MILITARY INTELLIGENCE CORPS HALL OF FAME INDUCTEES – 2020



To ensure the health and safety of all participants, the 2020 Hall of Fame induction ceremony has been postponed until June 2021. For more information about the Hall of Fame, visit: <https://www.ikn.army.mil/apps/MIHOF/Home>, or contact the Command Historian at usarmy.huachuca.icoe.mbx.command-historian@mail.mil.

Colonel Jasey B. Briley, U.S. Army, Retired

Jasey Brando Briley entered the U.S. Army as a Reserve Officer Training Corps (ROTC) cadet at Virginia State University. After graduating with honors (cum laude) as a distinguished military graduate, he became the first cadet at that university to commission in the Military Intelligence (MI) Branch.

After commissioning, COL Briley was assigned to the 525th MI Brigade at Fort Bragg, North Carolina, where he served as platoon leader, company executive officer, detachment commander, and corps G-2 emergency deployment readiness officer. In August 1985, he transferred to Korea to serve as the southern area counterintelligence officer and battalion S-3, 524th MI Battalion, 501st MI Brigade. Two years later, he transferred to Fort Meade, Maryland, as group training officer and company commander in the 902nd MI Group.

In March 1990, COL Briley returned to Korea as a company commander and battalion S-3 in the 102nd MI Battalion, 2nd Infantry Division. Returning to Fort Bragg, he was assigned as operations officer on the G-2 staff of the XVIII Airborne Corps and then as 2nd Brigade S-2 in the 82nd Airborne Division. In June 1994, he was assigned as operations officer of the ROTC Command at Fort Bragg before becoming executive officer of the 519th MI Battalion, 525th MI Brigade.

Next, COL Briley was selected to serve for 2 years on the White House military staff as a program manager and then assumed command of the 310th MI Battalion at Fort Meade in June 1999. Following his battalion command, he was selected as G-2, 10th Mountain Division, Fort Drum, New York. While in this position, he deployed to Kosovo in support of Operation Joint Guardian and then went directly to Afghanistan following the terrorist attack of September 11th, where he served as the first senior intelligence officer on the ground as the J-2 for Joint Task Force Mountain in support of Operation Enduring Freedom/Anaconda. Upon graduating from the National War College, he was assigned as executive officer to the Army G-2 at Headquarters, Department of the Army, Pentagon. Then, after serving as the U.S. Army Intelligence and Security Command's assistant chief of staff for operations, COL Briley assumed brigade-level command of the Joint Field Support Center, Defense Intelligence Agency. In 2007, he moved to Fort Huachuca, Arizona, as



Chief of Staff of the U.S. Army Intelligence Center. His final assignment was the G-2 of XVIII Airborne Corps, during which he deployed to Haiti in support of Operation Unified Response and to Iraq as deputy J-2, Combined Forces Iraq, in support of Operation New Dawn.

COL Briley retired from active duty on 31 May 2012 after 31 years of dedicated service. His awards and decorations include the Distinguished Service Medal, Defense Superior Service Medal, Legion of Merit (two Oak Leaf Clusters), Bronze Star Medal (one Oak Leaf Cluster), Defense Meritorious Service Medal (one Oak Leaf Cluster), Meritorious Service Medal (four Oak Leaf Clusters), Army Commendation Medal (one Oak Leaf Cluster), and Army Achievement Medal (two Oak Leaf Clusters), as well as numerous campaign and service ribbons, and the Presidential Service, Army Staff, Senior Parachutist, and German Airborne badges. COL Briley was also awarded the MI Corps Association's Knowlton Award in 2001. In 2017, he was inducted into the Virginia State University Hall of Fame. 

2020

MILITARY INTELLIGENCE CORPS
HALL OF FAME
INDUCTEES

**2020**

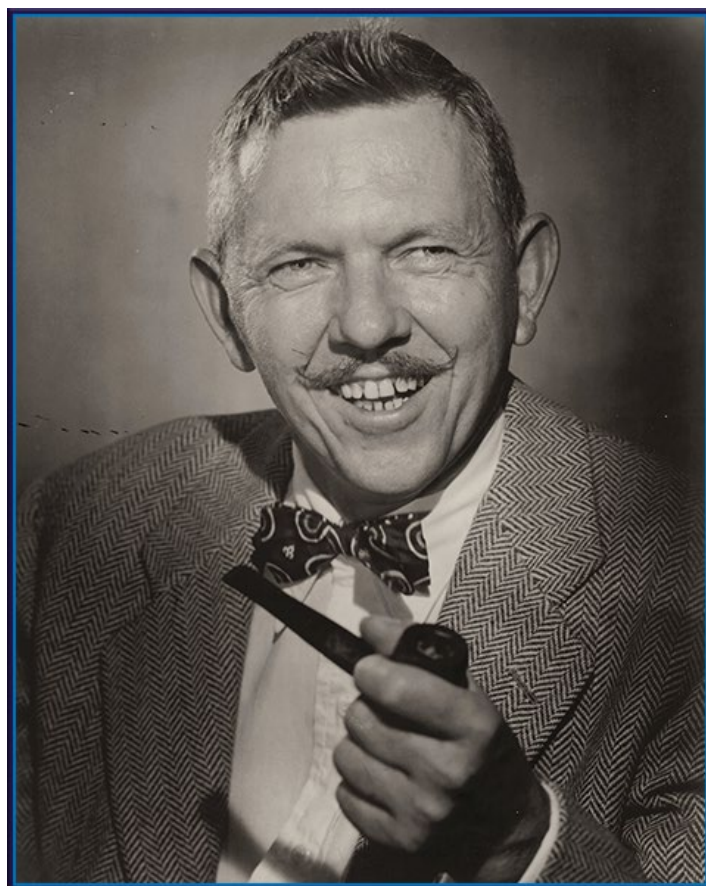
Lieutenant Colonel Jack B. Cameron, U.S. Army, Retired (Deceased)

Jack Cameron entered the U.S. Army in 1933, and after a short time with the 12th Field Artillery, he transferred to the G-2 section of the 8th Corps Area. By the late 1930s, he had been accepted into the Corps of Intelligence Police, the U.S. Army's first counterintelligence (CI) organization, with service at Fort Sam Houston, Texas. In 1939, he was assigned as the first CI agent in Puerto Rico, where he had to develop his own standard operating procedures.

In 1942, MSG Cameron attended the first and only Military Intelligence Officers Candidate School in Chicago and received a commission as a second lieutenant. After an assignment at First Army Headquarters in Boston, he served as the Counter Intelligence Corps (CIC) Detachment Commander for the 3rd Infantry Division. On 7 November 1942, he took part in Operation Torch, the largest amphibious assault in history up to that time and the first tactical deployment of Army CI agents. Landing at Fedala, French Morocco, Cameron and his detachment helped secure the town of Casablanca, located German military personnel and sympathizers, and exploited captured document caches. He received a Legion of Merit for his efforts in Morocco. Moving with the frontline troops of the 3rd Infantry, he conducted similar operations after an amphibious landing at Licata, Sicily, and during successive operations in Agrigento and Palermo. After the invasion of the Italian peninsula, on 9 September 1943, Cameron took command of the CIC Detachment for southern Italy. By 1945, he was assigned to the 11th Armored Division as Chief of CI operations for occupied Austria, with headquarters at Innsbruck. There, his primary responsibility was to identify and locate Nazis wanted by the Nuremberg Tribunal.

By 1946, LTC Cameron had returned to the United States and left the Army. Two years later, however, he returned to active duty and was assigned to CIC Headquarters at Fort Holabird, Maryland, as Chief of Operations and Training. While there, he wrote a manual on CI detachment operations based on his World War II experiences.

On 16 January 1951, Cameron established and took command of the 450th CIC Detachment, Supreme Headquarters



Allied Powers Europe, in Paris, France. This was the first CIC detachment to be assigned to an international headquarters. He served as the CI advisor to GEN Dwight D. Eisenhower, established relationships with intelligence leaders from other North Atlantic Treaty Organization countries, and assisted in the neutralization of hostile Soviet activities directed against the alliance.

After 4 years with the 450th, in 1955, LTC Cameron transferred to Sixth Army Headquarters at the Presidio in San Francisco, California, as Chief of the Counter Intelligence Division. The following year, he retired from the U.S. Army after 20 years of service. LTC Cameron passed away on 6 January 1979.



The final test of a leader is that he leaves behind him in other men the conviction and the will to carry on.

—Walter Lippmann, American writer, reporter, and political commentator

2020

MILITARY
HALL OF FAME
INDUCTEES

**2020**

Chief Warrant Officer 5 Joe D. Okabayashi, U.S. Army, Retired

Joe Okabayashi enlisted in the U.S. Army in 1977. In 1986, SFC Okabayashi was appointed directly to the rank of chief warrant officer 2 as an all-source intelligence technician.

CW5 Okabayashi's warrant officer career began with two 4-year assignments as an order of battle technician with the 303rd Military Intelligence (MI) Battalion at Fort Hood, Texas, separated by a 1-year tour with the 2nd Infantry Division in Korea from 1990 to 1991. During his time at Fort Hood, he assisted in developing and integrating the new Analysis and Control Element Target Development Branch within III Corps to provide intelligence support to corps fires and corps deep-attack operations. He then spent nearly 3 years as the first Army warrant officer intelligence observer/controller with the U.S. Army Battle Command Training Program at Fort Leavenworth, Kansas.

In February 1997, he returned to Fort Hood, this time as an all-source intelligence technician with the 104th MI Battalion to participate in the Army's Division Advanced Warfighting Experiment. He next served as the National Target Base production supervisor for U.S. Strategic Command, Offutt Air Force Base, Nebraska, from 1999 to 2001. During this assignment, he provided key intelligence support to Operations Allied Force, Noble Anvil, and Skilled Anvil in the Balkans.

In February 2001, CW5 Okabayashi served a second year-long tour in the Republic of Korea as an all-source intelligence technician with the 102nd MI Battalion. Returning to the United States in January 2002, he was assigned as Chief of the Order of Battle Section, J-2, U.S. Central Command (CENTCOM) at MacDill Air Force Base, Florida. He spent 3 years at CENTCOM during the challenging early years of the Global War on Terrorism. He then brought his valuable operational experience and skills to the U.S. Army Intelligence Center as Chief of the Warrant Officer Training Branch in the 304th MI Battalion.

After 4 years focused on revitalizing the training and education of MI's Warrant Officer Corps, CW5 Okabayashi deployed for 1 year to Kabul, Afghanistan, as the senior in-



telligence analyst for the International Security Assistance Force Joint Command. He then returned to the U.S. Army Intelligence Center for his final assignment as Chief Warrant Officer of the MI Corps.

CW5 Okabayashi retired on 31 October 2015 after 38 years of service. His military awards include the Legion of Merit, Defense Meritorious Service Medal (two Oak Leaf Clusters), Meritorious Service Medal (six Oak Leaf Clusters), Joint Service Commendation Medal, Army Commendation Medal (five Oak Leaf Clusters), Army Achievement Medal (two Oak Leaf Clusters), and numerous other service ribbons. He was twice awarded the MI Corps Association's Knowlton Award in 1997 and 1998. 

The greatest leader is not necessarily the one who does the greatest things. He is the one that gets the people to do the greatest things.

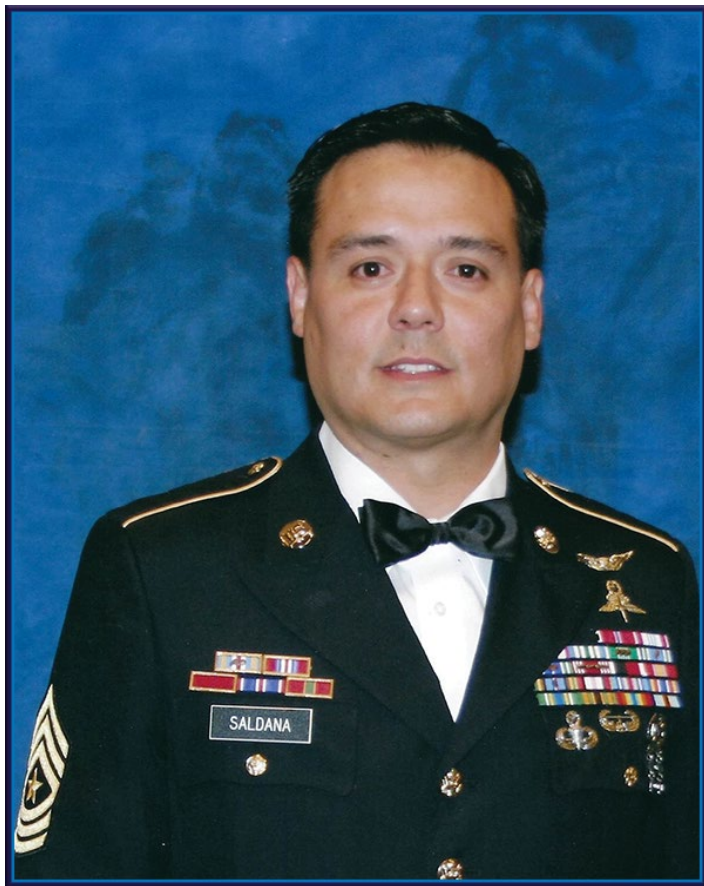
—Ronald Reagan, 40th President of the United States, and former Captain in the Army Reserves

2020**MILITARY INTELLIGENCE CORPS
HALL OF FAME
INDUCTEES****2020****Sergeant Major Jorge A. Saldana, Sr., U.S. Army, Retired**

Jorge Saldana entered the U.S. Army Reserves in May 1980 as a light wheel vehicle and power generator mechanic. In October 1982, he reclassified to a military occupational specialty 92Y (unit supply specialist) and was assigned to Field Station Berlin for the U.S. Army Intelligence and Security Command. In 1986, he reclassified again to military intelligence (MI) as a signals intelligence analyst and Spanish linguist.

SGM Saldana's first MI assignment was as a team leader for a low-level voice intercept team in Alpha Company, 313th MI Battalion, 82nd Airborne Division, Fort Bragg, North Carolina. Later assignments included Charlie Company, 3rd Battalion, 7th Special Forces Group (Airborne), Fort Davis, Panama; U.S. Army Military District of Washington Special Mission Unit (SMU) in Washington, DC; Bravo Company, 344th MI Battalion, Goodfellow Air Force Base, San Angelo, Texas; Headquarters and Headquarters Company, 501st MI Brigade, Seoul, Korea; and U.S. Central Command, MacDill Air Force Base, Florida.

In October 2001, SGM Saldana returned to the Military District of Washington SMU, to which he was assigned until November 2012. During his multiple assignments with the SMU, he served as an operator, team sergeant, operations troop sergeant, squadron S-3 sergeant major, and SMU mission commander (forward). From 2009 to 2012, he served as the SMU recruiting troop sergeant major and was instrumental in the recruitment of select personnel for extremely specific and challenging requirements. SGM Saldana served seven combat tours in Afghanistan while attached to Red Squadron, SEAL Team Six; one tour in Panama; and multiple tours to other high-danger locations, providing intelligence support to the missions of the Joint Special Operations Command and U.S. Special Operations Command. He is the only MI noncommissioned officer to have conducted a military freefall, high-altitude, low-opening (HALO) combat jump at over 25,000 feet over Afghanistan.



SGM Saldana retired from the U.S. Army on 1 November 2012 after 32 years of service. His military awards include the Legion of Merit, Bronze Star, Military Free Fall Jump Master Badge with Bronze Service Star (Combat HALO Jump, Afghanistan), Defense Meritorious Service Medal (one Oak Leaf Cluster), Meritorious Service Medal, Joint Service Commendation Medal, Army Commendation Medal (one Oak Leaf Cluster), Joint Service Achievement Medal (two Oak Leaf Clusters), Army Achievement Medal (two Oak Leaf Clusters), various unit awards, and campaign and service ribbons, as well as the Aviation Crewmember, Master Parachutist, and Air Assault badges. 

It doesn't take a hero to order men into battle. It takes a hero to be one of those men who goes into battle.
—GEN Norman Schwarzkopf, U.S. Army

2020**MILITARY INTELLIGENCE CORPS
HALL OF FAME
INDUCTEES****2020****Ms. Lynn Schnurr, Defense Intelligence Senior Executive Service-2, Retired**

Lynn Schnurr graduated from Virginia Tech in 1975 and held positions within the government and as a congressional staff member before beginning her career in Army intelligence as a computer scientist intern at the U.S. Army Intelligence and Security Command (INSCOM), Arlington Hall Station, Virginia, in 1981. She was assigned to INSCOM and began her 3-year internship attending computer science and industry-based college courses coupled with on-the-job training. This training and experience set the stage for her 34-year career, in which she focused on applying technology to the Army intelligence mission set, fielding many new capabilities ranging from the command database at INSCOM to rapid wartime technology solutions in communications, data, infrastructure, open-source intelligence, and biometrics. Ms. Schnurr was a leader in providing innovative solutions rapidly to the warfighter and for the Army intelligence enterprise. Many innovations were used across the Department of Defense (DoD) and the intelligence community.

In 1995, Ms. Schnurr moved to the Pentagon after 14 years at INSCOM to serve as the Deputy Director for Information Management. In 1999, she entered the Senior Executive Service as the Director of Information Management, Deputy Chief of Staff, G-2, and served as the Army Intelligence Chief Information Officer (CIO). During this time, Ms. Schnurr programmed, designed, developed, and implemented the Land Intelligence, Surveillance, and Reconnaissance Network, ensuring the Army's intelligence mission was totally interoperable at all echelons and had connectivity to the DoD and intelligence community enterprises. She led the Joint Intelligence Operations Capability (JIOC) in Afghanistan and Iraq to rapidly improve the synchronization and sharing of operational and intelligence data for Operations Iraqi Freedom and Enduring Freedom. Ms. Schnurr briefed the Deputy Secretary of Defense, received funding, and rapidly fielded JIOC in 5 months.

Ms. Schnurr served as a member of the Army CIO Board, Intelligence Community CIO Council, DoD Intelligence Information System Executive Council, Defense Intelligence Information Enterprise Council, Joint Information Enterprise DoD Board, Document and Media Exploitation Executive Committee, and Army and DoD-level biometrics councils and fora. She also created the first DoD-level Data Council and Open-Source Intelligence and Data Symposia recog-



nized throughout the DoD and intelligence community. Ms. Schnurr traveled to combat zones in Iraq and Afghanistan frequently to gain a clear understanding of information technology and mission requirements. She ensured higher headquarters approvals for resourcing, information assurance, and fielding direct to the Army and other Services, particularly on tactical communications, biometrics, data management, cloud solutions, JIOC, and open-source intelligence.

Ms. Schnurr retired as a Defense Intelligence Senior Executive Service Tier 2 on 3 January 2013. Her awards include the Presidential Rank Award for Distinguished Senior Level Professionals, National Intelligence Distinguished Service Medal, Department of the Army Exceptional Service Medal, National Geospatial Intelligence Agency Medallion for Excellence In Duty, Secretary of the Army Decoration for Exceptional Performance of Duty award, and an Army Chief of Staff Letter of Commendation for Extraordinary Contributions. Ms. Schnurr is also a Knowlton Award recipient. 

2020**MILITARY INTELLIGENCE CORPS
HALL OF FAME
INDUCTEES****2020****Distinguished Civilian of the Military Intelligence Corps**

In 2020, the Chief of the Military Intelligence (MI) Corps filled a position that has been vacant since the passing of the esteemed Mrs. Dorothe K. Matlack in 1991. The Distinguished Civilian of the MI Corps, like our Honorary Colonel, Honorary Sergeant Major, Honorary Chief Warrant Officer, and other Distinguished Members of the MI Corps, provides a link with history for today's Soldiers and leaders. They not only help us perpetuate the traditions of the Corps and enhance morale and esprit, but they can also provide mentorship and advice and represent the MI Corps at ceremonies and other events. If you would like to contact any of our Distinguished Members, please send an email to usarmy.huachuca.icoe.mbx.command-historian@mail.mil.

Ms. Claudia S. Gaul, Defense Intelligence Senior Level/Tier 1, Retired

Claudia Gaul began her career as an intern at the U.S. Army Intelligence and Security Command's Security Office at Arlington Hall Station, Virginia, in 1980. In 1985, she was detailed to the Office of the Assistant Chief of Staff for Intelligence, Department of the Army (now the Office of the Deputy Chief of Staff, G-2 (ODCS, G-2)) to serve as Advisor to the Director of the Army Staff in his role as a member of the Stilwell Commission, which examined Department of Defense security policies and practices. Ms. Gaul was then hired into a security specialist position in the ODCS, G-2 where she remained for the rest of her career except for a yearlong assignment at the Army Materiel Command in the Special Access Programs Division. When Ms. Gaul returned to the ODCS, G-2 in 1988, she served as a counterintelligence specialist until 1991 when she was selected to serve as the Counterintelligence Division Chief.

After 4 years as the Counterintelligence Division Chief, Ms. Gaul completed a 6-month developmental assignment as Executive Assistant to the Assistant DCS, G-2 from January to June 1995. She was then assigned as the Intelligence Production Functional Manager. In November 1996, she became the Integration Division Chief, a position she held until June 2001. At that time, she moved into the position of Deputy Director of Operations and Plans where she assisted in the ODCS, G-2's support to the Global War on Terrorism. In November 2008, Ms. Gaul was selected for Defense Intelligence Senior Level service (Tier 1, a brigadier general equivalent). Her final assignment, beginning in January 2015, was as Special Advisor in the Plans and Integration Directorate. Ms. Gaul retired from this position on 3 January 2020, culminating nearly 40 years of service as a Department of the Army Civilian (DAC).

Over the last two decades, she became a driving force for supporting worldwide Army intelligence operations and future intelligence planning. In 2009, she coordinated intelligence support to the surge in Afghanistan, pushing to ensure warfighters had the personnel, equipment, and capabilities to support force protection and combat operations. In 2014, she contributed to the G-2's Vision for Intelligence 2020, resulting in better structured military intelligence capabilities and capacities to support a regionally focused, globally engaged Army.



Among other accomplishments, Ms. Gaul directed the development, coordination, and approval of Army intelligence policy as it affected intelligence collection, foreign languages, training, readiness, cyberspace, and weather support. Recognizing future challenges, she supported the transformation from a counterinsurgency-focused intelligence posture to large-scale combat operations against a near-peer opponent.

Throughout her career, Ms. Gaul was widely respected for her knowledge of Career Program 35, the Defense Civilian Intelligence Personnel System, and all facets of civilian service within military intelligence. Her succession of positions in the ODCS, G-2 gave her insight into all the Army intelligence disciplines and the challenges, opportunities, and unique aspects of DAC intelligence service.

Ms. Gaul's awards and honors include the Presidential Rank Award (Meritorious), Intelligence Community Seal Medallion, Army Superior Civilian Service Award, and Achievement Medal for Civilian Service. 

2020**MILITARY INTELLIGENCE CORPS
HALL OF FAME
INDUCTEES****2020****Honorary Member of the Military Intelligence Corps**

Honorary Members of the Corps are officers, warrant officers, Soldiers, Civilians, spouses, or other individuals, either active or retired, who have made a significant contribution or provided a service to the Military Intelligence (MI) Corps, but who are not otherwise qualified to be members of the MI Corps.

Ms. Clarine Moorman, Department of Army Civilian (Deceased)

Clarine Moorman's career spanned more than 25 years as a human resources specialist and assignment manager at the U.S. Army Personnel Command in Alexandria, Virginia, and the U.S. Army Human Resources Command (HRC) at Fort Knox, Kentucky. For the majority of her career, she was assigned to HRC's Operations Support Division of the Officer Personnel Management Directorate. There, she was responsible for the assignment and management of military intelligence (MI) officers entering the active duty Army as well as developing and improving the effectiveness of work methods and procedures related to the organization and manpower utilization. On an annual basis, she prepared hundreds of MI Branch files for promotion boards, analyzed board results, and registered hundreds of MI officers for Intermediate Level Education to meet Army educational timelines. She was also integral in formalizing, publicizing, and coordinating the annual selection panel for MI programs, including the Junior Officer Cryptologic Career Program, Warrant Officer Cryptologic Career Program, and Army Intelligence Development Programs.

Promoted to Chief of Operations for the Operations Support Division, she was responsible for administering technical guidance and policy interpretation, as well as managing multiple division-level programs, including the HRC Identity Management System, the Applied Suicide Intervention Skills Training, and the Information Assurance Security Officer. She also expertly managed the processing of a variety of nuanced personnel actions, including retirements, unqualified resignations, advanced civil schooling applications, and by-name nominations for the Army and joint staffs for officers of all ranks.



Through her unwavering enthusiasm and dedication, Ms. Moorman positively impacted thousands of military and civilian personnel across the MI Corps, from the most senior intelligence officers to the newly accessioned lieutenant. She passed away unexpectedly on 29 January 2015, but her legacy of mentorship, guidance, and joy continues to resonate in MI Branch at HRC and throughout the MI Corps. 

Heroism doesn't always happen in a burst of glory. Sometimes small triumphs and large hearts change the course of history.

—Mary Roach, American Author



Contact and Article Submission Information



This is your professional bulletin. We need your support by writing and submitting articles for publication.

When writing an article, select a topic relevant to Army MI professionals.

Our goals are to spark discussion and add to the professional knowledge of the MI Corps and the intelligence community. Articles about current operations, TTPs, and equipment and training are always welcome as are lessons learned, historical perspectives, problems and solutions, and short “quick tips” on better employment of equipment and personnel. Explain how your unit has broken new ground, give helpful advice on a specific topic, or discuss how new technology will change the way we operate.

When submitting articles to MIPB, please consider the following:

- ◆ Feature articles, in most cases, should be between 2,000 and 4,000 words, double-spaced with normal margins without embedded graphics.
- ◆ We cannot guarantee we will publish all submitted articles and it may take up to a year to publish some articles.
- ◆ Although MIPB targets quarterly themes, you do not need to write your article specifically to a theme. We publish non-theme articles in most issues.
- ◆ Please do not include any personally identifiable information (PII) in your article or biography.
- ◆ Please do not submit an article to MIPB while it is being considered for publication elsewhere; nor should articles be submitted to MIPB that have been previously published in another publication or that are already available on the internet.
- ◆ All submissions become property of MIPB and may be released to other government agencies or nonprofit organizations for reprint upon request.

What we need from you:

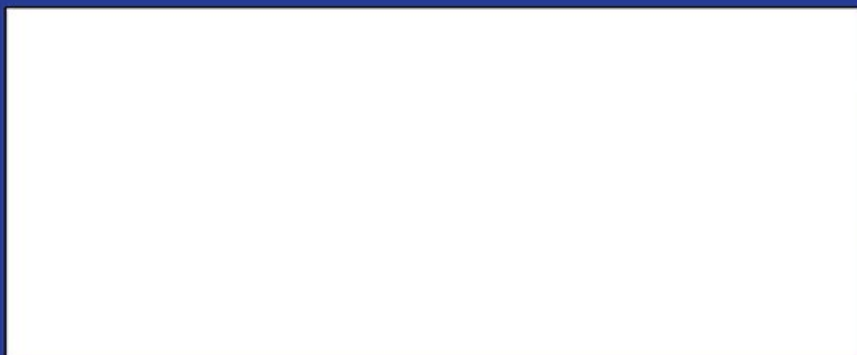
- ◆ Compliance with all of your unit/organization/agency and/or installation requirements regarding release of articles for professional journals. For example, many units/agencies require a release from the Public Affairs Office.

- ◆ A cover letter/email with your work or home email, telephone number, and a comment stating your desire to have your article published.
- ◆ **(Outside of USAICoE)** A release signed by your unit’s information security officer stating that your article and any accompanying graphics and photos are unclassified, not sensitive, and releasable in the public domain. A sample security release format can be accessed via our webpage on the public facing Intelligence Knowledge Network website at: <https://www.ikn.army.mil/apps/MIPBW>
- ◆ **(Within USAICoE)** Contact the Doctrine/MIPB staff (at 520-533-3297 or 520-533-1242) for information on how to get a security release approved for your article. A critical part of the process is providing all of the source material for the article to the information security reviewer in order to get approval of the release.
- ◆ Article in Microsoft Word; do not use special document templates.
- ◆ Pictures, graphics, crests, or logos relevant to your topic. Include complete captions (the 5 Ws), and photographer credits. Please do not send copyrighted images. **Do not embed graphics or photos within the article. Send them as separate files such as .tif or .jpg.** Photos must be at least 300 dpi. If relevant, note where graphics and photos should appear in the article. PowerPoint (**not in .tif/.jpg format**) is acceptable for graphs, figures, etc.
- ◆ The full name of each author in the byline and a short biography for each. Biographies should include authors’ current duty assignment, related assignments, relevant civilian education and degrees, and any other special qualifications.

We will edit the articles and put them in a style and format appropriate for MIPB. From time to time, we may contact you during the editing process to help us ensure a quality product. Please inform us of any changes in contact information.

Submit articles and graphics to usarmy.huachuca.icoe.mbx.mipb@mail.mil. For any questions, email us at the above address or call 520-533-7836/DSN 821-7836.

MIPB (ATZS-DST-B)
Dir. of Doctrine and Intel Sys Trng
USAICoE
550 Cibequa St.
Fort Huachuca, AZ 85613-7017



Headquarters, Department of the Army.
This publication is approved for public release.
Distribution unlimited.

PIN: 208441-000