

Military Intelligence Support to Army Special Operations



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 Robert P. Walters, Jr.

Chief of Staff

COL Douglas R. Woodall

Chief Warrant Officer, MI Corps

CW5 David J. Bassili

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 Emily R. Morrison

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:

MARK A. MILLEY
General, United States Army
Chief of Staff

Official:


KATHLEEN S. MILLER
Administrative Assistant
to the Secretary of the Army
1903507

From the Editor

The following themes and deadlines are established:

October-December 2019, *Intelligence Preparation of the Battlefield*. The intent of this issue is to take a holistic look at IPB and the input provided by all staff sections to conduct mission analysis. Deadline for article submission is 1 July 2019. **This is a change from the previously published theme for this quarter.**

January-March 2020, *Intelligence at Echelons Above Corps*. This issue will discuss aspects of intelligence support and operations at Echelons Above Corps. Deadline for article submission is 28 September 2019. **This is a change from the previously published theme for this quarter.**

April-June 2020, *Intelligence Analysis*. This issue will focus on the various aspects of intelligence analysis and their importance to operations. Deadline for article submission is 19 December 2019.

July-September 2020, *Collection Management*. This issue will focus on the how the intelligence staff executes the tasks of collection management in support of information collection. Deadline for article submission is 3 April 2020.

If you would like to receive a notification email when new MIPB issues become available on Intelligence Knowledge Network, send an email to us.army.huachuca.icoe.mbx.mipb@mail.mil requesting to be added to MIPB's announcement distribution list.

If you would like to receive a notification email when new intelligence doctrine is published, send an email to us.army.huachuca.icoe.mbx.doctrine@mail.mil requesting to be added to the new doctrine announcement list.

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.

We would like to express our sincere gratitude to COL Patrick Wempe, U.S. Army Special Operations Command (USASOC) G-2, who provided invaluable guidance as the "stakeholder" during the development of this issue. Additionally, we would like to thank Mr. James (Andy) Gordon, USASOC G-25/9, for his role as the day-to-day conduit to ensure the accuracy and quality of the issue. The enthusiasm and dedication of the USASOC G-2 team was instrumental in producing this highly informative issue.

FEATURES

- 6 Army Special Operations Intelligence: Capable and Ready**
by COL Patrick Wempe
- 11 Army Special Operations Forces Data Integration Initiative**
by Mr. William D. Goss and Mr. James A. Gordon
- 14 The 75th Ranger Regiment Military Intelligence Battalion: Modernizing for Multi-Domain Battle**
by MAJ Paul A. Lushenko
- 25 ATP 3-05.20, Special Operations Intelligence**
by CPT Brandon Bragg
- 29 An Excerpt from ADRP 3-05, Special Operations**
- 31 Countering Violent Extremist Organization High-Profile Attacks**
by 1LT Adria K. Penatzer
- 36 Reconnaissance Found: Redefining Army Special Operations Forces Integration**
by MAJ Orlando N. Craig, CPT William P. Hurt, CPT Albert W. Oh, and 1SG Christopher B. Melendez
- 43 Issues, Goals, Influence, Vulnerabilities, and Opportunities: Key Intelligence Considerations for Irregular Warfare**
by Mr. Marcus Canzoneri, Mr. Richard Oakley, and Mr. David Walther
- 51 Intelligence Support to Unconventional Warfare**
by LTC Thomas J. McCarthy (Retired)
- 58 Addressing Army Aviation Intelligence Training**
by CW3 Brandon R. Mesa
- 61 U.S. Army Special Operations Forces Military Intelligence Training Strategy**
by MSG Thad R. Heiges

- 65 Unstoppable Small Unmanned Aircraft Systems**
by CPT Sean D. Hayball, CPT Peter L. Kerkhof, and SFC Ryan K. Sarver
- 73 Preparing the Redesigned Company Intelligence Support Team for Decisive Action Employment**
by LTC Anthony Barbina, CPT Alex Reinwald, and CPT Michael Heim
- 78 4th Infantry Division Military Intelligence Training Strategy**
by LTC Thomas Spahr and CPT Michael Weiss
- 83 Brigade Combat Team Intelligence Transformation for High-Intensity Peer Conflict**
by CPT Kyle Hanratty
- 90 Sometimes, You Really Have to KNOW: The Peninsula Campaign of 1862**
by Mr. Donald W. Smith

DEPARTMENTS

- | | |
|--------------------------------|--|
| 2 Always Out Front | 96 USAICoE Lessons Learned |
| 4 CSM Forum | 99 Awards for Excellence in Military Intelligence |
| 5 Technical Perspective | 103 Moments in MI History |

Inside back cover: Contact and Article Submission Information

Always Out Front

by Major General Robert P. Walters, Jr.
Commanding General
U.S. Army Intelligence Center of Excellence



In the last issue of *Military Intelligence Professional Bulletin* (MIPB), the theme was the broad topic of intelligence support to large-scale combat operations, which is the Army's new focus area and most significant readiness requirement. In contrast, this issue of MIPB is very different. It highlights the missions of a single community—special operations—and the intelligence warfighting function's role within that community. Special operations recruits, trains, and re-sources their force based on a unique mission set and an incredibly challenging operational tempo.

During my career, I have had the privilege of serving with the special operations community for 12 years, as an intelligence officer for the Night Stalkers in Task Force 160, as the J-2 at the Joint Special Operations Command, and as the J-2 at the U.S. Special Operations Command. From this experience, I can attest to the primary theme that is reinforced across the special operations forces (SOF)-related articles in this issue of MIPB—while the intelligence warfighting function in SOF is unique, the fundamental intelligence principles are the same across all intelligence operations.

The Office of Strategic Services (OSS) developed the Special Operations branch after the 1941 attack on Pearl Harbor. Mirroring the British Special Operations Executive, OSS created the Special Operations branch to “‘effect physical subversion of the enemy,’ in three distinct phases: infiltration and preparation, sabotage and subversion, and direct support to guerrilla, resistance, or commando units.”¹ As the organization grew, special forces units deployed worldwide in support of conventional units, establishing coalitions and providing humanitarian assistance. The U.S. Army Special Operations Command (USASOC) currently comprises the—

- ◆ 1st Special Forces Command (Airborne).
- ◆ U.S. Army John F. Kennedy Special Warfare Center and School.
- ◆ U.S. Army Special Operations Aviation Command.
- ◆ 75th Ranger Regiment.

The history of Army special operations is vast, and members of the special forces community have a strong bond that unites them for life. Since the creation of SOF, every special operations mission has required competent intelli-


gence professionals who understand multiple intelligence disciplines. Intelligence professionals must also fully understand intelligence preparation of the battlefield and how to apply it to every operation. Becoming grounded in doctrine and understanding how it relates to every operation will make you successful in the SOF community.

Through the media and in the military, we have all heard stories of special operations missions. A famous, relatively recent vignette, in which intelligence played a crucial role, is the U.S. Navy Sea, Air, and Land Team (SEALs) raid on Osama bin Laden's Abbottabad compound in 2011. During this operation, decision makers evaluated several possible courses of action, including an airstrike and a raid. They determined that an airstrike in a populated city could result in foreign policy consequences, along with additional collateral damage, and possible failure to positively identify the target, and therefore chose to conduct a raid. Former U.S. Under Secretary of Defense for Intelligence Michael Vickers later explained that a raid gave the United States “greater strategic certainty.”² Once sufficient information had been collected and analyzed, the Navy SEALs' raid commenced—on order of the President of the United States, at the direction of the Director of the Central Intelligence Agency, and under the tactical command of then-VADM William McRaven (later ADM McRaven).

In this quarter's MIPB you will discover a myriad of articles that illustrate the intertwined nature of the intelligence warfighting function and special forces. You will read COL Wempe's article, “Army Special Operations Intelligence: Capable and Ready,” in which the USASOC senior intelligence officer provides an overview of the Army special operations forces' (ARSOF) mission and USASOC's vision and command strategy. He also explains how the intelligence warfighting function operates within SOF and the various opportunities available to intelligence professionals. The material is comprehensive; it will give you a foundation of how our warfighting function trains and supports SOF. You will also read an article by retired LTC McCarthy in which he explains how to improve intelligence support to a single irregular warfare activity. He describes SOF missions, how intelligence shapes these missions, and the processes being developed to analyze

intelligence. Another interesting article, by Bill Goss and Andy Gordon, describes how ARSOF is using a data repository to share data across our intelligence system of record, the Distributed Common Ground System-Army. The article explains the importance of this repository to ARSOF missions and intelligence Soldiers.

The SOF community influences various environments, and the opportunities for your involvement are endless; the high operational tempo and frequent deployments offer professionally rewarding experiences. The skills you develop, the

leadership you encounter, and the Soldiers you serve will forever leave an imprint on your military career. 

Endnotes

1. U.S. Army Special Operations Command website, "Office of the Strategic Services" page, accessed 3 December 2018, <http://www.soc.mil/OSS/special-operations.html>.
2. Michael Vickers, "Decisions in the Situation Room," interview by Eric Jaffe, Gerson Lehrman Group, Inc. (GLG), 21 April 2017, <https://glg.it/videos/michael-vickers-interview-osama-bin-laden-raid>.

Always Out Front!

Intelligence Doctrine Update

On 1 March 2019, the U.S. Army published ATP 2-01.3, *Intelligence Preparation of the Battlefield*, also known as IPB. IPB is a collaborative staff effort led by the J-2/G-2/S-2 and the intelligence staff. The IPB process is a critical staff function, as it impacts the range of military operations, is relevant across all echelons, and is a fundamental element within all planning. IPB serves as the primary framework for analysis of the battlefield during the military decision-making process. The July-September 2019 issue of *Military Intelligence Professional Bulletin* will contain an article emphasizing important updates within the IPB publication. Until then, here are the highlights:

What remains the same in this version?

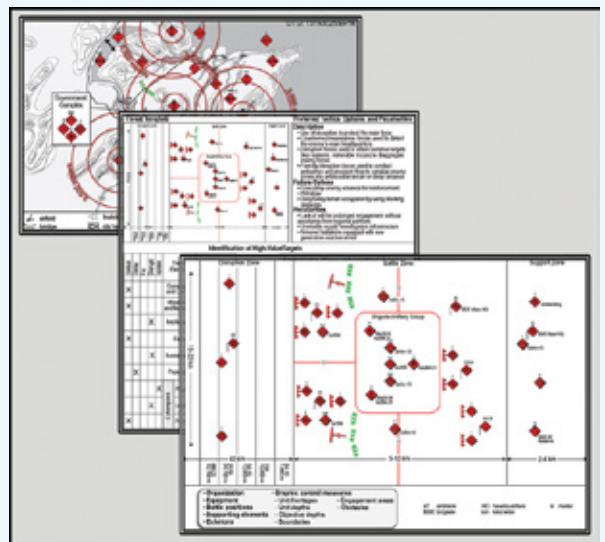
- ◆ Retains the time-tested doctrinal steps and sub-steps of the IPB process.
- ◆ Highlights staff processes and products to assist commanders and staffs in identifying when and where to leverage friendly capabilities during operations.

What is new or significantly revised?

- ◆ Aligns terminology with current doctrine.
- ◆ Focuses on large-scale combat operations, multi-domain operations, and operations against a peer threat.
- ◆ Addresses the complex operational environment in which U.S. forces will operate across all domains (air, land, space, maritime, and cyberspace), the information environment, and the electromagnetic spectrum.
- ◆ Adds an entire appendix on cyberspace considerations.
- ◆ Adds an appendix on terrain, movement, and weapon data tables from the rescinded FM 34-130, *Intelligence Preparation of the Battlefield*, dated 8 July 1994.

Where can I access the publication?

- ◆ Army Publishing Directorate: <https://armypubs.army.mil/> then – Publications – Doctrine and Training – ATP – ATP 2-01.3.
- ◆ Intelligence Knowledge Network Public Portal: <https://www.ikn.army.mil/> then select the MI Doctrine icon.
- ◆ Intelligence Knowledge Network (common access card required): <https://ikn.army.mil/> then select the MI Doctrine icon.



CSM FORUM

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



The special operations community provides Soldiers a unique opportunity to be part of an elite team, expand their knowledge beyond the confines of conventional warfare, and execute some of our Nation's most critical missions. For military intelligence (MI) professionals, the community offers a challenging and beneficial environment to enhance their tactical skills and develop greater technical proficiency in their military occupational specialties (MOS) while having an impact on America's long-term strategic goals and tactical objectives around the globe.

As a whole, these assignments offer diverse and complicated mission sets that place these units at the forefront of U.S. foreign policy in many regions. While a special operations forces (SOF) unit's mission varies depending on the location and U.S. objectives, the intelligence warfighting function's application does not. Intelligence still drives operations, and therefore MI professionals assigned to SOF units must thoroughly understand the intelligence warfighting function's conventional contribution to mission planning and find innovative ways to leverage this understanding in unconventional settings.

SOF elements often operate in small, cohesive teams conducting unique missions in various locations. Enabling SOF operators with accurate, timely, and relevant intelligence is an extremely daunting task that requires a great deal of mental and physical stamina while operating at a very high level. Understanding the intelligence warfighting function beyond just one MOS is immensely helpful to provide the necessary support to each individual team.

SOF elements sometimes work in areas controlled by conventional forces and, at times, conduct operations in cooperation with these elements. This collaboration requires leveraging intelligence from all Army echelons and from members of the greater intelligence community. Army MI professionals with experience operating in a variety of communities can help fill intelligence gaps because they understand other mission sets and are capable of reaching

across community lines to offer positive synergistic outcomes. Every assignment creates knowledge, skills, and abilities, and supporting the special operations community develops leaders in ways that make them valuable at any echelon.

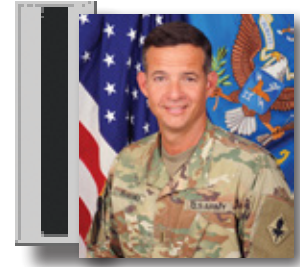
MI Soldiers often express a concern that they are unable to "do their job" or practice their technical skills. MI professionals assigned to support SOF are empowered to apply their MOS-specific skills in support of ongoing operations around the world. MI Soldiers may even find themselves embedded with SOF teams, providing direct support with a specific intelligence discipline while participating in a broad spectrum of operations. The U.S. Army Special Operations Command maintains a continuing worldwide mission that requires the most proficient and well-trained fighting force. In order to meet this need, MI professionals assigned to special forces units may be afforded an opportunity to attend the most up-to-date military training and MOS-specific schools, enhancing the level of expertise they provide to the community. Troop schools, such as Ranger, Airborne, Air Assault, and Pathfinder, and other selective courses are opportunities that most MI Soldiers will find difficult to acquire in conventional units; however, the need for these specialized skills in the special operations community increases the opportunity for MI Soldiers to attend non-traditional training and set themselves apart from their peers in their MOS.

It is true that assignments in the special operations community are both demanding and challenging, but they are also among the most gratifying and rewarding for Soldiers. Regardless of whether the focus of the individual is to challenge themselves or increase their skillsets for career progression, the benefits for MI professionals to serve in the special operations community are immense. Senior leaders across the Army understand if they are assigned a Soldier of any rank who served in special operations, they are receiving someone who will positively impact their mission. ✨

Always Out Front!

Technical Perspective

by Chief Warrant Officer 5 David J. Bassili
Chief Warrant Officer of the MI Corps
U.S. Army Intelligence Center of Excellence



One look at my biography and you can see I never had an opportunity to serve in a special operations unit. That fact does not stop the excitement I feel when I read, or hear, about the exploits of our cohort's technical leaders who have served, or are serving, in the special operations community. During the first decade of my career, interaction and cooperation between special operations forces (SOF) and general-purpose forces rarely occurred at the level they have since the Global War on Terrorism began. My experiences in Iraq, Afghanistan, and other locales opened the doors to unprecedented cooperation and collaboration that afforded me close working relationships with SOF intelligence professionals and operators alike. Prior to this, I was under the misconception that SOF intelligence professionals were trained on and had access to special intelligence analytical skills and tools—unlike the rest of us. This is not to say that SOF intelligence professionals do not possess unique capabilities for their missions; or that they do not possess unique techniques to describe the operational environment and to derive threat courses of action. In reality, the same strong doctrinal foundation that makes for a successful intelligence analyst in an armored brigade combat team is likewise what creates success in SOF.

Whether assigned to a combat aviation brigade, field artillery battalion, or an infantry brigade combat team, one aspect that enables successful intelligence professionals is a strong understanding of those organizations' doctrine. The same holds true within the joint and Army 3-05 series doctrinal publications for those serving within a special operations unit. Like any Army operation, it is imperative that we as intelligence professionals understand the difference between, and the specific details of, the Army SOF core competencies of special warfare and surgical strike, as well as the 12 core activities that describe SOF operations listed in ADRP 3-05, *Special Operations*. Developing this operational understanding is critical to enabling timely, detailed, and accurate intelligence support, whether we are working a foreign internal defense mission or conducting an area defense in an armored brigade combat team.

Intelligence professionals in SOF organizations rely on the principles outlined in ADP 2-0, *Intelligence*. As part of an

increased collaboration with SOF units since 2001, many of us are familiar with the memory aids ASCOPE, PMESII, and CARVER¹ as an additional means to assess and define civil considerations and target selection criteria. ATP 3-05.20, *Special Operations Intelligence*, currently in revision, provides other techniques that may prove useful to certain conventional Army units at a particular time in a joint or Army operation. Another process, which some of you may not be familiar with, is the IGIVO analysis (issues, goals, influence, vulnerabilities, and opportunities) that is used to assess populations.

Like FM 2-0, *Intelligence*, ATP 3-05.20 describes intelligence tasks and techniques for employment in support of SOF core activities. The greatest challenge to providing intelligence support for SOF missions is the nature in which most of these operations occur: small teams in denied and/or politically sensitive environments against a "strategic" target where speed and accuracy are critical and the need to "make a call" on less than perfect information is paramount to the commander on the ground. All of that description is mostly true and applies to many of us who support any Army operation—but right or wrong, there is a difference between strategic and tactical significance. Possessing a sound understanding of doctrine is the starting point; otherwise, the chances of being successful diminish. Although I cannot provide examples from my experience, I am confident this remains true for those within our Army SOF formations. This quarter's *Military Intelligence Professional Bulletin* offers additional depth and context from those serving in SOF organizations. If you are looking for a challenging and rewarding assignment in the special operations community but are apprehensive because you aren't sure...reach out to these professionals or your peers currently serving in SOF. They can answer your questions.

I hope 2019 continues to bring nothing but success and happiness to each and every one of you! 🌟

Endnote

1. ASCOPE—areas, structures, capabilities, organizations, people, and events; PMESII—political, military, economic, social, information, and infrastructure; and CARVER—criticality, accessibility, recuperability, vulnerability, effect, and recognizability.

Always Out Front!

Army Special Operations Intelligence: Capable and Ready

by Colonel Patrick Wempe



Introduction

For more than 60 years, U.S. Army special operations forces (ARSOF) have served at the tip of the spear in defense of the Nation. Today, as the Nation stands at an inflection point with the return of interstate strategic competition, the U.S. Army Special Operations Command (USASOC) represents a force of approximately 33,000 personnel and more than half of the Nation's special operations forces (SOF). They are the Army's experts in irregular warfare, playing a critical role in sharpening the United States' competitive edge to compete, deter, and win across the conflict continuum.

ARSOF elements consistently fill more than 60 percent of all U.S. SOF deployments worldwide, with ARSOF Soldiers deployed in more than 70 countries on any given day of the year, delivering strategic value to the Nation through four complementary capabilities—USASOC Capability Pillars: an Indigenous Approach, Precision Targeting, Developing Understanding and Wielding Influence, and Crisis Response.

ARSOF personnel are employed throughout the operational spectrum and across all campaign phases. Together, the USASOC Capability Pillars provide options to shape or prevent outcomes in support of our national interests. These capabilities, coupled with tailorable mission command nodes and scalable force packages that are low-signature and employ a small footprint, are particularly suited for employment in politically sensitive environments, as well as in denied territory in large-scale combat operations.

Across the ARSOF community, military intelligence (MI) Soldiers are integral members of the ARSOF team, providing credible, responsive, and timely intelligence capabilities to survivable, lethal, and agile special forces, civil affairs, psychological operations, ranger, and SOF aviation formations around the globe.

Army Special Operations Forces Mission

As the Army Service component command for U.S. Special Operations Command (USSOCOM) and a major command for the Department of the Army, USASOC "mans, trains, equips, educates, organizes, sustains, and supports forces

to conduct special warfare and surgical strike across the full range of military operations and spectrum of conflict in support of joint force commanders and interagency partners, to meet theater and national objectives."¹

USASOC, as the senior headquarters for all Army SOF, combines the roles, responsibilities, and authorities that U.S. Army Forces Command (FORSCOM), U.S. Army Training and Doctrine Command, and U.S. Army Futures Command execute on behalf of the broader Army. These responsibilities include—

- ◆ Training and readiness oversight.
- ◆ Initial entry training and professional military education for special forces, civil affairs, and psychological operations Soldiers.
- ◆ Doctrine and proponentcy.
- ◆ Capability and concept development.
- ◆ Resource sponsorship.

Vision of the U.S. Army Special Operations Command Commanding General

USASOC Commanding General LTG Francis Beaudette has provided a vision in which "ARSOF will be globally postured and ready to compete, respond, fight, and win against adversaries across the range of military operations, anytime and anywhere, as part of a joint force. ARSOF will leverage adaptive and innovative institutions, empowered Soldiers, and integrated units capable of delivering unmatched special operations capabilities in order to provide joint force commanders operational options and advantage over our Nation's adversaries."² ARSOF intelligence is integral to this vision, supporting planning, decision making, and operations, synchronized and in many cases integrated with Army and joint SOF partners.

U.S. Army Special Operations Command's Command Strategy

To accomplish the USASOC mission and achieve the Commanding General's vision, the command is updating

its ARSOF Strategy. The end state of this strategy will be a globally postured, multi-domain dominant ARSOF, ready to compete, respond, fight, win, and consolidate gains against adversaries across the range of military operations, anytime and anywhere, as part of the joint force. Foundational to this strategy are the USASOC Capability Pillars. These capability pillars form the foundation of what ARSOF provides for our Nation through the joint force. Our purpose as an institution is to provide survivable, lethal, and agile ARSOF to joint force commanders and interagency leaders. The sum of our four capability pillars represent what ARSOF brings to prevail in competition while simultaneously setting conditions to win in war:

“The indigenous approach is a different lens through which to view challenges to regional stability; to view them as problems to be solved by empowered populations living in the region. It includes core tasks such as Foreign Internal Defense and Unconventional Warfare and involves advise, assist, and accompany type activities. Through an indigenous approach, ARSOF personnel live among, train, advise, and fight alongside people of foreign cultures, achieving effects with and through partner forces.

Precision targeting operations involve Direct Action and counter-network activities enabled by SOF unique intelligence, technology, and targeting processes. Precision targeting operations can be employed against uniquely difficult target sets that require long-range movement and careful application of force. They can be employed to buy time and space for other operations to gain traction, as seen in counterinsurgency efforts. Precision targeting operations also collapse transregional threat networks through deliberate targeting of critical enemy nodes, as seen in counterterrorism campaigns.

Developing understanding and wielding influence are essential aspects of the value SOF capabilities provide the Nation. The SOF network of personnel, assets, and formations represents means by which to obtain early understanding of trends, emerging transregional threats, and where opportunities exist. Employment of the SOF network also provides capabilities needed to influence outcomes, especially in environments experiencing conflict short of overt war.

Crisis response, through alert forces, persistently deployed and dispersed units, and our network of allies and partners, provides national decision makers with the agile and rapidly employable special operations formations necessary to respond to emergencies. These forces provide options to rescue people under threat, to recover sensitive materials such

as [weapons of mass destruction] WMD components, or to execute other short notice requirements.”³

These capability pillars are interdependent and reinforcing. An indigenous approach enables ARSOF to develop understanding of the operational environment, which increases the effectiveness of influence in competition, precision targeting, and crisis response, as situations escalate. MI is a critical enabler of these capability pillars, providing intelligence capabilities that contribute to the development of understanding and sharing across the intelligence community resulting in a more holistic shared situational understanding of the operational environment.

Army Special Operations Forces and the National Defense Strategy

Within the context of the national defense strategy and in the contemporary and future operating environments, ARSOF must deliver proactive and scalable military options for decision makers across the four interdependent layers of the Global Operating Model (contact, blunt, surge, and homeland).⁴

Within the contact layer, ARSOF can help deter adversary aggression by strengthening alliances and attracting new partners, while simultaneously imposing costs on adversary malign behavior. In the blunt layer, ARSOF can delay, deter, degrade, and deny adversary advances by creating multiple multi-domain dilemmas, complicating decision making, and inducing cognitive duress. In support of surge, ARSOF can facilitate the defeat and destruction of enemies in large-scale combat operations by delivering multi-domain effects, penetrating and disintegrating antiaccess/air defense systems, and creating positions of relative advantages for the joint force. ARSOF can achieve surprise through maneuver across strategic distances and arrive at locations where the enemy does not expect them. For support to the homeland layer, ARSOF must defend the United States by sharing information and enhancing multilateral partnerships; respond to chemical, biological, radiological, nuclear, and high-yield explosive events; and provide support to civil authorities when required.

Notably, one of the highest priorities of ARSOF leadership is a focus on conventional forces/SOF integration, interoperability, and interdependence (CF/SOF I3). This priority applies to doctrinal, training, systems, and personal relationships, and it informs and influences virtually every aspect of ARSOF’s organizational planning. The end result of these CF/SOF I3 efforts is improved shared situational understanding and synchronized conventional forces/SOF multi-domain effects in competition and large-scale combat

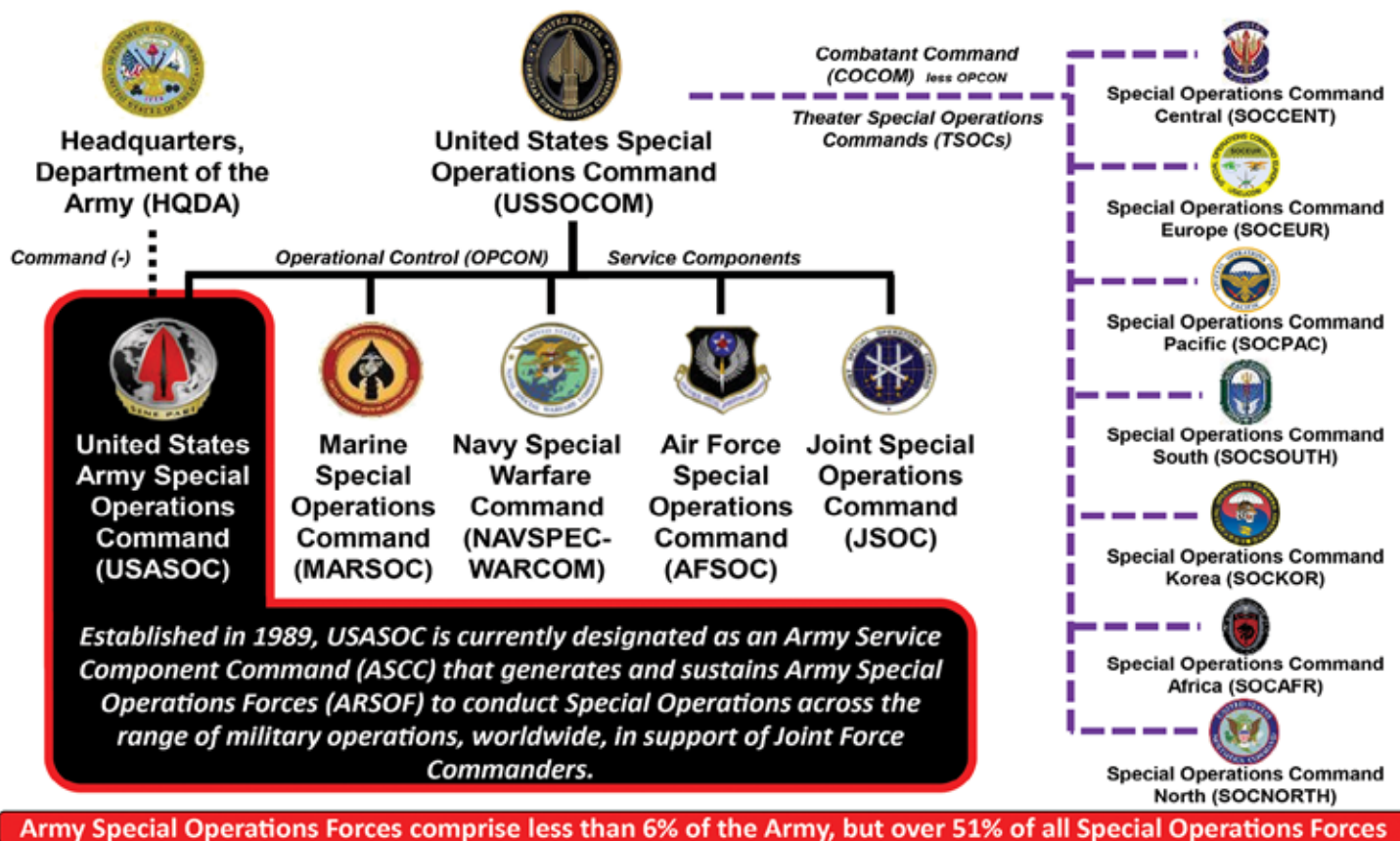


Figure 1. USSOCOM Task Organization

operations. ARSOF is committed to joining with Army and joint service partners in mutually beneficial, enduring partnerships. This is being accomplished by:

- ◆ increasing our participation in combat training center rotations and other training venues;
- ◆ ensuring complementary, and mutually supporting, doctrinal concepts, interoperability of mission command systems, and intelligence data;
- ◆ exploring shared training and operational facilities; and
- ◆ conducting other initiatives.

Army Special Operations Forces Organization

USASOC is under operational control to and serves as the Army Service component command for USSOCOM, as shown in Figure 1.

Within ARSOF, several subordinate commands and subordinate units provide critical capabilities to the joint force and the Nation (Figure 2, on the next page).

Significantly enhancing these capabilities are the enduring regional alignments of ARSOF (Figure 3, on the next page), providing deep and broad regional and cultural understanding, continuity in relationships with foreign regional partners, language capabilities, and responsiveness.

The preponderance of the ARSOF intelligence force resides within our seven special forces groups, the largest component of the ARSOF formation. These special forces groups are enabled with a full complement of MI capabilities. These personnel typically operate in small footprint, sensitive, and partnered operations in theater, many of which are sustained for years and even decades.

Army Special Operations Forces Opportunities

Assignments to ARSOF as an MI Soldier provide outstanding opportunities for advanced training, operational deployments, professional and technical development, adventure, and challenge. Most of the assignments within ARSOF are not nominative, and our Soldiers, particularly our junior enlisted, receive assignment to SOF through standard Human Resources Command and MI Branch processes. At the sergeant first class, master sergeant, and sergeant major level, our MI senior enlisted advisors work closely with MI Branch to slate the right noncommissioned officers into those positions in ARSOF. The slating process also deliberately assigns current ARSOF MI noncommissioned officers into non-SOF positions in FORSCOM, U.S. Army Intelligence and Security Command (INSCOM), and other communities to enhance their development and to help deepen the relationships between ARSOF and those non-SOF formations. Warrant officers and officers are generally managed on a by-name basis.

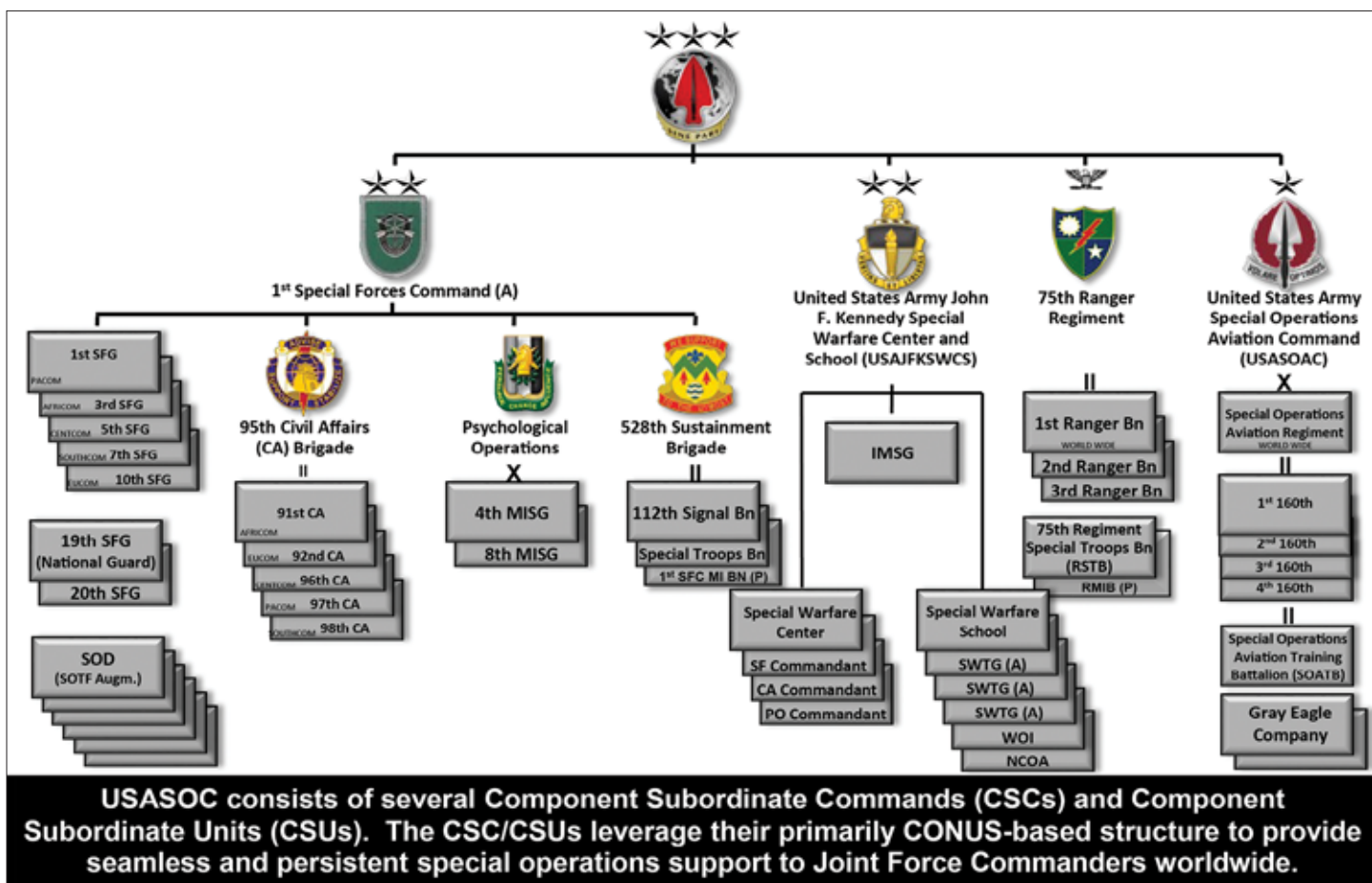


Figure 2. USASOC Task Organization

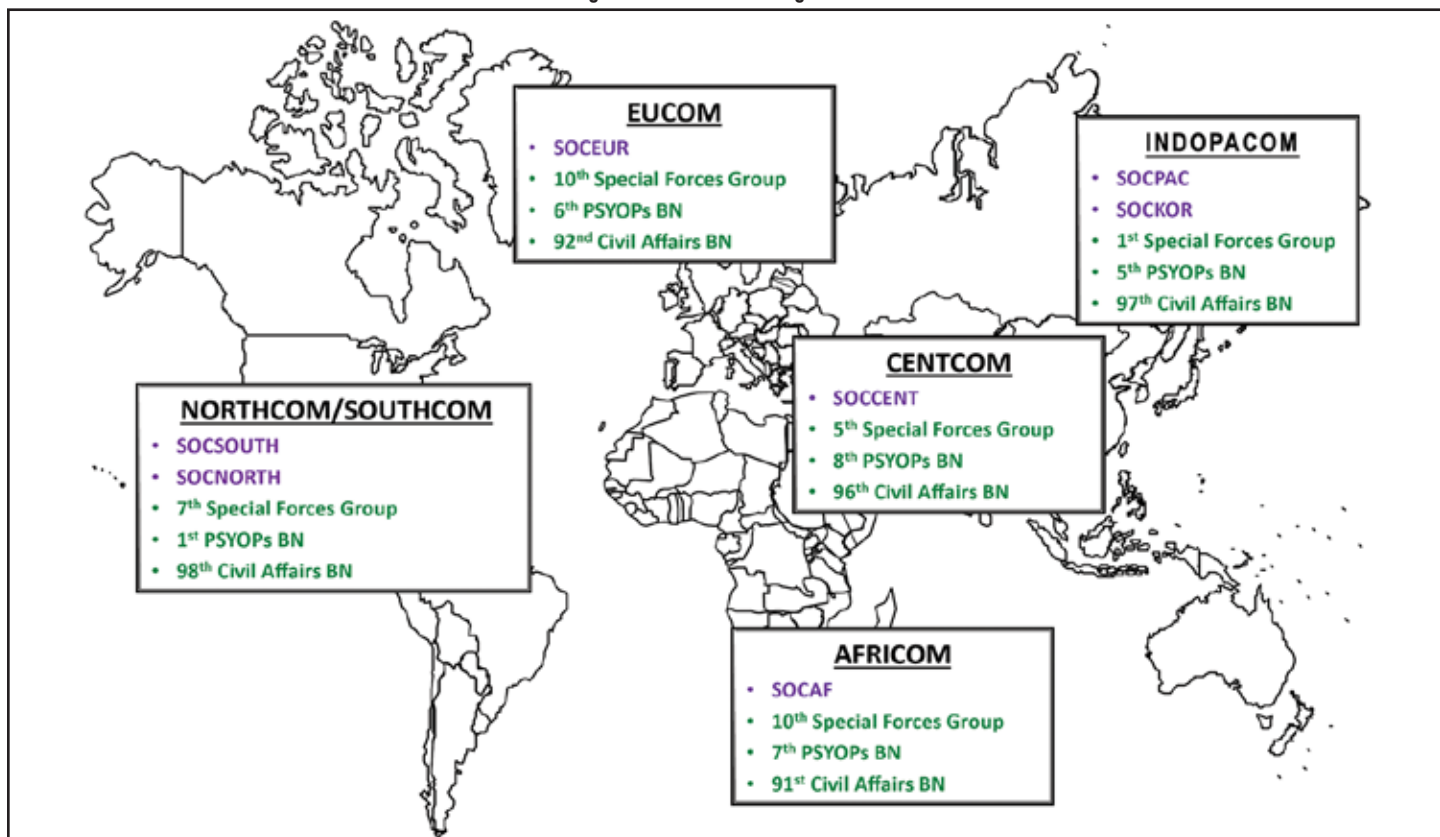


Figure 3. ARSOF Theater Alignment

<p>Officer KD Opportunities</p> <ul style="list-style-type: none"> • O5: 1 x DIV G2, Starting FY19 (CSL) 2 x BN Commands (pending VCSA approval) • O4: 11 x Group/BDE/RGT S2s; 2 x BN S3/XO • O3: 38 x BN/BDE S2s; 2 x MICO Commands • CW4: 5 x 351M; 5 x 352N • CW3: 5 x 350F; 6 x 351L • CW2: 15 x 350F; 5 x 350G 	<p>Noncommissioned Officer Opportunities*</p> <ul style="list-style-type: none"> • E7: SWTG SR Instructor Writer; SF Group Senior Intel Sergeant; Crypto Linguist Supervisor; Sr. CI Sergeant; Sr. Imagery Sergeant • E8: SFG Chief Intel Sergeant; SIGINT Sergeant; SFG MI Company 1SG; 1SFC MI BN CO 1SG; PED DET NCOIC • E9: 1SFC G2 SGM; 1SFC MI BN CSM; USASOC G2 SGM; 75th RGR S2 SGM; 160th S2 SGM; ARSOAC G2 SGM; RMIB CSM <p>*Slating process ICW HRC and ARSOFC CSMs/SGMs</p>
<p>Enlisted CMF Progression in ARSOF</p> <ul style="list-style-type: none"> • 35F: Special Operations Intel Analyst, Intel Sergeant • 35G: Imagery Analyst/Sergeant • 35L: SFG/75 RGR/1SFC/ CI Agent/Sergeant • 35M: SFG/75 RGR/1SFC/ HUMINT Collector/SGT • 35N: SOT-B Team Member, SIGINT SGT • 35S: Special Operations Team SIGINT Specialist • 35P: SOT-A Team Member, SIGINT SGT • 35S: SOT-B Team Member • 35T: SFG/75 RGR/1SFC/ System Maintainer • 12Y: 64th GPC Engineer, SFG GEOINT 	<p>Assignment within ARSOF provides:</p> <ul style="list-style-type: none"> • Exposure to global SOF missions and operations • Unique small-team, tight-knit environment • Opportunities for specialty schools such as Airborne School and Ranger School (SOT-A's) • Promotion and advancement rates highly competitive against Conventional Force rates • Broadens perspectives and provides experience useful to future assignments

Figure 4. ARSOF Key Intelligence Assignments

For most MI military occupational specialties and grades, many opportunities exist within ARSOF for key developmental and other assignments (Figure 4).


Conventional Forces/Special Operations Forces Integration, Interoperability, and Interdependence

USASOC has initiated a number of efforts for CF/SOF I3, such as the ARSOF Data Integration Initiative. This issue of *Military Intelligence Professional Bulletin* includes an article titled "Army Special Operations Forces Data Integration Initiative" that highlights the ARSOF initiative. USASOC is also continuing its efforts to increase readiness and enhance CF/SOF I3 by partnering with FORSCOM, INSCOM, U.S. Army Installation Management Command, and others to develop the Fort Bragg Intelligence Campus concept. This effort, intended to generate operational synergies while achieving investment and sustainment efficiencies, will create a "hub" for the Fort Bragg military intelligence community, which includes operations; training; processing, exploitation, and dissemination; and other activities. With already programmed USASOC military construction starting in fiscal year 2022 to anchor the concept, the partnered planning effort will establish a phased approach to developing the Fort Bragg Intelligence Campus as the other part-

ners pursue Army resourcing for intelligence training, FORSCOM processing, exploitation, and dissemination, and other facilities requirements.

Conclusion

ARSOF, with their organic MI Soldiers, elements, and capabilities, play an important role in the Army and in joint, interagency, intergovernmental, and multinational environments. Robust operational capabilities, specialized skills, sustained readiness, responsiveness, and agility are inherent elements of ARSOF capabilities. Global presence and enduring regional relationships further enhance those capabilities, and they

provide situational understanding and operational flexibility to joint force commanders. Along with FORSCOM, INSCOM, theater Army Service component commands, and our special operations partners, ARSOF is ready and capable of responding to the demands of the National Defense Strategy to ensure the security of the United States. 

Endnotes

1. U.S. Army Special Operations Command, *USASOC Strategy-2035* (April 2016), 2, <https://www.soc.mil/AssortedPages/USASOCStrategy2035.pdf>.
2. U.S. Army Special Operations Command, *Army Special Operations Vision* (18 August 2018), 1, [https://www.soc.mil/AssortedPages/ARSOF%20Vision%20\(Final%2020AUG18\).pdf](https://www.soc.mil/AssortedPages/ARSOF%20Vision%20(Final%2020AUG18).pdf).
3. U.S. Army Special Operations Command, *USASOC Campaign Plan 2035 Annual Update* (1 March 2018), 7-8, http://www.soc.mil/AssortedPages/USASOCCampaignPlan2035_2018.pdf.
4. "The Global Operating Model describes how the Joint Force will be postured and employed to achieve its competition and wartime missions...It comprises four layers: contact, blunt, surge, and homeland. These are, respectively, designed to help us compete more effectively below the level of armed conflict; delay, degrade, or deny adversary aggression; surge war-winning forces and manage conflict escalation; and defend the U.S. homeland." Office of the Secretary of Defense, *Summary of the 2018 National Defense Strategy of the United States of America*, n.d., 7, <https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf>.

COL Patrick Wempe is the G-2 for the U.S. Army Special Operations Command headquartered at Fort Bragg, NC. He has 27 years of experience in tactical, U.S. Army Intelligence and Security Command, special operations, joint, and interagency assignments.

Army Special Operations Forces Data Integration Initiative



by Mr. William D. Goss and Mr. James A. Gordon

Background

Joint forces operate across the range of military operations, in environments of cooperation, competition, and conflict. These forces require access to current and historical operations and intelligence information to enable situational understanding of the operating environment and to inform military decision making.

FM 6-05, *Multi-Service Tactics, Techniques, and Procedures for Conventional Forces and Special Operations Forces Integration, Interoperability, and Interdependence*, provides the doctrinal foundation for conventional forces' and special operations forces' (SOF) collaboration in the development of this situational understanding. FM 6-05 opens with "Recent conflicts have changed the paradigm for conventional forces (CF), special operations forces (SOF), and other partner operations. Traditionally, CF and SOF operated in their own distinct area of operations (AO), requiring minimal deconfliction of time and space...CF, SOF, and other partners are now operating in proximity or in overlapping AOs. Increasingly, they rely upon each other's capabilities in support of regional and theater objectives."¹ The manual further states "CF and SOF intelligence sharing and collaboration must occur, at every level, to develop an understanding of the threat's actions, activities, and anticipated steps...Information considered unimportant to one may be the critical missing piece for the other."²

Data sharing has historically been a challenge for elements such as SOF—globally deployed across geographic combatant command areas of responsibility and operating numer-

ous systems on differing networks and domains. Despite these challenges, U.S. Army Special Operations Command (USASOC), in partnership with the Army, has developed a capability to share SOF operations and intelligence data across the intelligence community and intelligence architecture at an unprecedented level—through the U.S. Army special operations forces (ARSOF) Data Integration Initiative (ADI2).

Overview

With support from the U.S. Army intelligence community, USASOC initiated ADI2 to establish a shareable repository of SOF-specific operational and intelligence data, using Distributed Common Ground System-Army (DCGS-A) equipment, technology, and architecture. To establish this database, the USASOC G-2 and a small team of data architecture subject matter experts identified SOF-specific data sets, negotiated for access, ingested and converted the data into a DCGS-compatible format, and stored it in a repository that is simultaneously shared across the DCGS-A enterprise. ADI2 is one of the most significant conventional forces/SOF integration, interoperability, and interdependence efforts, with the potential for unprecedented effects across the range of military operations.

Significance of ADI2

ARSOF Soldiers are deployed to more than 70 countries on any given day of the year. Over time, this persistent presence enables language-qualified, culturally astute ARSOF elements to develop a deep understanding in cooperation and competition environments, especially focused on

human aspects of the operating environment. Using DCGS—A capabilities, analysts in Army formations can integrate this SOF reporting and analysis with multidiscipline intelligence sources to enable an integrated, holistic understanding of the operating environment on a “single pane of glass.”

ADP 3-0, *Operations*, states “Because war is a fundamentally human endeavor, it is inextricably tied to the populations inhabiting the land domain...Understanding the human context that enables the enemy’s will, which includes culture, economics, and history, is as important as understanding the enemy’s military capabilities.”³ As noted above, much of SOF-developed intelligence and operational production is population-centric in nature. Special forces, civil affairs, and psychological operations units focus on and interact with foreign government, military, and civilian populations, viewing them through different lenses. The fusion of this data and the integration with other data sets provide a unique and valuable characterization of human aspects of the environment for joint forces. This information can be of immense value in understanding civil considerations and partner capabilities during planning and operations when conducting intelligence preparation of the battlefield and assessing mission variables using ASCOPE (areas, structures, capabilities, organizations, people, and events) and operational variables using PMESII-PT (political, military, economic, social, information, infrastructure, physical environment, and time).

ADI2 is of particular value for Army units and joint, interagency, intergovernmental, and multinational partners with any degree of regional alignment or focus. U.S. Army Intelligence and Security Command’s (INSCOM) military intelligence brigades—theater (MIB—T) provide regionally focused collection and analysis in support of theater army daily operations requirements. As they do this, they are the focal points of integration for regionally focused SOF data. MIB—Ts, like SOF, are regionally focused and deployed globally in steady state; they serve as an anchor point for integration of theater-focused data. Integration of ADI2 data at the MIB—Ts will contribute to their development of threat characteristics, intelligence estimates, threat and civil considerations, and all-source intelligence products in support of the theater commands. Similarly, this data will be of significant value to security force assistance brigades as they conduct training, advising, assisting, enabling, and accompanying operations with allied and partner nations globally.

ADI2 also has significant applicability in SOF support to large-scale combat operations’ preparation and execution. During cooperation and competition timeframes, SOF’s persistent global presence can be leveraged to develop an

understanding of adversary intentions, preparation, and activities. The resultant data from these observations is being made available using ADI2 connectivity with the intelligence community. During transition to conflict, results of intelligence collection and ongoing operations will populate the DCGS—A data environment through ADI2, improving integrated situational understanding of the threat and the operating environment.

Systems and Architecture

ADI2 operates on DCGS—A systems and architecture. The DCGS—A program office fielded a secret-level DCGS—A Intelligence Processing Center (IPC) to USASOC in fiscal year 2018. The IPC is the same system that hosts the fixed site brains at each of the regionally aligned MIB—Ts, providing significant storage and processing capabilities. SOF data ingested into USASOC’s IPC is organized into appropriate geographic combatant command-oriented folders by data source, which enables passing of the data to the appropriate MIB—T, to be further shared with theater army forces and integrated with existing theater intelligence data. In the near future, this data will also be shareable across coalition networks and moveable across domains to top secret/sensitive compartmented information networks to share with interagency partners across the intelligence community.

The Database

Currently, the data repository has 85 data sources and more than 400,000 records, with more records added every week. The data includes—

- ◆ Reporting from theater special operations commands.
- ◆ Special Operations Debrief and Retrieval System reports.
- ◆ Civil affairs surveys.
- ◆ SOF Information Dissemination Environment portal data.
- ◆ Psychological operations-generated cultural intelligence assessments.
- ◆ Deployed special operations task force data.
- ◆ Joint Improvised-Threat Defeat Organization data sets.
- ◆ Other SOF-specific data sets.

New SOF data sets are constantly evaluated for possible ingest; outreach to find other sources of data is a weekly order of business. The newly fielded IPC will allow ADI2 to expand data ingestion to hundreds of data sources and the storage of millions of documents that can be shared across the DCGS—A enterprise.

Accessing the Data

Since the regionally focused ADI2 data is pushed to each of the regionally aligned MIB-Ts, which provide theater intelligence data to deploying and regionally aligned Army forces, Army analysts can access the data on the DCGS-A Portable Multi-Function Workstation. Deploying units can also request the USASOC DCGS-A data sources through INSCOM's Ground Intelligence Support Activity. Finally, for non-DCGS-A hardware users, analysts can access the USASOC data through the web-based Ozone capability using the DCGS Integration Backbone.

Way Ahead

For the first time, ADI2 establishes an enduring repository of SOF activities, reports, and analysis over time, shareable across the intelligence community. This foundational data collection and standardization step places USASOC in position to move forward with the DCGS-A program office's future capability drops. It also allows USASOC to fully lever-

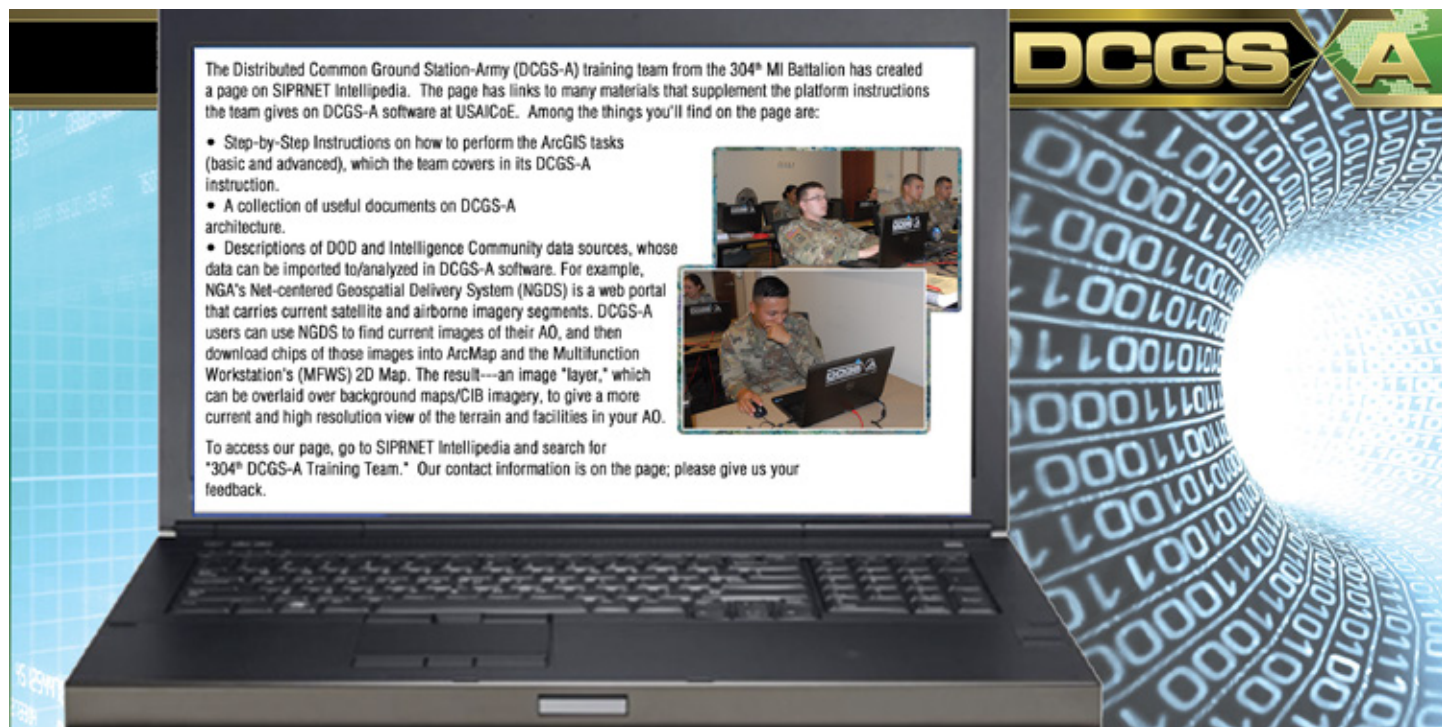
age emerging data science, artificial intelligence, and machine learning capabilities to uncover deeper insights from the data, integrated with other data sets. As capabilities are developed, the ADI2 data repository will be a robust test bed for these applications and management systems. It will reduce the analytical burden on the analysts and will enable machine-assisted trend analysis, indication and warning awareness, prediction models, and deeper situational understanding across commands. ✨

Endnotes

1. Air Land Sea Applications Center, Field Manual 6-05, *Multi-Service Tactics, Techniques, and Procedures for Conventional Forces and Special Operations Forces Integration, Interoperability, and Interdependence* (Washington, DC: U.S. Government Publishing Office [GPO], 4 April 2018), 1.
2. Ibid., 51.
3. Department of the Army, Army Doctrine Publication 3-0, *Operations* (Washington, DC: U.S. GPO, 6 October 2017), 2.

William (Bill) D. Goss is the data manager for U.S. Army Special Operations Command's (USASOC) U.S. Army special operations forces data integration initiative efforts. He is a retired Army lieutenant colonel who spent 12 years as an infantry officer before becoming a strategic intelligence officer (FA 34). His intelligence assignments include Joint Intelligence Operations Center Europe, U.S. European Command; U.S. Army Europe G-2, including time as the Analysis and Control Element Chief with the 66th Military Intelligence Brigade; and intelligence planner at Rapid Reaction Corps-France. He also worked as a contractor at the Defense Intelligence Agency as an intelligence planner and at the 902nd Military Intelligence Brigade as a Joint Terrorism Task Force counterintelligence analyst. Mr. Goss holds a bachelor of science in military history from the U.S. Military Academy and is a graduate of the Post Graduate Intelligence Program at the former Joint Military Intelligence College, with a certification in the Denial and Deception Advanced Studies Program.

James A. (Andy) Gordon is the G-25/9, Chief, Strategic Plans, Analysis, and Capability Development for USASOC G-2. He is a retired Army military intelligence lieutenant colonel with more than 23 years of military experience in U.S. Army Forces Command, U.S. Army Intelligence and Security Command, and U.S. Recruiting Command units and more than 6 years as a Department of the Army Civilian at USASOC.





The 75th Ranger Regiment Military Intelligence Battalion

Modernizing for Multi-Domain Battle

by Major Paul A. Lushenko, U.S. Army

A soldier pulls himself across a rope bridge 21 February 2011 during the Mountain Phase of Ranger School at Camp Merrill, Dahlonega, Georgia. Regimental Military Intelligence Battalion personnel complete the same training as combat arms soldiers assigned to the ranger battalions, including the U.S. Army's Airborne and Ranger courses. (Photo by John D. Helms, U.S. Army)



Editor's Note: This article is reprinted with the permission of Military Review, the Professional Journal of the U.S. Army, Combined Arms Center, Fort Leavenworth, Kansas. It was originally published in the July-August 2018 issue of Military Review.

Since the original publication of this article, there has been a change to terminology. Multi-domain operations has replaced multi-domain battle as the concept for how U.S. Army forces will approach defeating our adversaries in the future.

A focus on counterinsurgency and counterterrorism operations since 9/11 has eroded the U.S. Army's readiness according to Gen. Mark Milley, chief of staff of the Army. Defined by Milley, readiness approximates the Army's ability to exercise its organizational design and fulfill its mission.¹ The Army's doctrinal mission consists of fighting and winning America's wars through sustained land combat as a member of the joint force.² The most pernicious consequence of the Army's readiness deficit is its inability to overmatch the lethality of near-peer competitors including the so-called "Big Four": China, Iran, North Korea, and Russia. The Army's modernization strategy, published on 3 October 2017, is designed to ensure soldiers and units are prepared to confront these and other threats. This principal goal turns on several priorities including optimizing human performance and designing a "network" that is insured to operating environments characterized by a denied or degraded electromagnetic spectrum.³

One recent example of U.S. Army modernization is the establishment of the 75th Ranger Regiment's Military Intelligence Battalion (RMIB) on 22 May 2017 at Fort Benning, Georgia. I argue that while the RMIB furthers the Ranger Regiment's readiness through experimentation and innovation, it also informs the Army's broader structure and emerging operating concepts to help overmatch near-peer competitors.

Perhaps the most progressive of those concepts is multi-domain battle (MDB). According to then U.S. Army Training and Doctrine Command (TRADOC) commander, Gen. David Perkins, this concept "allows U.S. forces to take advantage of existing personnel quality and training strengths to outmaneuver adversaries physically and cognitively, applying combined arms in and across all domains."⁴ In consonance with the MDB concept, on the one hand, the RMIB encourages new collection, exploitation, and analytical practices to enable special operations including lethal strikes, raids, and offensive cyber operations that underpin the Army's lethality.⁵ On the other hand, the RMIB conditions the Army and joint force for tailorable, distributable, and interdependent capabilities sets. These formations "package individuals and teams with associated equipment against identified mission requirements that span the spectrum of conflict and enable

a multi-echelon, joint, and/or multi-national response."⁶ Such capabilities sets constitute a useful operating paradigm to assist the Army's goal of projecting power across multiple domains to decisively defeat threats to America's national security and provide for global security.⁷

The remainder of this article unfolds in three parts. First, it canvasses the Army's periodic formation of ranger units to better position the significance of the Ranger Regiment and its new military intelligence battalion. The article next unpacks the RMIB and addresses its approach to collection, exploitation, and analysis in the interest of cross-pollinating practices to conventional forces that can help redress the Army's readiness gap. The article concludes by briefly introducing the RMIB's central contribution to the MDB concept referred to as capabilities sets.

"Rangers Lead the Way"

Employed by English foresters in the thirteenth century, the term "ranging" described the activity of patrolling to prevent poaching and protect against marauders.⁸ Colonial rebels including Col. Daniel Morgan and Francis Marion adopted ranging during the American Revolution to circumvent the British army's equipment, training, and personnel advantages. Col. Thomas Knowlton, who served for Gen. George Washington and is considered the first ranger intelligence officer, built a network of informants to enable ambushes and raids against the British. These irregular warfare tactics represented a key pillar of Washington's strategy to "wear away the resolution of the British by gradual, persistent action against the periphery of their armies."⁹ Beyond Britain's ignominious defeat in 1783, due partly to the unconventional practices of Washington's regular and partisan forces, Army leaders developed ranger units at key turning points in the service's history.

While both the Confederate and Union armies employed rangers during the American Civil War from 1861 to 1865, the Army did not constitute similar organizations until World War II. Gen. George C. Marshall, then chief of staff, modeled a unit after the British Commandos to gain combat experience prior to invading Europe. The activation of the 1st Ranger Battalion in June 1942 by Lt. Col. William O. Darby bookends the modern ranger era. Given its success during Operation Torch in North Africa in November 1942, Gen. Dwight D. Eisenhower instructed Darby to establish two additional battalions. "Darby's Rangers" combined with the 3rd and 4th Battalions to form the 6615th Ranger Force. Tragically, the 6615th Ranger Force was decimated in Italy at the Battle of Cisterna in January 1944.¹⁰ Five months later, the 2nd and 5th Battalions participated in the invasion

of Europe known as Operation Overlord. Historians credit the latter for crystallizing the 75th Ranger Regiment's motto, "Rangers lead the way," when the 29th Infantry Division assistant commander, Brig. Gen. Norman Cota, enjoined the 5th Rangers to lead the way off Omaha Beach amid stiff German resistance.¹¹

Whereas the Army also sanctioned the 6th Ranger Battalion in the Pacific, the 5307th Composite Unit (Provisional) was formed by Lt. Gen. Joseph "Vinegar" Stillwell in January 1944 to disrupt Japan's supply lines across the China-Burma-India theater. "Merrill's Marauders," named after unit commander Brig. Gen. Frank Merrill, was the only U.S. ground force in the theater. As such, Barbara Tuchman argues it "attracted a greater share of attention from the press and from history than a similarly sized unit merited anywhere else."¹² This includes a dramatized portrayal of its actions in a 1962 film, *Merrill's Marauders*, which some historians contend whitewashed the unit's mismanagement, culminating in the capture of Myitkyina Airfield in May 1944 at significant cost to the remaining and exhausted rangers.¹³ As "the strategic jewel of northern Burma," this airfield provided Japan a land-bridge between China and India.¹⁴ The Ranger battalions dissolved following Germany and Japan's capitulation in 1945 but appeared again during the Korean and Vietnam Wars.¹⁵ To this point, ranger units were episodically formed and ephemeral. They lacked hierarchy, did not share uniform training standards, and their use was largely informed by anecdote.¹⁶

Gen. Creighton Abrams reactivated the 1st and 2nd Ranger Battalions in 1974 during his tenure as chief of staff. He intended the battalions to rectify the Army's readiness shortfalls following the Vietnam War by imbuing heightened professionalism through performance-oriented training.¹⁷ The "Abrams Charter" envisaged these battalions "to be a role model for the Army" and compelled leaders trained in them to "return to the conventional Army to pass on their experience and expertise."¹⁸ Gen. John Wickam Jr. and Gen. Gordon Sullivan, who respectively served as the thirtieth and thirty-second chiefs of staff, codified Abrams's intent in their own charters. They further identified the 75th Ranger Regiment, its headquarters established in 1984 alongside the 3rd Ranger Battalion, as a key inflection point between conventional and special operations forces.¹⁹ The Ranger Regiment has since evolved to represent the U.S. military's most responsive forcible entry option.²⁰ It is postured to conduct platoon- to regiment-sized operations anywhere in the world within eighteen hours after notification. The regiment recently demonstrated its capability to seize en-

emy airfields, for example, in Afghanistan and Iraq. The addition of a military intelligence battalion constitutes the regiment's latest structural adjustment and is designed to ensure lethality amid an arguable shift in the character of war. This consists of enhanced precision across multiple domains enabled by a proliferation of sensors.

Introducing the 75th Ranger Regiment Military Intelligence Battalion

From 1984 to 2007, the Ranger Regiment bifurcated its intelligence training and operations between battalion intelligence sections and a military intelligence detachment attached to the regimental headquarters. Offset training and deployment cycles stymied the regimental intelligence officer's ability to synchronize multiple echelons of intelligence operations in support of the regimental commander's priority intelligence requirements. Establishment of a special troops battalion in 2007 consolidated a preponderance of the regiment's intelligence functions, personnel, and capabilities within a military intelligence company. Yet, activation of the battalion and company did not enhance managerial oversight of the regiment's intelligence training and operations as intended.²¹ At times, they exacerbated tension between the regimental intelligence officer's intent to standardize the recruitment and training of analysts and the battalions' interest in autonomy. This organizational challenge, coupled with several additional considerations, encouraged the regimental commander, then Col. Marcus Evans, to recommend that the United States Army Special Operations Command provisionally activate the RMIB.²²

First, the RMIB enables the regiment to better understand and operate in the cyber domain. Second, by providing broader mission command of the intelligence warfighting function, the RMIB accords the regimental commander greater flexibility to rapidly adjust analytical focus against emerging threats while integrating insights from current operations. Finally, the RMIB facilitates more consistent coordination with the U.S. Army's intelligence enterprise and its key institutions including the Intelligence Center of Excellence and the Intelligence and Security Command.

Pending approval from the Department of the Army, the RMIB will officially activate in 2019 under the leadership of a lieutenant colonel and a command sergeant major selected by a special mission unit board. The RMIB's mission is to recruit, train, develop, and employ highly trained and specialized rangers to conduct full-spectrum intelligence, surveillance, reconnaissance, cyber, and electronic warfare operations to enhance the regimental commander's situational awareness and inform his decision-making process.

THE RANGER CREED

Recognizing that I volunteered as a Ranger, fully knowing the hazards of my chosen profession, I will always endeavor to uphold the prestige, honor, and high esprit de corps of the Rangers.

Acknowledging the fact that a Ranger is a more elite soldier who arrives at the cutting edge of battle by land, sea, or air, I accept the fact that as a Ranger my country expects me to move further, faster, and fight harder than any other soldier.

Never shall I fail my comrades. I will always keep myself mentally alert, physically strong, and morally straight, and I will shoulder more than my share of the task, whatever it may be, one hundred percent and then some.

Gallantly will I show the world that I am a specially selected and well-trained soldier. My courtesy to superior officers, neatness of dress, and care of equipment shall set the example for others to follow.

Energetically will I meet the enemies of my country. I shall defeat them on the field of battle for I am better trained and will fight with all my might. Surrender is not a Ranger word. I will never leave a fallen comrade to fall into the hands of the enemy and under no circumstances will I ever embarrass my country.

Readily will I display the intestinal fortitude required to fight on to the Ranger objective and complete the mission though I be the lone survivor. Rangers lead the way!

Rangers Lead the way!



Key to the RMIB's mission is inculcation of the Ranger Regiment's standards-based culture codified in the Ranger Creed developed by the 1st Ranger Battalion in 1975. Adherence to this ethos, which emphasizes discipline, resilience, and learning, will enable the RMIB to balance technical and tactical competencies to engender trust and confidence across the ranger battalions, other special operations forces, and the Army's intelligence corps. This means assignment of intelligence personnel to the RMIB is contingent on passing the Ranger Assessment and Selection Program, which consists of an evaluation board for officers and noncommissioned officers.²³ Pending this certification process, RMIB personnel will complete the same training as combat arms soldiers assigned to the ranger battalions including the Army's Airborne and Ranger courses. When formally established, the RMIB will consist of three companies and maintain a personnel end-strength equivalent to a conventional intelligence battalion assigned to one of the Army's three active-duty expeditionary military intelligence brigades (see figure, page 26). Presently, the RMIB consists of a detachment and two companies.

The staff and command group are embedded within the Headquarters Detachment. It leads the regiment's recruitment and management of intelligence officers and soldiers, synchronizes intelligence training and operations across the regiment and with other special operations and conventional forces, and also functions as the regiment's intelligence section. This means the battalion commander also serves as the regimental intelligence officer, the battalion executive and operations officers serve as assistants, and all three deploy as the senior intelligence officers for a joint special operations task force. The military intelligence company, reappointed from the special troops battalion, is the cornerstone of the RMIB. It possesses the most personnel and capabilities across the battalion including all-source analysts, geospatial analysts, human intelligence collectors, and unmanned aircraft systems (UAS). This enables the company to conduct multidiscipline collection and all-source analysis, as well as provide an expeditionary imagery collection and processing, exploitation, and dissemination (PED) capability to enable the regiment's training and operations.

The cyber-electromagnetic activities (CEMA) company integrates and synchronizes cyber, electronic warfare, signals intelligence, and technical surveillance in support of the regimental commander's objectives. Personnel and capabilities resident to the CEMA company are normally disaggregated across multiple echelons and lack a coordinating agent. The CEMA company is therefore on the leading edge of fulfilling the Army's intent to establish a CEMA



Photo courtesy of the 75th Ranger Regiment

The Ranger Regiment command team prepares to unfurl the Regimental Military Intelligence Battalion colors 22 May 2017 during the battalion's activation ceremony at Fort Benning, Georgia.

capability within tactical formations.²⁴ As reflected by operations against the Islamic State (IS) in the Middle East and South Asia, it also advances the Army's ability to combine electronic warfare and signals intelligence in support of lethal targeting through unique technologies and tactics. The CEMA company's mission is enabled by consolidation of the regiment's electronic warfare, signals intelligence, and technical surveillance personnel and capabilities; introduction of cyber personnel; and broader partnerships with the Intelligence and Security Command, Cyber Command, and other special operations forces.

The Ranger Approach to the Intelligence Cycle

While designed to enable special operations, the RMIB's evolving approach to the intelligence cycle, consisting of collection, exploitation, and analysis steps, can help the Army overmatch near-peer competitors given the regiment's expanded interoperability with conventional forces. The article now explores the RMIB's innovative practices within each phase of the intelligence cycle.

Collection. The RMIB continues to innovate tactics, techniques, and procedures to accelerate the Army's ability to

find and fix enemy combatants. Training and operations against IS demonstrate several contributions to the Army's readiness. The military intelligence company recently experimented with a small UAS, the Puma, to provide platoon and company commanders, who are often dislocated from headquarters in austere terrain, timely and reliable full-motion video. Although applicable to the spectrum of operations, the Puma is particularly salient to forcible entry operations conducted by the regiment and other global response forces including the 82nd Airborne Division and 173rd Airborne Brigade.

The military intelligence company tested its ability to integrate two operators to parachute the Puma with ranger assaulters during an airfield seizure training scenario. The operators deployed the Puma ten minutes after landing and provided the ground force commander near instantaneous situational awareness of the terrain and enemy. Of course, the Puma is merely one solution, and more compact aircraft exist. The Puma provides ground force commanders greater range and longevity, however, making it the most advantageous tactical collection capability at this

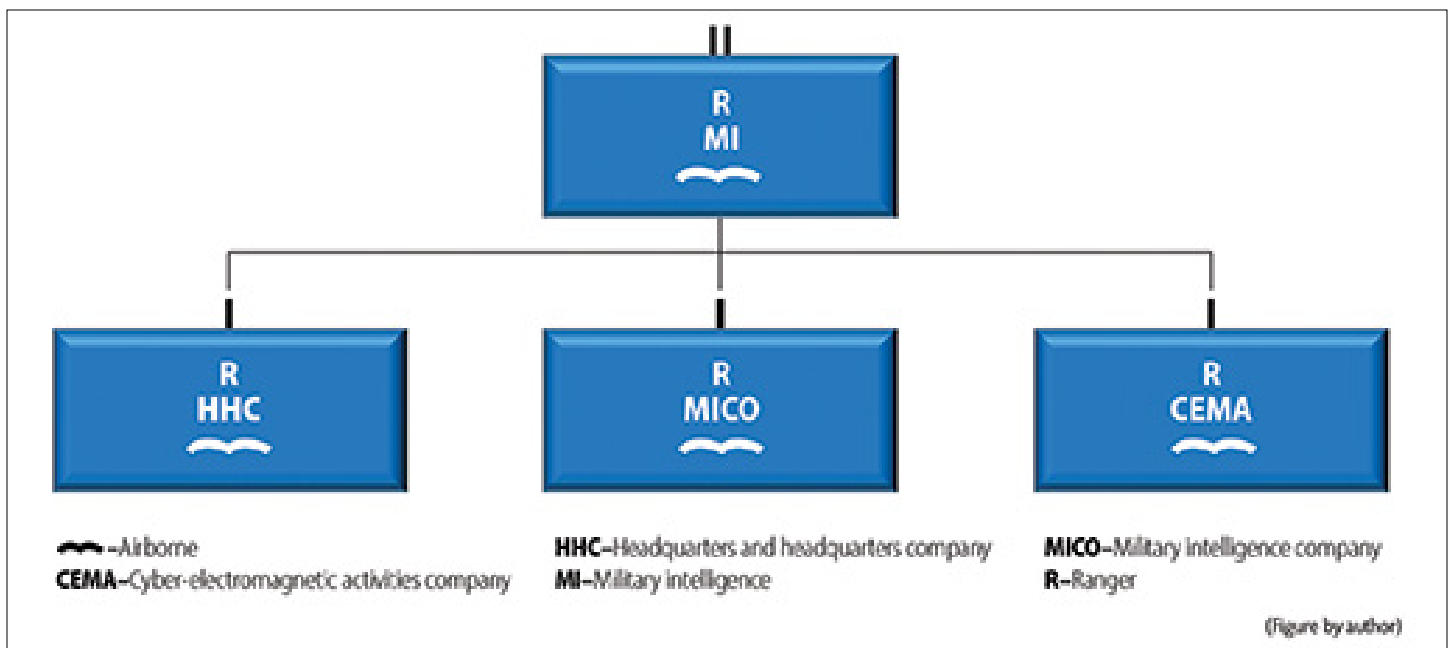


Figure. Simple Regimental Military Intelligence Battalion Task Organization

time according to testing. To facilitate similar training and operations across the Army, the military intelligence company is working with the Maneuver Center of Excellence to draft the doctrine that underpins employment of small UASs. The company has also developed an expeditionary PED capability integral to the employment of UAS resident to its UAS platoon. This advancement is designed to overcome a problem that threatens to malign Army PED cells. It is challenging to impart common understanding between mission commanders, aircraft operators, and geospatial analysts. The military intelligence company's PED capability consists of two geospatial analysts equipped with a portable system encompassing geospatial and analytical tools. Collocating geospatial analysts with the mission commander at a deployed site ensures they are aware of all mission events that provide critical context often not available. A conventional military intelligence company can adopt this practice given it also possesses a UAS platoon, has access to geospatial analysts, and will field expeditionary analysis systems.

The CEMA company also unifies disparate collection disciplines designed to operate in the electromagnetic spectrum. It exercises this capability by integrating cyber, electronic warfare, signals intelligence, and technical surveillance collectors into a special reconnaissance team. The team is capable of infiltrating hostile territory to enable sensitive collection, exploitation, and targeted operations against the enemy's computer and communications networks. The CEMA company recently enhanced the realism of a ranger battalion's airfield seizure exercise by replicating network configurations and communications protocols em-

ployed by near-peer competitors. The CEMA company also integrated its special reconnaissance team into the exercise. The team applied unique capabilities provided by national agencies to collect against the enemy's mission command systems and facilitated the ranger battalion's airborne operation. This training approach offers a useful framework for the Army's various combat training centers.²⁵

Exploitation. If intelligence drives the military decision-making process, then enrichment of data exploited from enemy material is decisive to the regiment's high-value targeting methodology known as "F3EAD"—find, fix, finish, exploit, analyze, and disseminate intelligence.²⁶ Experimentation with machine learning has enabled the RMIB to rapidly identify connections between seemingly disparate media devices, personalities, and their social networks. This advancement has reduced the time and labor required to wade through a meteoric rise in the volume of data confiscated during combat operations since 2001 and resulted in operations against "leverage points" central to insurgent and terrorist organizations including facilitators, financiers, and couriers.²⁷ Insights gained from these operations have enabled action against more serious threats to America's national security epitomized by the coalition airstrikes in northern Afghanistan in October 2016 that killed Faruq al-Qatani. As a senior al-Qaida official responsible for planning attacks against America, al-Qatani may have intended to disrupt the 2016 presidential election.²⁸

To further enrich data, the RMIB has integrated the exploitation of publicly available information into its all-source training and analysis. Although nascent, this practice



Two rangers from the military intelligence company deploy a Puma unmanned aircraft system in February 2016, providing a groundforce commander situational awareness during a training exercise in Dahlonaga, Georgia.

helped broaden the U.S. intelligence community's understanding of the lethality of IS's "Khorasan" branch defined by its ability to inspire, enable, and direct external attacks from Afghanistan. A 2016 attack on a German train by a seventeen-year-old Afghan asylum seeker resulting in five wounded passengers evidences this trend.²⁹ The digital footprint of America's near-peer competitors implies that the RMIB's integration of machine learning and publicly available information into exploitation operations is equally relevant to interstate conflict. Milley's identification of a readiness gap vis-à-vis the "Big Four" also means transference of the RMIB's exploitation operations to conventional forces can enable more rapid understanding and disruption of the enemy's decision-making cycle.³⁰

Arguably, it is the RMIB's integration of liaisons within key U.S. government departments and agencies, often referred to as the interagency, which stands to contribute the most to the Army's exploitation operations. The RMIB's representatives, immaterial of branch affiliation and ranging in rank from noncommissioned officers to warrant officers to company grade officers, are placed in agencies including the National Media Exploitation Cell and underline the regiment's network-based exploitation approach.

Proximity enables liaisons to build relationships that accord several dividends. First, liaisons gain access to data without which the regiment's understanding of the enemy's intent and capabilities would be disadvantaged. Liaisons also in-

fluence the interagency's exploitation priorities against the regiment's targeting lines of effort. In the best case, liaisons shepherd interagency coordination that, according to Joint Publication 1, *Doctrine for the Armed Forces of the United States*, "forges the vital link between the military and the diplomatic, informational, and economic instruments of national power."³¹ The ability of the RMIB's liaisons to articulate the impact of counterterrorism operations on the legitimacy of Afghanistan's government and regional security order-building contributed to justification of the coalition's continued assistance outlined in President Donald Trump's South Asia policy address in late August 2017.³²

Analysis. The RMIB's approach to talent management produces intelligence professionals that can confidently provide the regimental commander accurate and timely intelligence to turn his decisions into "yes" or "no" answers. It also enables ranger intelligence professionals to prudently justify or caution against lethal force. This competency derives from a disciplined approach to probabilistically assess the certainty of a target's location, critically evaluate a target's value to both enemy and friendly forces, project the risk to mission and force, and anticipate the impact to America's international standing.³³

The RMIB's talent management program, which balances the regiment's intelligence requirements against the interests of individual rangers, is based on two interrelated considerations. First, realistic training and

operational deployments allow the battalion commander and sergeant major to certify ranger intelligence professionals have mastered basic operations and intelligence planning frameworks. At times, ranger intelligence officers not previously obligated to serve in the combat arms will attend the Maneuver Captain's Career Course to gain a deeper appreciation for rigorously executing intelligence preparation of the battlefield lest a tactical scheme of maneuver fail to account for key considerations that result in casualties or mission failure. The course also emphasizes doctrinally sound language that maneuver commanders easily understand and imparts legitimacy. Second, unique and demanding training and assignments enable the RMIB to broaden the understanding and critical thinking skills of its personnel, especially its noncommissioned and warrant officers. Opportunities include liaison positions for all-source analysts and warrant officers, advanced technical training for human intelligence collectors, and interoperability training for signals intelligence collectors with other special operations forces.

The RMIB also capitalizes on the talents of soldiers across the reserve component to enable broader situational awareness and rigorous analysis critical to closing the Army's readiness gap. Similar to the Army's Intelligence Readiness Operations Capability, conceived as "supporting a forward element or a member of the intelligence community from a sanctuary location," the RMIB established the Ranger Intelligence Operations Center (RIOC).³⁴ The RIOC pivots on live-environment training. This expands the scope and audience of training management to include soldiers with less common occupation specialties that support intelligence operations, including analysts, teams, and capabilities. As a pillar of the integrated training environment, live-environment training through the RIOC also enables the Ranger Regiment's ongoing operations.³⁵ By integrating intelligence analysts from the reserve component, the RIOC has the added benefit of facilitating the Army's Total Force Policy. This is designed to organize, train, and equip the active-duty and reserve components as an integrated force.³⁶ The 335th Signal Command (Theater), responsible for providing cyber and signal units in support of the Third Army, Army Central Command, and homeland defense missions, recently invested ten U.S. Army Reserve analysts into the RIOC to meet annual training requirements while supporting the regiment's operational intelligence requirements.

Capabilities Sets: The RMIB's Contribution to Multi-Domain Battle


Although addressed discretely, the RMIB's innovative approaches to collection, exploitation, and analysis are the

constituent components of the intelligence cycle. They also undergird one promising way the RMIB can help enable the MDB concept: *capabilities sets*. The RMIB's understanding of the composition, disposition, and intent of capabilities sets derives from multifunctional teams that participated in counterinsurgency operations in Iraq and Afghanistan. These teams, consisting of multidiscipline collectors that gathered, exploited, and disseminated combat intelligence to tactical-level commanders, provided expertise to focus combat power as well as to sequence and synchronize lethal and nonlethal operations.³⁷

Capabilities sets, which couple collectors and analysts with requisite equipment, replicate the tailorable and distributable qualities of multifunctional teams. They provide for an expansion or decrement of capability based on shifts in the threat and the commander's priority intelligence requirements and objectives. By decentralizing personnel and resources, capabilities sets also maximize mission command, defined by Army Doctrine Publication 6-0, *Mission Command*, as "the exercise of authority and direction by the commander using mission orders to enable disciplined initiative within the commander's intent to empower agile and adaptive leaders."³⁸ In practice, capabilities sets are smaller-scaled forces, no greater than platoon size, that operate disassociated from headquarters for extended periods given broad guidance. In the case of a war against a near-peer competitor in the Indo-Asia-Pacific, for instance, commanders could establish various capabilities sets to conduct multidiscipline—cyber, human, imagery, and signals—intelligence collection, exploitation, and analysis to enable operations that outpace the enemy's ability to react.

The RMIB's capabilities sets provide two additional advantages essential to the MDB concept. First, they engender interoperability between conventional and special operations forces across all Army components. The RMIB's integration of the 335th Signal Command (Theater) into the RIOC sets the conditions to deploy reserve-component analysts in support of unique operational requirements. Second, the RMIB's capabilities sets enable joint and multinational interdependence. According to the former chief of naval operations, Adm. Jonathan Greenert, this "implies a stronger network of organizational ties, better pairing of capabilities at the system level, willingness to draw upon shared capabilities, and continuous information-sharing and coordination."³⁹ The RMIB's incorporation of analysts from the 17th Special Tactics Squadron, which provides the regiment tactical air controllers, represents movement toward broader joint force interdependence.⁴⁰ Meanwhile, the RMIB's exercises

with foreign militaries are important to set theaters of operations defined as having the necessary forces, bases, and agreements established to enable regional operations.⁴¹ Given broader interoperability within the Army, and more meaningful interdependence across the joint force and with allies and partners, capabilities sets promise to enhance a commander's situational awareness, preserve freedom of maneuver, and confront the enemy with multiple dilemmas. As a result, they may serve as a useful starting point to formulize the "multi-domain task force" envisioned by

Gen. Robert Brown, commander of the United States Army Pacific, and retired Gen. David Perkins, former commander of TRADOC.⁴² 

The author is indebted to several reviewers for their valuable comments and suggestions on earlier drafts of this article. These include Maj. Gen. Gary Johnston, Maj. Gen. Robert Walters, and Brig. Gen. Joseph Hartman; previous regimental and ranger battalion commanders including Col. Marcus Evans; former regimental intelligence officers including Col. Joshua Fulmer and Lt. Col. Bryan Hooper; and the Ranger Military Intelligence Battalion staff and company command teams, especially Sgt. Maj. Lee Garcia.

Notes

1. Capt. David Darling, email to the author, 5 November 2017. Gen. Mark Milley defined organizational readiness during a speech at the 2017 Captains Solarium symposium, attended by approximately one hundred captains, including Darling, drawn across all U.S. Army components; see also Rick Maze, "McCarthy Gets Tough on Army's Priorities," *Army Magazine* 67, no. 10 (October 2017), 11. Ryan D. McCarthy, former acting secretary of the Army, defines readiness as the ability to "put soldiers on a plane to immediately address a priority" and preparedness to "fight tomorrow."
2. Army Doctrine Publication (ADP) 1, *The Army* (Washington, DC: U.S. Government Publishing Office [GPO], September 2012), 1-8.
3. Ryan D. McCarthy and Mark A. Milley, "Modernization Priorities for the United States Army, October 2017, accessed 7 March 2018, <https://admin.govexec.com/media/untitled.pdf>.
4. David Perkins, "Multi-Domain Battle: Joint Combined Arms Concept for the 21st Century," Association of the United States Army, 14 November 2016, accessed 7 March 2018, <https://www.ausa.org/articles/multi-domain-battle-joint-combined-arms>.
5. Paul Lushenko and Anthony Williams, "Defeating the Islamic State: Reconciling Precision and Pressure High Value Targeting," *Counter Terrorist Trends and Analysis* 8, no. 9 (September 2016): 10.
6. Paul Lushenko, "Intellectualizing the U.S. Army's Rebalance Within Asia," U.S. Army Intelligence Center of Excellence, *Military Intelligence Professional Bulletin* 40, no. 3 (July-September 2014): 53.
7. U.S. Joint Chiefs of Staff, *The National Military Strategy of the United States of America* (Washington, DC: U.S. Joint Chiefs of Staff, June 2015), 7, accessed 21 March 2018, http://www.jcs.mil/Portals/36/Documents/Publications/2015_National_Military_Strategy.pdf.
8. Dominic J. Caraccilo, *Forging a Special Operations Force: The US Army Rangers* (West Midlands, UK: Helion, 2015), 19.
9. Russell Weigley, *The American Way of War* (New York: MacMillan, 1973), 15.
10. William O. Darby and William H. Baumer, *We Led the Way* (San Rafael, CA: Presidio Press, 1980), 156-70.
11. Caraccilo, *Forging a Special Operations Force*, 26.
12. Barbara Tuchman, *Stillwell and the American Experience in China 1911-1945* (New York: MacMillan, 1970), 432-33.
13. Gavin Mortimer, *Merrill's Marauders: The Untold Story of Unit Galahad and the Toughest Special Mission of World War II* (Minneapolis: Zenith Press, 2013).
14. Ibid., 28.
15. Ralph Puckett, *Ranger: A Soldier's Life* (Lexington, KY: The University of Kentucky Press, 2017); see also Michael Lanning, *Inside the LRRPs: Rangers in Vietnam* (New York: Ivy Books, 1988).
16. Ken Keen, "75th Ranger Regiment: Strategic Force for the 21st Century" (strategy research project, U.S. Army War College, 1998), 9, accessed 7 March 2018, <https://www.dtic.mil/get-tr-doc/pdf?AD=ADA341454>.
17. Caraccilo, *Forging a Special Operations Force*, 37-45.
18. Keen, "75th Ranger Regiment," 5.
19. Ibid., 6.
20. Joint Publication (JP) 3-18, *Joint Doctrine for Forcible Entry Operations* (Washington, DC: U.S. GPO, July 2001), I-1.
21. Caraccilo, *Forging a Special Operations Force*, 153.
22. Scott R. Gourley, "Interview: Col. Marcus S. Evans," Defense Media Network, 29 June 2017, accessed 7 March 2018, <https://www.defensemedianetwork.com/stories/interview-col-marcus-s-evans-75th-ranger-regiment-us-army-rangers/>.
23. The Ranger Assessment and Selection Program, or RASP, consists of two parallel courses. RASP 1 trains and assesses sergeants and below. RASP 2 trains and assesses staff sergeants and above. Small Unit Ranger Tactics, or SURT, is a mandatory course for members of the Ranger Regiment preparing to attend the U.S. Army Ranger School.
24. "Lessons Learned from Cyber Support to Corps and Below," *Journal of Asymmetric Warfare* 2, no. 2 (August 2017): 43; see also "US Army to Unleash New War Tactics, Now Cyber Soldiers Will Lead the Combat on Battlefield," India Times, 14 December 2017, accessed 7 March 2018, <https://www.indiatimes.com/news/world/us-army-to-unleash-new-war-tactics-now-cyber-soldierswill-lead-the-combat-on-battlefield-335597.html>. The closest approximation of the CEMA [cyber-electromagnetic activities] company is the

U.S. Army's Cyber Command's recent integration of cyber soldiers into the 3rd Brigade Combat Team with the 25th Infantry Division in Hawaii.

25. Maj. Matthew Sheftic, conversation with the author, 12 December 2017. Sheftic serves as a brigade combat team intelligence officer and previously served as an observer coach/trainer at the National Training Center in Fort Irwin, California.

26. John Hardy and Paul Lushenko, "The High Value of Targeting: A Conceptual Model for Using HVT against a Networked Enemy," *Defence Studies* 12, no. 3 (September 2012): 413–33.

27. Paul Lushenko, "Reconsidering the Theory and Practice of High Value Targeting," *Counter Terrorist Trends and Analysis* 7, no. 9 (August 2015): 23–30.

28. Ananya Roy, "Pentagon Confirms Death of Senior al-Qaeda Leader Faruq al-Qatani in Latest Strike in Afghanistan," *International Business Times*, 5 November 2016, accessed 7 March 2018, <https://www.ibtimes.co.uk/pentagon-confirms-death-senior-al-qaeda-leader-faruq-al-qatani-latest-strike-afghanistan-1589987>.

29. Kim Hjelmgard, "Islamic State Says It's Behind German Train Attack," *USA Today* (website), 19 July 2016, accessed 7 March 2018, <https://www.usatoday.com/story/news/world/2016/07/19/afghan-train-attacker-germany-had-islamic-state-flag/87279220/>.

30. J. M. Boyd, "Destruction and Creation" (unpublished manuscript, 1976).

31. JP 1, *Doctrine for the Armed Forces of the United States* (Washington, DC: U.S. GPO, March 2013), II-13.

32. Donald Trump, "Remarks by President Trump on the Strategy in Afghanistan and South Asia," White House website, 21 August 2017, accessed 27 March 2018, <https://www.whitehouse.gov/briefings-statements/remarks-president-trump-strategy-afghanistan-south-asia/>.

33. Philip E. Tetlock and Dan Gardner, *Super Forecasting: The Art and Science of Prediction* (New York: Broadway Books, 2015).

34. Brian Murphy, "The Evolution of Intelligence," *Army.mil*, 29 July 2013, accessed 7 March 2018, https://www.army.mil/article/108209/the_evolution_of_intelligence.

35. Paul Lushenko and David Hammerschmidt, "Back to the Future: Managing Training to 'Win in a Complex World,'" *Military Review* 95, no. 1 (January-February 2015): 55.

36. John M. McHugh, *Army Directive 2012-08 (Army Total Force Policy)*, 4 September 2012, accessed 7 March 2018, https://armypubs.army.mil/epubs/DR_pubs/DR_a/pdf/web/ad2012_08.pdf.

37. Lushenko, "Intellectualizing the U.S. Army's Rebalance within Asia," 55.

38. ADP 6-0, *Mission Command* (Washington, DC: U.S. GPO, May 2012), 1.

39. Jonathan Greenert, "Navy Perspective on Joint Force Interdependence," *Joint Force Quarterly* 76, no. 1 (2015): 11.

40. Craig Savage, "24th SOW Re-designates 17th ASOS," *Air Force Special Operations Command*, 28 August 2013, accessed 7 March 2018, <http://www.afsoc.af.mil/News/Article-Display/Article/495171/24th-sow-re-designates-17th-asos/>.

41. Vincent Brooks, "Rebalanced and Beyond," *Army Magazine* 64, no. 10 (October 2014), 108.

42. Robert B. Brown and David G. Perkins, "Multi-Domain Battle: Tonight, Tomorrow, and the Future Fight," *War on the Rocks*, 18 August 2017, accessed 7 March 2018, <https://warontherocks.com/2017/08/multi-domain-battle-tonight-tomorrow-and-the-future-fight/>.

MAJ Paul Lushenko, U.S. Army, is currently assigned to the Office of the Deputy Chief of Staff for Intelligence, G-2. He previously served as the operations officer for the Regimental Military Intelligence Battalion and has served at every echelon within the 75th Ranger Regiment. He is a distinguished honor graduate of the United States Military Academy, attended the Australian National University as a Rotary Ambassadorial Scholar where he earned an MA in international relations and a master of diplomacy degree, and recently graduated from the Naval War College with an MA in defense and strategic studies as the honor graduate. He has deployed multiple times to Iraq and Afghanistan with both conventional and special operations forces.



ATP 3-05.20, *Special Operations Intelligence*

by Captain Brandon Bragg

Photo by U.S. Air Force SSgt Kenneth W. Norman



U.S. Army Soldiers from the 7th Special Forces Group walk to a UH-60 Black Hawk during fast rope insertion and extraction training as part of Emerald Warrior at Hurlburt Field, FL, April 22, 2015.

Introduction

As members of the Profession of Arms, we all use doctrine in one way or another throughout our careers. We read it, refer to it, and follow it as guidance for how to conduct business in a garrison or combat environment. But do we ever *really* think about doctrine? What is it? Who writes it? What is the process to create it? We all know that doctrine guides the entire U.S. Army, down to specifics for each warfighting function, yet we rarely think about what is involved to develop it. We pretty much take it for granted.

First Assignment – Learn What You Don’t Know

Imagine you are a former infantry officer and recent graduate of the Military Intelligence Captains Career Course. Your first assignment as an intelligence officer is a nominative assignment to 1st Battalion, 3rd Special Forces Group (Airborne). When you arrive, you have 3 months to take command of your military intelligence detachment, complete your train-up, and deploy to Afghanistan to serve in the Special Operations Task Force as a collection manager and an intelligence planner. Sounds great, right? You’ve got a special operations assignment, a good unit with lots of history, great leaders, and an immediate combat deployment. Life is good for a young intelligence captain. The problem is, you don’t know anything about special operations forces. You’re hearing terms and acronyms that you don’t understand—RSM, AOB, and SOTF, to name a few. You don’t know what intelligence assets and architecture are going to be available or how you will use them throughout your military intelligence detachment. How do you learn about these things? And even more important, how do you learn about the things you don’t know that you don’t know? The answer is in the doctrine.

If you haven’t already guessed, the “you” in the vignette was me in 2015. After my key development time in 3rd Special Forces Group (Airborne), I moved to a broadening assignment as the G-2X for the U.S. Army John F. Kennedy Special Warfare Center and School. Aside from conducting special operations forces training for 18-, 37-, and 38-series military occupational specialties, the headquarters is also the Special Operations Center of Excellence, which is responsible for writing and maintaining all doctrine for special forces, psychological operations, and civil affairs. As an intelligence professional, I became involved in the revision of ATP 3-05.20, *Special Operations Intelligence*, and got an insider’s perspective on the doctrine writing process. I am now able to answer some of the questions from the vignette above by using my firsthand experiences, and more importantly, I can now explain the process of how ATP 3-05.20 was revised.

ATP 3-05.20, *Special Operations Intelligence*

ATP 3-05.20, *Special Operations Intelligence*, provides the U.S. Army special operations forces (ARSOF) commander and his staff “a broad understanding of intelligence support to, and the capabilities of, select ARSOF units to collect information and actionable intelligence. This publication also provides guidance for commanders who determine the force structure, budget, training, materiel, and operational

requirements needed to prepare organic military intelligence assets to conduct their missions.”¹ ATP 3-05.20 is immediately subordinate to FM 3-05, *Army Special Operations*, and is complemented by the following publications:

- ◆ ATP 3-05.40, *Special Operations Sustainment*.
- ◆ ATP 3-05.60, *Special Operations Communications System*.
- ◆ ATP 3-05.2, *Foreign Internal Defense*.
- ◆ ATP 3-05.68, *Special Operations Noncombatant Evacuation Operations*.

ATP 3-05.20 is informed by a host of other doctrine publications, including joint and Army intelligence, targeting, and operations publications, as well as observations, insights, lessons learned, and formal intelligence training, as shown in Figure 1 (next page). ATP 3-05.20 will also be consistent with, and logically linked to, the most recent FM 2-0, *Intelligence*, and ADP 2.0, *Intelligence*.

ATP 3-05.20 is an intelligence publication but is not within the hierarchy of FM 2-0, *Intelligence*; rather, it nests with FM 3-0, *Operations*, because ATP 3-05.20 addresses intelligence activities in special operations and is subordinate to FM 3-05, *Army Special Operations*. This relationship makes ATP 3-05.20 unique because its creation, publication, and revisions are from an operational intelligence perspective, thereby nesting the publication with other doctrine in the FM 3-0 family. Writing an intelligence publication with insight from both intelligence and operational doctrine, while classifying it under operations, helps to bridge the gap between the two doctrinal areas. This is particularly important in the special operations environment where constant integration between operations and intelligence is of utmost importance for mission success.

The revision process for ATP 3-05.20 started in January 2018 with approval and guidance from U.S. Army Training and Doctrine Command (TRADOC) to proceed with the revision. From that point, the planning process began and the initial staffing of the task was completed. The author of the publication developed a rough draft of ATP 3-05.20 between March and August 2018. The next step was to initiate a staffing process for the author’s draft, aided by input from across the ARSOF formation and a working group.

The Working Group

In November 2018, we formed a working group, bringing in subject matter experts from U.S. Army Special Operations Command (USASOC), 1st Special Forces Command, Army Special Operations Aviation Command, multiple special forces groups, 4th Psychological Operations Group, 95th Civil

What is Doctrine, Who Writes it, and What is the Process to Create it?

Doctrine is not a new concept, nor is it unique to the Army or the military. “The word doctrine, from the Latin word *doctrina*, means a body of teachings, instructions, or taught principles or positions, as in the body of teachings in a branch of knowledge or belief system.” In the Army, “doctrine is the body of professional knowledge that guides how Soldiers perform tasks related to the Army’s role: the employment of landpower in a distinctly American context.”² Simply stated, Army doctrine is the guidebook we use to accomplish the mission—whatever that may be. It is a guide to action, rather than fixed rules. Doctrine provides a common frame of reference across the military. It helps to standardize operations—facilitating readiness by establishing common ways of accomplishing military tasks.

The center of excellence for a specific discipline or warfighting function creates and manages doctrine for that discipline. The process of publishing new doctrine or revising existing doctrine is the responsibility of TRADOC. In general, developers follow the Army doctrine process, which consists of five phases—assessment, planning, development, publishing, and implementation. The process is continuous: once doctrine is published and implemented, the assessment may begin almost immediately, which starts the process again. According to TRADOC and Department of the Army guidance, the estimated timeframe for a full revision is 2,175 man-hours spread over 18 months. A new publication may take 2,756 man-hours over 23 months. Urgent revisions, based on guidance from TRADOC and Department of the Army, may take 1,015 man-hours over 7 months.³

Three types of Army doctrine exist, each with a different purpose in the hierarchy:

- ◆ Army doctrine publications, known as ADPs, contain the fundamental principles by which operating forces and elements of the generating force that directly support operations guide their actions in support of national objectives.
- ◆ Field manuals, known as FMs, contain an expansion of principles, tactics, procedures, and other doctrinal information.
- ◆ Army techniques publications, known as ATPs, such as ATP 3-05.20, *Special Operations Intelligence*, consist of techniques.⁴

Affairs Brigade, and 1st Special Forces Command Military Intelligence Battalion. The most important part of conducting an effective working group is having the right people in the room, and we were fortunate enough to get the right people from each unit to attend.

The organizer of the working group asked three key questions to guide the discussion:

- ◆ What are your commanders and their staffs looking for in this publication?
- ◆ What information about special operations intelligence would you want a new analyst to know?
- ◆ What techniques from your specific unit need to be included and shared with the ARSOF community?

The working group met for 4 days in November 2018; we

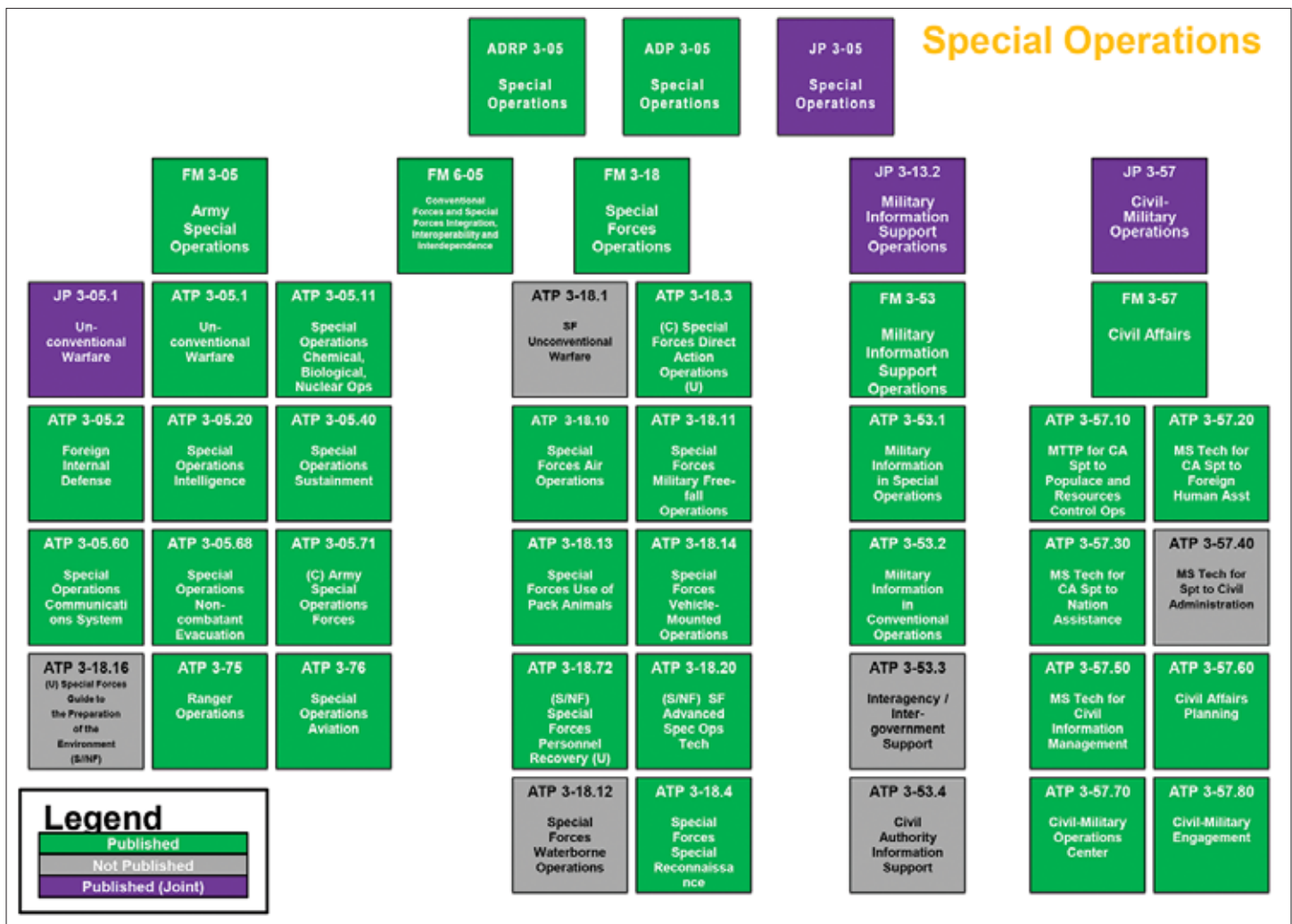


Figure 1. Doctrine Hierarchy for Special Operations⁵

sat together and reviewed the author's draft of ATP 3-05.20. We gave everyone a block of time to read a chapter, process their thoughts, and create notes and discussion points. This technique worked well because the information was fresh on everyone's mind at the time we discussed it and the discussion remained focused on a particular chapter. Participants shared many thoughts and insights—from how to best structure the manual, to wording that the author may have updated or changed. We discussed things from the macro level, all the way down to the micro level. As a result, we were able to provide the author with great notes and talking points.

The predominant outcome of the working group was a need to place emphasis on the publication's structure. Participants agreed that the chapter format should start with a broad overview of special operations forces intelligence, with every subsequent chapter going into a more detailed description of the particular mission sets and intelligence disciplines and methodology.

Additionally, a common, recurring theme was the term

"planning considerations." Since the objective of the publication is to provide commanders and their staffs with guidance on intelligence support to ARSOF missions, it became clear the publication needed to focus on those planning considerations that intelligence professionals and the commander's staff would use to advise the commander and allow him or her to make informed operational decisions.

The last major topic that resulted from the working group was a need for classified annexes. In order to provide valuable information on disciplines such as signals intelligence and human intelligence, the team decided additional annexes needed to be available on the SECRET Internet Protocol Router Network.

The Way Forward

After meeting with the author of ATP 3-05.20 and reviewing notes from the working group, we set a timeline for the future of the publication:

- ◆ Incorporate initial changes from the working group into the author's draft before the ARSOF Intelligence Training

and Readiness Working Group at Fort Huachuca, Arizona, in late January 2019, as well as the USASOC Military Intelligence Leaders Roundtable in February 2019.

- ◆ After the incorporation of all inputs, submit the document to the assigned editor to create an initial draft.
- ◆ Staff the initial draft within USASOC and specific external centers of excellence.
- ◆ Adjudicate comments received from the staffing process and submit them to the editor to develop a final draft.
- ◆ Staff the final draft across the Army. Staffing provides agencies and organizations the opportunity to provide input that will make the publication more relevant and useful. It is also an opportunity to gain consensus from as many organizations as possible.
- ◆ Adjudicate and finalize the last set of draft comments in late fiscal year 2019.
- ◆ Request that the Commanding General sign the completed publication.
- ◆ Send the signed publication to TRADOC and the Army Publishing Directorate to format for hard copy and electronic distribution.

In addition to these staffing techniques, we also created a Wiki page on the milSuite website. Acknowledging that techniques are constantly evolving, we decided it was important to keep ATP 3-05.20 “alive” throughout the process. By creating a Wiki page, we allow users (i.e., customers) of this publication—the ARSOF units—an opportunity to provide ongoing input and comments for review by the author. Not only will this assist in the publication of the 2019 version of ATP 3-05.20, but it will also greatly help the process of ensuring that every subsequent revision has the most up-to-date information, straight from the units.

Conclusion

The purpose of this article was not to emphasize the importance of doctrine—we already know that it is very

For access to the milWiki page for ATP 3-05.20, log on to https://www.milsuite.mil/wiki/Portal:Army_Special_Operations_Intelligence_Doctrine.

Your feedback is greatly appreciated.

milSuite is the Department of Defense (DoD) Enterprise Social Network, available to all members of the DoD workforce (common access login required). Any member of the milSuite community may access and edit milWiki, which is a knowledge management tool.

important. Instead, the goal was to make readers think about what doctrine is, who writes it, how the Army creates it, and how we can all individually have an impact on it during the development process. Doctrine publications are the guidelines that we, as professionals, use to inform our decision-making process—and input from end users is extremely valuable. Similarly, when a software company creates a video game or application (app), it sends it to potential users who become participants in the beta-testing group. Their feedback helps the software company make the game or app as perfect as possible for the widest group of users. So, the next time a doctrine publication comes through your inbox for staffing and community-wide comments, think of yourself as a lucky member of a beta-testing group who can influence the development of an important, widely used U.S. Army product. 🌟

Endnotes

1. Department of the Army, Army Techniques Publication 3-05.20, *Special Operations Intelligence* (Washington, DC: U.S. Government Publishing Office [GPO], 3 May 2013), v.
2. Department of the Army, Army Doctrine Publication (ADP) 1-01, *Doctrine Primer* (Washington, DC: U.S. GPO, 2 September 2014), 1-1–1-2.
3. Department of the Army, Training and Doctrine Command (TRADOC) Regulation 25-36, *The TRADOC Doctrine Publication Program* (Fort Eustis, VA: TRADOC, 21 May 2014).
4. Department of the Army, ADP 1-01, 2-5.
5. Department of the Army, *Doctrine Smart Book* (Washington, DC: U.S. GPO, 17 November 2016), 20.

CPT Brandon Bragg is the G-2X at the U.S. Army John F. Kennedy Special Warfare Center and School. He served as a battalion S-2 and military intelligence detachment commander for 1st Battalion, 3rd Special Forces Group (Airborne), and served as an infantry officer in 3rd Armored Brigade Combat Team, 3rd Infantry Division. In the Afghanistan and Africa areas of responsibility, he has experience at the levels of Special Operations Task Force, Theater Special Operations Command, and Special Operations Command Forward. He attended the Military Intelligence Captains Career Course.

“Understanding future warfare is the most important responsibility of those who must defend a nation from future enemies!”

—Major General Perry M. Smith



An Excerpt from ADRP 3-05, *Special Operations*

Chapter 5, Intelligence

Special Operations Intelligence Criteria

Special operations missions are both intelligence driven and intelligence-dependent. Intelligence products developed for [Army special operations forces] ARSOF must be detailed, accurate, relevant, and timely. For example, infiltrating a building in a nonpermissive noncombatant evacuation operation requires exact information on its structure and precise locations of hostages or persons to be rescued. National- and theater-level intelligence products are often required at a lower echelon than is normally associated with support to conventional forces. They may also require near-real-time dissemination to the operator level.

Special operations requirements are heavily mission- and situation-dependent largely driven by diverse and unique operational environments. The problems ARSOF are tasked to address are often not regional but trans-regional or global. Because ARSOF missions may vary widely, the associated intelligence support may also vary. Therefore, intelligence support for [special operations forces] SOF requires a thorough understanding of special operations requirements at the tactical level and integration of intelligence products from across the operational environments and geographic combatant commands. This causes national and theater support to be much more detailed and precise to support special operations requirements.

The following variables can affect intelligence support:

- ◆ Combat (hostile) or cooperative noncombat (permissive) environments.
- ◆ Multinational, combined, joint, or unilateral operations.
- ◆ Force composition.
- ◆ Maritime or land-based operations.
- ◆ Mission duration.
- ◆ Availability of mission command system elements and intelligence support facilities.
- ◆ Adversary capabilities, objectives, and operational concepts.
- ◆ Connectivity to agencies outside the operational environment.

Intelligence Criteria for Surgical Strike Missions

This set of criteria supports [counterterrorism] CT, [counterproliferation] CP, direct action, recovery operations, and [special reconnaissance] SR missions. Because SOF missions apply

direct military force to concentrate on attacking or collecting information on critical targets, the information required is highly perishable, requires near-real-time reporting, and often requires special handling to protect sources. Intelligence products are built to erase uncertainty before, during, and after execution.

SOF engaged in these missions depend on detailed and current target materials for mission planning and execution. SOF require extensive information from national, theater of operations, and SOF-specific threat installation and target assessment databases, files, studies, and open-access Internet information. SOF require current intelligence updates on targets and target changes from assignment of the mission through planning, rehearsal, execution, and poststrike evaluation. These requirements drive valuable resources, to include what has become known as the 'unblinking eye', constant imagery feeds of targets, key locations, and key actors.

Note: Open-source research pertains to electronic data that is publicly available without requiring an account, login, or other measures to access the information. Exploitation of Internet Web sites or social media that are not open-access should not be confused with open-source research. This type of exploitation will likely fall under other activities (intelligence or otherwise) and may include collection and acquisition of publically available information in cyberspace. These activities may include cyberspace operations, information operations, [military information support operations] MISO, special operations, information security, personnel security, disaster and humanitarian support operations, force protection, or criminal investigative authorities. Open-source intelligence is an intelligence discipline and may only be conducted by intelligence professionals because of the authorities and restrictions placed upon intelligence personnel in Executive Order 12333, *United States Intelligence Activities*, DOD 5240.1-R, *Procedures Governing the Activities of DOD Intelligence Components That Affect United States Persons*, Army Directive 2016-37, *U.S. Army Open-Source Intelligence Activities*, and AR 381-10, *U.S. Army Intelligence Activities*. See ATP 2-22.9/MCRP 2-10A.3, *Open-Source Intelligence (U)*, for details.

The basis for successful SOF mission planning is the target intelligence package normally developed by [theater special operations command] TSOC intelligence staff in coordination with the theater of operations [joint intelligence center] JIC or joint analysis center (United States European Command only). The information and intelligence necessary for the target intelligence package is gained by leveraging the intelligence

enterprise. Target intelligence packages must contain timely, detailed, tailored, and all-source intelligence describing the—

- ◆ Target description.
- ◆ Climate, geography, or hydrography.
- ◆ Demographic, cultural, political, and social features of the [joint special operations area] JSOA.
- ◆ Threat, including the strategy and force disposition of the military, paramilitary, or other indigenous forces, as well as any forces that endanger U.S. elements.
- ◆ Infiltration and exfiltration routes.
- ◆ Key target components, including lines of communication.
- ◆ Threat command, control, and communications.
- ◆ Threat information systems.
- ◆ Evasion and recovery information.

Current geospatial intelligence (imagery, imagery intelligence, and geospatial information) products of the target and [area of operations] AO are an important part of any target intelligence package. SOF elements in permission isolation use target intelligence packages as primary intelligence resources. The target intelligence packages help focus requests for information not covered or for data requiring further detail.

During all phases of these missions, SOF teams depend upon the timely reporting of detailed and highly perishable intelligence related to their operational situation. They also require rapid, real-time, or near-real-time receipt of threat warnings to enable them to react to changing situations and to ensure personnel protection. For example, in a recent operation, the executing direct action force did not have access to the real-time imagery being monitored by supporting ARSOF intelligence forces. The supporting force, despite being continental United States-based, was able to provide a warning of an incoming threat to the direct action force in near-real-time.

Teams conducting missions are primary providers of information that feeds the intelligence process for both SOF and conventional forces assigned to a theater of operations or joint operations area. Mission preparation requires that participants be aware of collection requirements and that procedures are established for reporting and dissemination.

Intelligence for Special Warfare


This set of criteria supports [unconventional warfare] UW, [foreign internal defense] FID, MISO, [Civil Affairs operations] CAO, and security assistance, as well as ARSOF involvement in humanitarian assistance and disaster-relief operations. Intelligence required to support indirect missions may be historical in nature and less perishable than that required for direct missions. The information may be unclassified, with much of it available in open-source formats. The emphasis is gen-

erally away from detailed, target-specific intelligence toward general military intelligence. Intelligence support focuses on leveraging the intelligence enterprise for social, economic, political, and psychological conditions within a targeted country or area to U.S. benefit. Developing and maintaining good rapport with [host nation] HN governments and indigenous population groups is essential to successful mission accomplishment. To establish rapport, ARSOF Soldiers require extensive knowledge of the local populace and its culture and language. Intelligence products are designed to allow the force to wade into uncertainty and prevail.

UW operations require extensive information on pre-existing, developing, and historical insurgent groups and their organization, location, and capabilities. UW also requires information on the presence and viability of subversive movements and military activity, as well as target-specific information. In addition, the information must describe the populace's likely response to government actions, thereby indicating the strength of potential local opposition to the foreign nation government.

ARSOF teams engaged in FID and foreign humanitarian assistance require detailed intelligence on the indigenous economic, military, social, and political structure and situation. Country or area studies are often invaluable sources of background information. Such studies encompass a wide range of topics covering all aspects of a country and its populace. However, they may be dated and require validation. Many country or area studies are unclassified and prepared using a variety of resources. They normally include text, imagery, and mapping data.

[Psychological Operations] PSYOP forces require access to open-access networks (such as public radio, television, newspapers, Internet) and the intelligence enterprise to assess the impact of all information activities. Requirements for MISO are often nontraditional (indigenous newspaper distribution figures, sentiments of local population to key communicators, and local media and advertising). The cultural intelligence section within PSYOP units provides ARSOF commanders useful military, sociological, psychological, and political information, as well as valuable demographic data. PSYOP forces rely heavily on operational variables (PMESII-PT) analyses to provide insight into the factors that drive population behavior.

Through area study, civil reconnaissance, and the execution of CAO, special operations [Civil Affairs] CA forces gather civil information on the PMESII-PT variables. Special operations CA elements conduct civil information management to develop, maintain, and fuse the civil common operational picture with the commander's common operational picture. Civil information management enables current operations tracking, future operations planning, and a holistic understanding of the operational environment. 

Countering Violent Extremist Organization High-Profile Attacks



Photo by U.S. Air Force TSgt Robert Cloys

by First Lieutenant Adria K. Penatzer

U.S. Air Force A1C Landon conducts preflight checks on an MQ-9 Reaper equipped with Gorgon Stare before a sortie on Kandahar Airfield, Afghanistan, Dec. 5, 2015.

Introduction

This article discusses how a special operations joint task force (JTF) developed an airborne intelligence, surveillance, and reconnaissance (A-ISR) collection strategy employing the Gorgon Stare capability to answer priority intelligence requirements¹ critical to countering violent extremist organization (VEO) high-profile attacks (HPAs).² It also provides an assessment of Gorgon Stare's initial 30 days of collection in theater by analyzing measures of performance³ and measures of effectiveness.⁴ The intent of the article is to capture lessons learned from the application of the Gorgon Stare capability to provide intelligence support to counterterrorism operations. And finally, the article provides recommendations for the future employment of the asset that are applicable in any theater of operation.

The JTF assessed that disruption of the VEO's support zone and HPA facilitation routes would have a significant impact on the network's ability to conduct HPAs. The JTF also assessed the best way to answer essential elements of information⁵ regarding the HPA facilitation network was to exploit observables of enemy activity in the form of logistical support trains. Following these logistical support trains would likely lead to the identification of VEO training camps, as well as staging areas for lethal material or HPA operatives being transported out of the VEO's support zone.

To execute this strategy, the JTF identified "collection anchor points" (CAPs),⁶ or ISR start points, by layering human intelligence, signals intelligence, theater and national collection, and geospatial analysis of terrain. These CAPs were initial locations of interest assessed to be associated with HPA training or facilitation. The JTF then employed the Gorgon Stare capability, conducting ISR follows from these static points of interest, specifically looking for indicators of logistical support activity to illuminate facilitation routes and compounds of interest actively in use by the enemy network. Focusing Gorgon Stare collection at these CAPs facilitated the confirmation or denial of enemy indicators,⁷ enabling fix/finish options at critical nodes within the VEO's HPA training and facilitation networks.

Information Collection Strategy Development

The JTF began development of its A-ISR collection strategy by building a threat model for HPAs. The intent of this exercise was to identify intelligence gaps regarding the HPA cycle. The identification of these intelligence gaps then drove the development of information requirements, and eventually specific collection requirements, necessary to interdict HPAs.

The threat model in Figure 1 on the next page illustrates a general outline of the HPA cycle, derived from tactical,

multiple “subviews,” with the intent to broadcast smaller fields of view for near-real-time PED, providing analysts with situational awareness over multiple geographically dispersed areas/compounds of interest. The Gorgon Stare processor can produce up to 48 subviews, depending upon the resolution requested and available bandwidth at the end-user level. Gorgon Stare also enables the end user to submit post-ingest exploitation requests for information to the continental United States-based PED cell, which is able to provide forensic tracks¹⁰ of persons and vehicles of interest throughout the WAMI field of view.¹¹

The JTF’s collection plan required static pattern of life collection to characterize CAPs and identify the arrival and departure of logistical resupply trains; it also required a dynamic collection capability to conduct follows. Whereas this strategy would typically require two A-ISR assets or one dual-sensor asset to execute effectively, the JTF was able to execute static and dynamic collection tasks with one Gorgon Stare-equipped ISR platform.

Gorgon Stare end of mission products also allowed the team to validate NAIs effectively by providing a record of arrivals and departures of vehicles and personnel at CAPs over time. This data assisted the team in identifying which CAPs to shelve from current collection priorities and which CAPs had a level of activity warranting nomination as official NAIs. Recorded and tracked over time, these metrics offered excellent inputs to measure the effectiveness of the collection strategy.

The post-ingest exploitation capability also provided the ability to conduct an unlimited number of forensic vehicle or personnel follows falling within the WAMI field of view, limited only by PED manpower available. Because targetable signatures of HPA training/facilitation activity can be fleeting in nature, it was essential to have the capability to record all activity in a 50 km² area throughout the course of the VUL, review the feed, and analyze activity of interest that may not have been observed in the full motion video (FMV).

Forensically tracking vehicles and personnel through the WAMI field of view, and fully leveraging the continental United States-based PED capability, illuminated facilitation routes actively in use by the VEO to a degree not previously observed in theater. Conducting follows to illuminate facilitation routes is not a novel concept; however, the ability to leverage the system architecture of Gorgon Stare was an unprecedented opportunity to map and record critical nodes in the VEO’s training and facilitation network. In particular, the opportunity to leverage the system included the geospatial intelligence data ingested and stored at the

ground-based Gorgon Stare archive manager and the provided PED manpower to analyze that data.

To tailor the collection strategy to effectively employ Gorgon Stare, the JTF grouped its priority CAPs into 50 km² WAAS orbits daily. The JTF then directed the creation of a WAAS subview over each CAP, requesting near-real-time callouts of vehicle or personnel arrivals and departures within each subview. These near-real-time callouts served to cue the platform’s FMV sensor to locations of interest and provide a record of activity of interest that may warrant a post-ingest exploitation request for information.



Photo by U.S. Air Force TSgt Robert Cloy

A1C Landon (left), 62nd Expeditionary Reconnaissance Squadron (ERS) aircraft specialist and A1C Tyler (right), 62nd ERS crew chief, perform preflight checks on an MQ-9 Reaper with Gorgon Stare for a sortie at Kandahar Airfield, Afghanistan, Dec. 5, 2015.

Measures of Performance and Measures of Effectiveness

Approaching the 30-day mark of the introduction of Gorgon Stare into theater, the JTF conducted an initial assessment of how well the asset had performed in theater and how effectively the asset had answered the JTF’s priority intelligence requirements relating to HPA training and facilitation networks.

The goal of this assessment was threefold:

- ◆ First, to determine the efficacy of Gorgon Stare sensors in observing threat indicators and supporting the counter-HPA collection strategy.
- ◆ Second, to analyze the intelligence value of Gorgon Stare’s post-ingest exploitation capability.
- ◆ Third, to provide an assessment of how successfully the team’s collection strategy developed the JTF’s understanding of HPA training and facilitation networks.

To achieve all three goals, the JTF divided measures of performance and measures of effectiveness into three categories: “sensor employment,” “post-ingest exploitation capability,” and “collection strategy.” The end state of this assessment was to produce a body of data supporting

recommendations to address any identified deficiencies in ISR performance or effectiveness.

Measures of Performance:

1. Sensor Employment

- 1.1. Tasked versus actual collection hours
- 1.2. Total FMV collection hours
- 1.3. Number of WAAS observations
- 1.4. WAMI quality

2. Post-Ingest Exploitation Capability

- 2.1. Request for information processing

3. Collection Strategy

- 3.1. Number of dynamic and forensic follows enabled
- 3.2. Utilization of the post-ingest exploitation capability

Measures of Effectiveness:

1. Sensor Employment

- 1.1. Special operations forces-specific tactics, techniques, and procedures validated

2. Post-Ingest Exploitation Capability

- 2.1. Intelligence value of post-ingest exploitation products received
- 2.2. Number of requests for information resulting in new CAP nomination

3. Collection Strategy

- 3.1. Number of follows resulting in new CAP nomination
- 3.2. Number of CAPs with WAAS collection
- 3.3. Number of NAIs validated
- 3.4. Number of precision pattern of life products generated

Measure of Performance and Measure of Effectiveness Summary

During 96.8 hours of collection over 11 missions with Gorgon Stare, the JTF collected on 28 different CAPs. This collection—

- ◆ Enabled the development of pattern of life products on seven NAIs.
- ◆ Confirmed four lethal aid facilitation routes.
- ◆ Identified one possible HPA training facility.
- ◆ Facilitated one structure strike.
- ◆ Provided critical intelligence supporting one human intelligence-triggered operation targeting an HPA high-value individual.

Gorgon Stare's unique technical features provided the opportunity to illuminate lethal aid facilitation networks; drive the find, fix, finish, exploit, analyze, and disseminate cycle; and potentially interdict imminent HPA threats. The JTF also validated Gorgon Stare's employment in support of special operations forces-specific tactics, techniques, and procedures, specifically validating Gorgon Stare's use in support of aerial strike operations, human intelligence operations, and signals intelligence operations.

Lessons Learned

The application of the Gorgon Stare capability provided lessons learned about intelligence support to counterterrorism operations. The three main lessons were—

- ◆ Prioritize quality over quantity of collection.
- ◆ Validate CAPs and NAIs.
- ◆ Dedicate analytical manpower to Gorgon Stare.

Prioritize Quality over Quantity of Collection. The JTF designated an average of 7 to 10 WAAS subviews per ISR mission. Through analysis of end of mission products and the feedback from the PED cell, the JTF determined that eight subviews is the optimal number per mission due to a few limiting factors.

First, if employing the asset for pattern of life development on multiple compounds of interest, more than eight subviews will limit FMV collection at each location. On days when the platform executed a complete VUL, the FMV sensor was usually only able to soak each CAP twice before the asset's return to base time. By minimizing the number of subviews per mission, this will increase the volume of FMV collection at locations of interest, allowing more detailed pattern of life development over fewer VULs.

Second, more than eight subviews can saturate near-real-time callouts, clouding the tactical end user's ability to determine to which activity of interest to slew FMV. When FMV collection is sporadic, it is usually not of a high enough volume for the end user to glean any intelligence value. In order to maximize the value of FMV collection, the JTF recommends prioritizing compounds of interest and maximizing daily subview nominations at eight.

Third, having more than eight subviews significantly stresses PED capacity and may prevent the end user from receiving near-real-time callouts and end of mission "chip-out" products. The end user may have to decide between receiving near-real-time callouts, which cue FMV for follows, or end of mission chip-out products, which track arrivals and departures at compounds of interest. If the end user requires both near-real-time callouts and chip-out products, the best practice is to limit subview nominations to eight.

Validate Collection Anchor Points and Named Areas of Interest. The JTF recommends developing a standard operating procedure for when to nominate CAPs for NAI status and when to shelve CAPs from collection priorities. A potential way forward is to determine the number of essential elements of information that must be observed within a specific number of collection hours in order for a location of interest to either retain CAP status, lose CAP status, or be nominated as an official NAI.


Dedicate Analytical Manpower to Gorgon Stare. Properly managing the Gorgon Stare capability and employing it in support of targeting is exceptionally time-intensive. The JTF recommends dedicating an analyst to effectively manage the asset, submit detailed and proper ISR tasking guidance, analyze the collected data, and package and disseminate derived intelligence to the broader community.

A dedicated analyst to this asset also enables the systematic tracking of measures of performance and measures of effectiveness, enabling regular reports that describe the measures of performance and measures of effectiveness. In order to constantly refine and improve information collection, the JTF recommends regularly conducting formative and summative assessments for measures of performance and measures of effectiveness. Formative assessments after each mission help to fine-tune requirements for the next mission. Summative assessments would ideally occur at 30-, 60-, and 90-day intervals to refine the employment of the capability.¹²

Conclusion

The Gorgon Stare capability clearly demonstrated the potential to effectively illuminate HPA training and facilitation networks, directly enabling efforts to interdict HPAs. However, the collection strategy themes presented here are applicable to any problem set. These themes are—

- ◆ Begin with a threat model.
- ◆ Identify intelligence gaps.
- ◆ Align collection capabilities with collection requirements.
- ◆ Conduct regular assessments of measures of performance and measures of effectiveness.

The captured lessons learned regarding the employment of the Gorgon Stare capability also hold value for other task forces that may employ Gorgon Stare in the future. 

Endnotes

1. “An intelligence requirement that the commander and staff need to understand the threat and other aspects of the operational environment.” Office of the Chairman of the Joint Chiefs of Staff, Joint Publication (JP) 2-01, *Joint and National Intelligence Support to Military Operations* (Washington, DC: U.S. Government Publishing Office [GPO], 5 July 2017), III-8.

2. For the purposes of this article, a high-profile attack is defined as any attack involving mass casualty producing tactics (person or vehicle-borne improvised explosive device, semi- or automatic weapon ambush in a crowded space, etc.) targeting noncombatants or host nation security personnel, usually in a major urban center. An effective high-profile attack usually results in non-insurgent casualties but is considered effective if it garners media attention for the violent extremist group that conducted the attack, regardless of how few casualties occurred.

3. “Represents a quantitative measure and answers two questions: whether the [intelligence, surveillance, and reconnaissance] ISR capability performed within technical standards and whether the planned collection was accomplished.” Office of the Chairman of the Joint Chiefs of Staff, JP 2-01, B-7.

4. “Represents a qualitative measure and answers whether the collection that was accomplished satisfied the requirement.” Ibid.

5. “The most critical information requirements regarding the adversary and the environment needed by the commander by a particular time to relate with other available information and intelligence in order to reach a logical decision.” Office of the Chairman of the Joint Chiefs of Staff, JP 2-0, *Joint Intelligence* (Washington, DC: U.S. GPO, 22 October 2013), I-8.

6. Although “collection anchor point” is not a joint or Service doctrinal term, the joint task force used the term to facilitate a shared understanding and labeling of ISR start points.

7. “An item of information which reflects the intention or capability of an adversary to adopt or reject a course of action.” Office of the Chairman of the Joint Chiefs of Staff, JP 2-0, GL-8.

8. “A geospatial area or systems node or link against which information that will satisfy a specific information requirement can be collected.” Office of the Chairman of the Joint Chiefs of Staff, JP 2-01.3, *Joint Intelligence Preparation of the Operational Environment* (Washington, DC: U.S. GPO, 21 May 2014), GL-7.

9. A VUL refers to the “vulnerability period” or the time aircraft are away from the base and vulnerable. It is the complete time an aircraft is airborne, also known as a “sortie.”

10. The movement of persons or vehicles of interest derived from reviewing wide area motion imagery after the ISR platform has landed and ingested data to the Ground Station Archive Manager. The continental United States-based Distributed Ground System-2 processing, exploitation, and dissemination cell can provide analysts stationed forward with these forensic tracks upon receipt of a request for information.

11. U.S. Air Forces Central Command, Reconnaissance Operations Center, *Gorgon Stare Increment 2* (April 2017).

12. Office of the Chairman of the Joint Chiefs of Staff, JP 2-01, B-9.

1LT Adria Penatzer is a student at the Maneuver Center of Excellence Captains Career Course. Previous assignments were targeting officer with the Military Intelligence Battalion, 75th Ranger Regiment, and tactical intelligence officer with the 16th Military Police Brigade. 1LT Penatzer graduated from the University of Virginia with two bachelor of arts degrees in foreign affairs-government and East Asian studies.



U.S. Army SSG Peter Yi, right, and U.S. Marine LCpl Kylie Curtis, left, speak to Chaluay Wijarat, second from left, at the Phitsanulok Train Station 6 February 2014 during a civil reconnaissance mission executed to assess their capabilities and disaster response plans during Exercise Cobra Gold 2014 in Phitsanulok, Kingdom of Thailand.

Reconnaissance Found: Redefining Army Special Operations Forces Integration

by Major Orlando N. Craig, Captain William P. Hurt, Captain Albert W. Oh,
and First Sergeant Christopher B. Melendez

In today's information age, we must recognize that the essential "key terrain" is the will of a host nation's population. This...permits us to gain the trust of skeptical populations, thus frustrating the enemy's efforts and suffocating their ideology.

—GEN James N. Mattis

Introduction

Chairman of the Joint Chiefs of Staff GEN Joseph F. Dunford, Jr., recently acknowledged, “While the fundamental nature of war has not changed, the pace of change and modern technology, coupled with shifts in the nature of geopolitical competition, have altered the character of war in the 21st century.”¹ The 2017 update to the *National Security Strategy* recognizes this shift in the international security environment, calling for a U.S. response to the propensity of America’s adversaries to operate “below the threshold of military conflict—challenging the United States, our allies, and our partners with hostile actions cloaked in deniability.”² This is further echoed in U.S. Special Operations Command’s (USSOCOM) *Special Operations Forces Operating Concept*, which provides an “actionable framework” to adapt to “an increasingly complex set of challenges...from the destabilizing influence of state aggression, to the expansion of radical networks across regions, to the growing threat of ubiquitous information warfare.”³

Whether framed as China’s unrestricted warfare, Russia’s Gerasimov Doctrine, Iranian asymmetric warfare, or any number of other terms used to characterize competitive maneuvers short of armed conflict, the future of U.S. national security will rest in our Nation’s ability to dynamically respond to these hybrid threats. As we pivot to embrace an operational environment in which the integration of warfighting capabilities is critical to maintain an advantage over our adversaries, we must understand that the U.S. military cannot act alone, and that all military and nonmilitary actions are “inseparable from their psychological effect.”⁴

The question remains of how to apply USSOCOM’s actionable framework in a manner that embraces all levers of foreign policy yet specifies guidelines for Army special operations forces’ (ARSOF) input along the continuum of competition. The discussion in this article focuses on two areas:

- ◆ Conduct of ARSOF in 21st century warfare.
- ◆ Use of special operations civil affairs teams as the reconnaissance arm of a special operations forces (SOF) “combined arms” approach to the human/information domain.

21st Century Security Environment: An Uncertain Future

A recent U.S. Army Special Operations Command (USASOC) white paper defined political warfare as a “spectrum of activities associated with diplomatic and economic engagement, Security Sector Assistance (SSA), novel forms of Unconventional Warfare (UW), and Information and Influence Activities (IIA).”⁵ Army special forces maintain

the lead on unconventional warfare and its associated activities, while psychological operations forces have distinguished their capabilities in the realm of information and influence. While the psychological operations regiment’s value-added to the asymmetric fight is indisputable, to label them as the sole proprietors of influence is a misunderstanding of the application of SOF solutions. By its very nature, SOF is a human endeavor—in accordance with what are commonly known as the SOF Truths, all subcomponents of USSOCOM should ultimately seek to understand, influence, and transition their environment to another partner within the joint, interagency, intergovernmental, and multinational environment. Within this construct, it is ever important to delineate the division of labor required not only to achieve success but also to amplify the proprietary effects each ARSOF branch brings to the continuum of competition.

The most recent update to FM 2-0, *Intelligence*, nests the intelligence warfighting function into the greater framework of FM 3-0, *Operations*, with respect to the changing strategic landscape. On ADP 2-0, *Intelligence*, Commanding General, U.S. Army Intelligence Center of Excellence, MG Robert Walters, Jr., remarked “[it] provides a common construct for intelligence support in complex operational environments and a framework to support unified land operations across the range of military operations.”⁶ With regard to the complex operational environment, the concept of “fighting for intelligence” presents one of the most significant challenges to the Army, largely due to the fact that “activities in the information environment will often be inseparable from ground operations.”⁷

The gap between collecting valuable contextual information and providing clear inputs into the intelligence process is not a new dilemma for the U.S. military—if anything, the last 17 years of war present a cautionary tale of focusing too hard on facilitating lethal targeting cycles.⁸ In a 2017 article published through the Modern War Institute, Dr. Nicholas Krohley remarked, “if no one at the tactical level is looking beyond the immediate demands of the targeting process to collect substantive and meaningful contextual detail on the enemy, then that information will never enter the intelligence process. Instead, it will be left to others (who lack direct access) to invent narratives that ascribe meaning to our network targeting packages and quantitative data sets.”⁹ This presents a formidable challenge to our ability to outmaneuver our adversaries, particularly in low-intensity conflict environments where precision targeting and direct action operations are not feasible solutions.

Understanding the operational environment is a Herculean effort that requires intense study and practiced patience,

items not well suited to the Army's tactical requirements but ever necessary for the continued operational success of small SOF teams. The operational environment is not a motionless set of features to describe but rather a dynamic, ever-changing interaction of individual agency, physical geography, and human biology—an increasingly complex adaptive system in the changing character of warfare. Its depth and breadth are captured in its doctrinal definition as “a composite of the conditions, circumstances, and influences that affect the employment of capabilities and bear on the decisions of the commander.”¹⁰

Understanding commences with analysis, and analysis starts with reconnaissance—a focused study of one's surroundings, whether zone, route, area, or civilian. Civil reconnaissance is the most basic form required for all subsequent actions within the realm of human interaction. Its execution far surpasses tangible and observable aspects of a society such as language, style of dress, or customary behavior. Effective, valuable civil reconnaissance demands its practitioner to ask probing questions, weigh competing interests, and assess the intangible, unspoken elements of a culture or conversation. It is a nuanced endeavor that demands a nuanced yet bold approach.

Civil Reconnaissance Misunderstood: A Problem of Our Own Making

To operate across the spectrum of multi-domain conflict requires a unique understanding of the environment and how the actors interact. In the book *Military Strategy in the 21st Century: People, Connectivity, and Competition*, it is observed that “the US national security community must reorient how they think about power and influence in the twenty-first century and embrace a view of the world as a series of interconnected networks.”¹¹ As defined, the functions of civil reconnaissance and civil engagement that nest under the core competency of civil affairs activities directly support this perspective and the states and sub-elements of the competition continuum defined by the 2018 *Joint Concept for Integrated Campaigning*. This forms the basis to why civil affairs is uniquely suited for this environment.

The problem with civil reconnaissance is that it is widely misunderstood and subsequently misapplied. It has become a near-meaningless byword for moving through a given community, observing some phenomena tangentially interesting to civil affairs (or SOF), summarizing said phenomena via storyboards and situation reports, and then hoping that someone within the interagency would find the

information valuable. Earlier versions of civil affairs doctrine described civil reconnaissance as a supporting task under the core civil affairs task of civil information management, a feature that obscured the reason behind civil reconnaissance collection efforts. The 2018 version of the doctrine captures civil reconnaissance as one of five functions of civil affairs activities, as well as a tactical mission task. Civil reconnaissance is defined as, “a targeted, planned, and coordinated observation and evaluation of specific civil aspects of the environment,” driven by a civil information collection plan.¹² This simple revision in terminology serves to instill a culture of human terrain “scouts” who are mission-focused in their collection efforts, as opposed to the traditional im-

Civil reconnaissance is a targeted, planned, and coordinated observation and evaluation of specific civil aspects of the environment.

age of civil affairs as passive database managers or distributors of humanitarian assistance. Rather than the supporting role, one can argue that civil reconnaissance

is actually the sine qua non of civil affairs; a civil affairs Soldier who does not perform civil reconnaissance is not actually “doing” civil affairs in the best or most important sense of the term.

A historical misunderstanding of civil reconnaissance has resulted in ad hoc success for the civil affairs regiment—a matter of right time, right place, and right person. Short-term efforts proved necessary in the past, but the regiment is poised to develop a rich and doctrinally sound understanding of this critical task. The 95th Civil Affairs Brigade has made civil reconnaissance a mission-essential task at the battalion and company levels, thus empowering leaders to search, understand, and apply Objective-Task metrics to this often misunderstood and ill-defined task.

Evolving doctrine and new terms are necessary components of civil affairs' transformation, but members of the regiment are finding their efforts fade into irrelevance in an age in which strategic-level guidance places a high priority on understanding the human aspects of competitive spaces and bolstering partners against coercion. As the Department of Defense (DoD) defines their role to the whole-of-government approach in generating solutions to this problem set, civil affairs forces and their hard-earned lessons operating in this domain are in danger of being left behind. The authors contend that the regiment's ability to find new truths in old doctrine and redefine our role in ARSOF's future will lend legitimacy to a process that has historically been difficult to define to conventional and SOF brethren alike. A cursory review of reconnaissance doctrine reveals a systematic approach, outlining its purpose, fundamentals, methods,

engagement criteria, techniques, and forms.¹³ When applied to civil reconnaissance, these concepts would sharpen our current processes, breathing new life into what has become business as usual.

Army Special Operations Forces' Scouts—Civil Reconnaissance Out Front

It is not happenstance that U.S. Embassy country teams, host nation militaries, and many civil society organizations widely welcome SOF civil affairs teams. As described by USASOC, SOF personnel are specifically trained to “catalyze and sustain whole-of-government initiatives,”¹⁴ providing U.S. policymakers a menu of options based on a “blending of capabilities between the DoD and the interagency.”¹⁵ Unique training opportunities in language, cultural, and U.S. interagency skills enable ARSOF operators to engage at various levels of local, national, and U.S. Government—a necessary capability in order to achieve effects in a future operating environment that requires a whole-of-government approach.

The *USASOC Strategy-2035* highlights the pressing need to “prevent and mitigate threats,” facilitated by early detection and understanding to provide leaders “adequate decision space necessary to develop policies and plans that counter adversarial actions.”¹⁶ Within this construct, the civil affairs team, through indigenous and interagency partnerships, is uniquely suited to conduct civil reconnaissance to increase understanding of the operational environment and provide commanders with discrete, scalable, and proactive options to evolving problem sets. The execution of civil reconnaissance requires commander-driven information requirements and a deliberate approach; the training of civil reconnaissance should be no different. In the future of multi-domain operations, civil affairs elements provide critical intelligence, surveillance, and reconnaissance assets with regard to the human domain.

It is important to illustrate the difference between civil information collection and information collection with respect to intelligence analysis. According to the September 2018 update to ADP 2-0, *Intelligence*, information collection involves synchronizing and integrating the planning and employment of sensors, which can be conducted by “nonintelligence sources, which provide civil considerations and sociocultural information.”¹⁷ Within the scope of information collection, reconnaissance is a primary task typically conducted to collect information on geographic terrain, the enemy, or other operational or mission variable deemed to be important for a commander to formulate, confirm, or modify a course of action.¹⁸ If the “terrain” within the

human domain is represented by ideas and narratives, forces working within the human domain must seek different means of analyzing cognitive objectives, obstacles, and key terrain.¹⁹ The ability of the civil affairs team to maneuver within the narrative space, gain and maintain contact with key nodes, and provide early warning and detection of emerging threats is key to the success of the USSOCOM framework in providing the decision space necessary for our civilian leaders to generate policy options.

Reconnaissance doctrine finds its *raison d'être* in answering information requirements during the information collection process, as well as supporting targeting requirements by conducting target acquisition and surveillance. Just as scouts are tasked with information requirements and named areas of interest, civil affairs elements must prioritize their information collection efforts (i.e., orient on the reconnaissance objective) along the lines of the commander's priority intelligence requirements for their respective area of responsibility. Orienting on the reconnaissance objective also implies that civil affairs forces are receiving constant feedback from the commander and his staff, who provide guidance on information collection efforts and on whether to adjust civil affairs engagement criteria. This continuous loop of communication provides intelligence assets with an updated civil common operational picture, which in turn drives new information requirements, target reprioritization, and operational decisions. Used in a similar manner as traditional intelligence, surveillance, and reconnaissance platforms, civil affairs teams can use nonlethal operations, activities, and actions to provide a “purpose for presence” in named areas of interest to gather civil information, thereby addressing information requirements and enhancing situational understanding of the operational environment.

In accordance with the fundamentals of reconnaissance, once a reconnaissance unit gains contact with the threat, it must maintain contact unless the survival of the unit is at risk or the supported commander orders otherwise. Applied to civil reconnaissance, the “threat” is represented by the zone, area, or point of interest that addresses the commander's information requirements. By this logic, the civil reconnaissance force must gain and maintain contact through episodic engagements until the survival of the unit is at risk—in the case of a civil affairs team, until the mission is at risk of being compromised. Reconnaissance elements always consider engagement and disengagement criteria as a planning factor. This caveat should remind civil affairs forces of what they are not. “Going native” refers to the broader concern of mission creep: adopting the objectives of other U.S. or host nation interagency efforts at the

expense of one's own. Lacking clear command guidance and operational understanding, civil affairs teams have been vulnerable to compromising their mission in favor of another effort. To follow the analogy, civil affairs teams should "break contact" when they assess their own mission is at risk. In order to do so, civil affairs teams should avoid agreeing to long-term commitments or rushing to a decision to cooperate with a specific implementing partner.

Internally, this fundamental compels civil affairs to remain threat/target-oriented. Externally, it provides supported commanders with a theory of action to maximize the effectiveness of an already scarce resource (i.e., civil affairs teams). The extent to which a civil affairs team should engage a specific threat/target also highlights another fundamental of reconnaissance—to retain freedom of maneuver. By ensuring elements do not become decisively engaged, they maintain the freedom to continue mapping networks and gathering information for branches and sequels to current plans.

Civil affairs operations enable the observation, understanding, and manipulation of the operational environment through an indigenous approach by overt development of local, organic networks. These friendly networks enable U.S. forces to detect threats and prioritize efforts with appropriate responses. Since all cross-functional special operations teams must move and live within the partner nation's human terrain, understanding is an especially critical force protection factor. Furthermore, the ability to operate effectively requires influence. Responsible influence demands forethought and understanding—items inherently at odds with hasty activity in the operational environment. In order to maximize freedom of maneuver for military commanders, SOF must synchronize their individual capabilities to effectively shape, influence, or manipulate the operational environment.

Way Ahead for Special Operations Forces Civil Affairs

In the 21st century security environment, USSOCOM will be a critical asset in the great power competition. Although widely regarded as the "tip of the spear" over the last 17 years engaged in the Global War on Terrorism, recent events concerning SOF deployed to Africa and South America

have caused concern among members of Congress. For example, House Armed Services Committee Chairman Mac Thornberry said last year that he was worried about the "overuse of SOF."²⁰ In a December 2018 Congressional hearing, LTG Rich Clarke, current Director for Strategic Plans and Policy, Joint Staff (J5) and next in line to take command of USSOCOM, cited the recently updated National Defense Strategy in the Pentagon's intensive review of USSOCOM's roles and missions in an attempt to "alleviate the organizational and personal stress the force is under."²¹ While a high operational tempo is difficult to sustain, a misconstrued relationship exists between the operational capabilities afforded SOF through their "arduous assessment and selection processes" and the "missions of outsize responsibility" with which they are tasked.²² SOF elements can achieve tremendous effects in the information and influence domain under a relatively low budget, with a diverse array of capabilities and solutions for interagency and conventional military leaders.

The demand signal for the actionable framework proposed by USSOCOM forces has rung clear in the wake of the future of our national security in great power competition. One of the major hindrances to the proper framing


The future operating environment will present challenges that demand ARSOF to be adaptive, flexible, rapidly responsive, and capable of succeeding in ambiguous circumstances. Through deliberate effort, ARSOF will adapt operationally and institutionally to ensure the effectiveness of the force remains without equal for decades into the future.

—USASOC Strategy-2035

of intelligence problems is a lack of situational or contextual understanding to properly shape the commander's intent.²³ With regard to information collection, intelligence doctrine clearly delineates information collection as a supporting effort to the

production of intelligence. Information collection, as an intelligence warfighting function task, can and should include SOF civil affairs forces operating in the human domain.²⁴ As a task, information collection nests neatly into the intelligence process under the Collect and Process phase; it is only when collected information is provided to the appropriate processing elements under the relevant authorities that it can be analyzed as intelligence. Civil reconnaissance specifically addresses the contextual information gaps that often inhibit the ability of the U.S. military commander to effectively visualize and describe the operational environment in order to direct, lead, and assess military operations.²⁵

Civil reconnaissance serves as the essential first step in crafting priorities and tactical actions. Commanders who can visualize the battlefield accurately can design and

implement efforts that counter malign actors' activities within the area of operations, protect a vulnerable population, and strengthen the supported governance institution. As we progress toward the USASOC Strategy-2035 model of a cross-functional organization, it is important to highlight how the separate branches complement the capabilities of each other. Looking toward the future—a complex operational environment of competing influence forces and threats to stability in gray zones—it becomes more important than ever to recognize the potential for civil affairs to enrich targeting processes and systems, and to enable more careful planning. In today's multi-domain battlefield, adversaries seek to wield various methods of influence in order to undermine American security.²⁶ Though the methods of these efforts vary—misinformation, resource control, political repression, coercion, or violence—the aim remains to gain access to the politically relevant segments of the population and their resources. To this end, it is more important than ever for the SOF to present the “right balanced portfolio of capabilities” for our Nation to successfully shape the competition environment and deter future threats to national security.²⁷ 

Epigraph

Barak A. Salmoni and Paula Holmes-Eber, with a foreword by GEN James N. Mattis, *Operational Culture for the Warfighter: Principles and Applications* (Quantico, VA: Marine Corps University Press, 2008), vii.

Endnotes

1. GEN Joseph F. Dunford, Jr., “The Character of War and Strategic Landscape Have Changed,” *Joint Force Quarterly* 89 (2nd Quarter 2018): 2, <https://ndupress.ndu.edu/Media/News/News-Article-View/Article/1491632/from-the-chairman-the-character-of-war-and-strategic-landscape-have-changed/>.
2. U.S. White House, *National Security Strategy of the United States of America* (Washington, DC: December 2017), 3.
3. U.S. Special Operations Command, *Special Operations Forces Operating Concept* (Directorate of Force Management and Development, Concept Development and Integration Office, 1 February 2016), 1.
4. U.S. Joint Chiefs of Staff, *Joint Concept for Integrated Campaigning* (16 March 2018), 16.
5. U.S. Army Special Operations Command, *SOF Support to Political Warfare White Paper* (10 March 2015), 2.
6. Department of the Army, Army Doctrine Publication (ADP) 2-0, *Intelligence* (Washington, DC: U.S. Government Publishing Office [GPO], 4 September 2018), foreword.
7. Department of the Army, Field Manual (FM) 2-0, *Intelligence* (Washington, DC: U.S. GPO, 6 July 2018), 6-1.

8. Zachery Tyson Brown, “A Cult of Lethality?” *The Strategy Bridge*, December 14, 2018, <https://thestrategybridge.org/the-bridge/2018/12/14/a-cult-of-lethality>.
9. Nicholas Krohley, “The Intelligence Cycle is Broken. Here’s How to Fix It,” *Modern War Institute at West Point*, October 24, 2017, <https://mwi.usma.edu/intelligence-cycle-broken-heres-fix/>.
10. Office of the Chairman of the Joint Chiefs of Staff, *DOD Dictionary of Military and Associated Terms* (Washington, DC: The Joint Staff, January 2019), 175.
11. Charles Cleveland, Benjamin Jensen, Susan Bryant, and Arnel David, *Military Strategy in the 21st Century: People, Connectivity, and Competition* (Amherst, NY: Cambria Press, 2018).
12. Office of the Chairman of the Joint Chiefs of Staff, Joint Publication 3-57, *Civil-Military Operations* (Washington, DC: The Joint Staff, 9 July 2018), C-7.
13. Department of the Army, Army Techniques Publication 3-20.98, *Reconnaissance Platoon* (Washington, DC: U.S. GPO, 5 April 2013).
14. U.S. Army Special Operations Command, *SOF Support*, 28.
15. U.S. Army Special Operations Command, *ARSOF Operating Concept 2022* (Fort Bragg, NC: 26 September 2014), 14.
16. U.S. Army Special Operations Command, *USASOC Strategy-2035* (April 2016), 4.
17. Department of the Army, ADP 2-0, *Intelligence*, 5-4.
18. Department of the Army, FM 3-0, *Operations* (Washington, DC: U.S. GPO, 6 October 2017), 2-41. Change 1 was issued on 6 December 2017.
19. BG Charles L. Moore, Jr., et al., [Strategic Multilayer Assessment] *SMA White Paper, Maneuver and Engagement in the Narrative Space* (January 2016), 14-15.
20. Katie B. Williams, “Lawmakers Probe Role of Special Operations in Great Power Competition,” *Defense One*, December 4, 2018, <https://www.defenseone.com/politics/2018/12/lawmakers-probe-role-special-operations-great-power-competition/153274/>.
21. Sean D. Naylor, “Special Operations Boom Years May Be Coming to a Close,” *Yahoo! News*, September 13, 2018, <https://www.yahoo.com/news/special-operations-boom-years-may-coming-close-090019994.html/>.
22. Ibid.
23. Jason M. Brown, “Strategy for Intelligence, Surveillance, and Reconnaissance,” *Joint Force Quarterly* 72 (1st Quarter 2014): 42, https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-72/jfq-72_39-46_Brown.pdf.
24. Department of the Army, ADP 2-0, *Intelligence*, 2-2.
25. Department of the Army, ADP 5-0, *The Operations Process* (Washington, DC: U.S. GPO, 17 May 2012).
26. Chad M. Pillai, “The Dark Arts: Application of Special Operations in Joint Strategic and Operational Plans,” *Small Wars Journal*, June 8, 2018, <http://smallwarsjournal.com/jrnl/art/dark-arts-application-special-operations-joint-strategic-and-operational-plans/>.
27. U.S. Army Special Operations Command, *USASOC Strategy*, 7.

MAJ Orlando Craig is serving as Commander, F Company, 98th Civil Affairs Battalion (Special Operations) (Airborne). He is a civil affairs officer who recently returned from a deployment in support of Theater Special Operations Command South. He is a graduate of the U.S. Army Command and General Staff College. He also has a master's of military art and sciences in strategic studies and a master of science in engineering management from the Missouri Institute of Science and Technology. He has conducted research into the effectiveness of engineering civic assistance projects in achieving U.S. national security objectives in the U.S. Africa Command, U.S. Southern Command, and U.S. Indo-Pacific Command areas of responsibility.

CPT William Hurt is executive officer to the foreign policy advisor of U.S. Army Special Operations Command (Airborne). He has served in several infantry assignments. Most recently, he conducted two civil affairs rotations as a team leader in B Company, 98th Civil Affairs Battalion (Airborne), and subsequently served as Commander for Headquarters and Headquarters Company, 98th Civil Affairs Battalion (Airborne). CPT Hurt holds a bachelor's degree in history from Virginia Tech and a graduate certificate in project management from the University of North Carolina.

CPT Albert Oh is a small group instructor in Bravo Company, 3rd Battalion (Civil Affairs), 1st Special Warfare Training Group (Airborne). Before instructing, he served in the 98th Civil Affairs Battalion (Special Operations) (Airborne) as a civil affairs team leader, company operations chief, and battalion plans officer. He holds a bachelor of science from the U.S. Military Academy.

1SG Christopher Melendez is the First Sergeant for Headquarters and Headquarters Company, 98th Civil Affairs Battalion (Special Operations) (Airborne), 95th Civil Affairs Brigade (Special Operations) (Airborne). He holds a bachelor of science from Excelsior College and a master of arts from the National Defense University's College of International Security Affairs. He is a doctoral candidate at Trevecca Nazarene University, where he is researching civilian education among Army special operations forces' noncommissioned officers.



The screenshot shows the MI Professional Bulletin website interface. The top navigation bar includes links for Home, Archive, Write Submission, Professional Reader, and Contact Us. A large banner on the right side of the page reads "MI Professional Bulletin Has an updated website!". Below this, a text box states: "The current issue of MIPB is still available on the front page of our website at <https://www.ikn.army.mil/apps/MIPBW>." The main content area displays a grid of 24 issue covers, arranged in 3 rows and 8 columns, representing issues from 1974 to the present. A text box at the bottom right of the grid reads: "Now To access all of our issues back to 1974, click the archive tab. A CAC is no longer required."

Issues, Goals, Influence, Vulnerabilities, and Opportunities

Key Intelligence Considerations for Irregular Warfare

by Mr. Marcus Canzoneri, Mr. Richard Oakley, and Mr. David Walther

Introduction

Irregular warfare presents unique challenges for intelligence professionals who support efforts at the tactical, operational, and strategic levels. U.S. doctrine defines irregular warfare as a “violent struggle among state and non-state actors for legitimacy and influence over the relevant population(s).”¹ Irregular warfare is conducted independently of, or in combination with, traditional warfare and usually consists of at least one, or a blend of any or all, of five main operations: “counterterrorism; unconventional warfare; foreign internal defense; counterinsurgency; and stability operations.”² Other activities support irregular warfare. They may include—

- ◆ Military engagement.
- ◆ Security cooperation.
- ◆ Deterrence activities.
- ◆ Cyberspace operations.
- ◆ Military information support operations (also known as psychological operations).
- ◆ Strategic communications.
- ◆ Civil-military operations.
- ◆ Intelligence.
- ◆ Counterintelligence.
- ◆ Space.
- ◆ Counter threat finance.
- ◆ Support to foreign governance and law enforcement entities.³



Photo by U.S. Air Force TSgt Ian Dean

U.S. Army SSG Matthew Hoffman, 407th Civil Affairs Battalion, Charlie Company, Team 0733, gestures to Djibouti army soldiers during a key leader engagement exercise as part of the civil-military cooperation training at Bat Hill 2, in Arta, Djibouti, on Dec. 17, 2014.

In short, irregular warfare encompasses a broad range of military (and whole-of-government) activities in which the operational environment is fluid, adversaries are adaptive, and *the population is central*.⁴ The principal challenge for intelligence professionals is knowing how to provide relevant analytic insight to help resolve the conflict given these conditions. However, existing analytic frameworks are insufficient or are outpaced quickly by intelligence requirements in irregular warfare.

Creating an Irregular Warfare Intelligence Course

In 2010, U.S. Special Operations Command tasked the Joint Military Intelligence Training Center to create an irregular warfare intelligence course in a compressed timeframe. We looked for key intelligence considerations that were common to all the operations and vital to conducting successful irregular warfare operations. We conducted exhaustive research of current doctrine, various manuals, special operations publications, books by subject matter experts, and other sources (books, articles, and papers) that veterans of the current and past irregular warfare conflicts had written. We noticed that striking similarities existed among these sources.

Most used the intelligence preparation of the battlefield (IPB) model, or a model very similar to IPB, as the basis of intelligence knowledge in the irregular warfare environment. This was not surprising, really, when you consider that IPB is an indispensable tool for planning and considering the nature and effects of the relevant environment and the adversary. This includes IPB's corresponding joint doctrine, joint intelligence preparation of the operational environment; and the North Atlantic Treaty Organization (NATO) doctrine, comprehensive preparation of the operational environment. Unfortunately, many years ago it wasn't clear how to adapt IPB to focus on the population. Thus, several frameworks aimed at adapting IPB to address the civil considerations inherent in irregular warfare. ASCOPE (areas, structures, capabilities, organizations, people, and events) was developed and adopted in U.S. doctrine as a good model to use in combination with IPB and PMESII (political, military, economic, social, information, and infrastructure).

Initial questions regarding the irregular warfare environment:

What do they want?

What do they need?

Why are they fighting?

Most militaries presently make good use of IPB and a combination of ASCOPE/PMESII frameworks and have adapted to account for basic civil considerations. However, to provide the incisive analysis needed in fluid, population-centric conflict against adaptive adversaries, intelligence professionals must answer fundamentally different and deeper questions about the "relevant population(s)."

The IGIVO Model Explained

The issues, goals, influence, vulnerabilities, and opportunities (IGIVO) model aims to complement other analytical processes and techniques in the existing frameworks and to answer questions about the underlying nature and drivers—the *key intelligence considerations*—of a particular irregular conflict. IGIVO provides an approach to begin disaggregating the complex matters common to all irregular conflict: what the involved parties want, what they need, and why they are fighting.⁵ In doing so, analysts and decision makers are better positioned to prevent, deter, and/or defeat an adversary; resolve conflict; and enable informed policy decisions.



Before making use of IGIVO, it is important to note several key points:

- ◆ IGIVO is intentionally ordered to provide a logical and prioritized sequence of analysis.
- ◆ Some factors of IGIVO may be seemingly nonexistent, or not clearly recognizable, in some conflicts.
- ◆ "Relevancy" of a population is dependent on one's perspective or a state's interests; due diligence must be exercised to account for all groups involved, including one's own group, and coalition partners (all stakeholders).
- ◆ The more thoroughly each IGIVO dimension is explored for each relevant population, the more potential value is generated. (However, a fine line exists between

minutiae and nuanced insight—in irregular warfare it’s easy to get lost in the blur.)

- ◆ IGIVO is not a stand-alone framework, is not a replacement for IPB, and should be used in conjunction with other analytic frameworks—they inform each other and become mutually reinforcing in irregular warfare.⁶

Note that we don’t talk about destroying our enemy’s capabilities or their forces. We believe that the essence of irregular warfare is a conflict of ideas, ideology, influence, and perceptions. We cannot kill or destroy these esoteric elements; we can only change, legitimize, or delegitimize them within the perceptions of the relevant population. When we speak of the relevant population, relevancy depends on your own area of interest—from the tactical level (tribal/clan and village), to the operational (district or province), to the strategic (national, regional, and international).

Unpacking the Acronym

The words that make up the acronym IGIVO correspond to elements of the IGIVO model—issues, goals, influence, vulnerabilities, and opportunities. The following paragraphs describe each one in detail.

Issues

Issues stem from the perception(s) that something is wrong, unfair, corrupt, or needed, and there is no effort to correct the problem(s). It is critical to remember perceptions are what matter, not truth or reality. People act on those perceptions, for they believe them to be true. Therefore, we need to look at these issues from each party’s point of view.

When considering the population and adversary points of view, the crucial issues are the underlying problems, ideas, beliefs, and perceptions that may support an insurgency or lead to political violence. These are widespread perceptions that cause the populace to resent and distrust their governance. Examples of underlying issues that can cause insurgency or political violence are corruption, racism and ethnocentrism, lack of governance, lack of (or breakdown of) basic services and infrastructure, and oppressive rule.

Many things can inflame one group of people against another—revenge, poverty, envy, ideology, ethnic tension, and even plain old,

simple greed. Many types and variations of issues exist, some of which may seem trivial, or even nonexistent, in our own culture. One must use critical thinking to recognize one’s own biases and mindsets in order to mitigate them as we identify these issues. One’s own values and beliefs are irrelevant when considering how a foreign population perceives issues. We must explore the issues fully and objectively to determine if they can be eliminated or reduced to a point at which they do not continue to drive conflict or political violence. If we can address the underlying issues, then we may be able to prevent an insurgency or achieve a much-needed goal without bloodshed.

Leadership and governance are classic areas for real and perceived issues in a counterinsurgency environment. What

problems are present in the current leadership? Do leaders have legitimacy within the population? How, generally and specifically, is governance meeting (or failing to meet) the needs of the people?⁷ The issues are what legitimize the actions of the insurgents in the minds of the insurgent and in the minds of the population. In this view, addressing these issues to a majority of the population’s satisfaction will undercut the legitimacy of the insurgents. It is improbable that issues

can be addressed to the satisfaction of everyone within the relevant population. Yet, we must still identify and address issues. Thus, a majority is the aim. If we address those issues satisfactorily for a majority of the population, the populace will tend to stop supporting the insurgency, and the insurgents will tend to become disaffected from the cause.

Goals

In some respects, an intelligence professional is like a detective who is trying to answer the interrogatives: who, what, where, when, why, and how. We are rather proficient in answering the who, what, where, when, and how interrogatives. Indeed, answering these questions has been the priority for intelligence personnel from time immemorial and will be far into the near future. We are not as adept at identifying the why of conflicts. Identifying the goals of our adversaries may answer the why, but usually the goals of our adversaries alone will not be sufficient to fully answer the why. Knowing the background, history,

Issue:

A point in question or a matter that is in dispute, as between contending parties in an action at law; a point, matter, or dispute, the decision of which is of special or public importance.

Goal:

The result or achievement toward which effort is directed; aim; end.

culture, and current attitudes of all parties involved is necessary to understand the adversary's goals, and understand how the adversary intends to reach those goals.

In warfare, and especially in irregular warfare, we should not limit ourselves to collecting information on our adversary. If we do, then we will miss many important factors that have a bearing on our mission. We also need to identify the goals of the local government, the national government, the populace (local and national), and even our coalition partners' goals. In addition, we need to identify our own goals: national, diplomatic, strategic, operational, and tactical—a task we sometimes ignore and have trouble with when we don't.

We need to determine several things concerning the population: their goals, wants, needs, and perceptions. From the population's goals, we can see what is important to undertake on behalf of the populace (their needs). Providing for these needs is required for a population to reach those overarching goals. Wants are those things that a population desires but likely will not advance them toward a goal. And the perceptions of the populace are what matter to us in determining success, not the truth as we see it or factual information. Only the population's perception of whether they are moving toward their goals matters. If the population does not see progress, they will likely not support our cause. As long as the populace goals don't conflict with our goals, identifying those projects and activities that further the populace goals should be a priority, and those projects that do not further their goals (those wants) can be deferred.

Although the population rises in importance in irregular warfare, the adversary is still important and we must address adversary goals as well. From adversary goals, we can determine what possible adversary courses of action may occur; what might be deception; how to counter adversary information operations; and what friendly force courses of action may prevent, deter, and defeat the adversary's courses of action.

Of course, we aren't just dealing with the population and the adversary, although they are probably our primary focus of effort. We also need to assess the local government and determine goals from its point of view. From the local government's goals, we can determine how to more effectively cooperate with and/or influence the local government. From assessing the local government, we may

see goals that converge with the adversary and population goals. These convergences will give us opportunities to prevent and deter conflict.

"Your enemy is never a villain in his own eyes. Keep this in mind, it may offer you a way to make him your friend."⁸

Where goals overlap, we should cooperate with our coalition partners, the populace, the government, and, yes, even the adversary. What better way to conduct successful operations than to co-opt the population, the government, and the adversary to cooperate on those common objectives? If our mission is truly to establish and maintain an acceptable level of stability, then we should not just consider, but rather focus on, cooperating on common goals that may deter the adversary from fighting, offer the adversary areas for negotiation, and induce defections among the adversary's supporters and fighters.

"Never appeal to a man's better nature. He may not have one. Invoking his self-interest gives you more leverage."⁹

At times, it can be difficult to recognize what our own goals are in a conflict. National and/or coalition objectives, often determined by political exigencies of the moment, can be in constant flux, unattainable in reality, or simply incoherent. When these strategic objectives are not clear, military and diplomatic operational objectives can be equally confusing. Military objectives at the operational and tactical levels are normally much easier to identify; mission statements and commander's intent usually clearly define the objectives of military operations.

Influence

Perhaps the most difficult information to acquire is the varied nuances of who has what types of influence in your area of interest. However, it is immensely important to know who has influence over others, what type of influence it is, and how they use that influence. Having identified these influences and the parties that have influence, and through an understanding of the social and cultural environment, we may then use our influence, counter the adversary's influence, and co-opt others' influence to further our goals.

Influence:

The capacity or power of persons or things to be a compelling force on or produce effects on the actions, behavior, opinions, etc., of others.

As an example, let us look at the conflict in Afghanistan. The United States has influence in Afghanistan at several levels, through—

- ◆ Diplomatic support of the national government.
- ◆ Funds for the Afghan government.
- ◆ Funds for local projects.
- ◆ Our military strength.
- ◆ Our face-to-face discussions (strategic communication, information operations, psychological operations, and civil-military operations) with Afghan leaders and people.

The Taliban have influence in Afghanistan at several levels as well, through—

- ◆ Commonality of language, culture, and history.
- ◆ Threat of violence against villages or individuals.
- ◆ Family, clan, and tribal ties.
- ◆ Establishment of order rather than chaos.
- ◆ Creation of a justice system and dispute resolution.
- ◆ Shared belief system.
- ◆ Military strength.

The populace also has influence on U.S. forces, the coalition, and the Taliban. Local tacit and/or complicit support to our forces allows our coalition to conduct operations more efficiently in that local populace's area of influence—however, the same is true for Taliban and/or other hostile forces and local populace support for their cause. Antipathy toward one side or the other can make carrying out operations in that populace's area of influence ineffective, dangerous, and deadly. We can win battles against the Taliban day after day and still lose the war by losing the population's support. "Winning hearts and minds" is a simplistic way of seeing popular support. They don't have to like us; they don't have to want us in their villages; they don't have to think the way we do; we just need their support in attaining common goals.

Vulnerabilities

Vulnerabilities are important to identify in order to defend yourself, to conduct successful attacks against an adversary, and to protect a populace. Vulnerabilities are something that those of us in the military are used to identifying in ourselves and in our adversary but maybe not so much when it comes to the population.

Traditionally, when we evaluate our adversary, as step three of joint intelligence preparation of the operating environment or IPB, part of that evaluation is to determine strengths and weaknesses (vulnerabilities). By determining these strengths and weaknesses, combined with our knowledge of the physical and electronic environment, we can conduct an analysis of the possible adversary courses of action against our forces, and then determine which of these possible adversary courses of action are most dangerous to our forces and which are most likely to occur. In irregular warfare, however, we should also consider what the possible courses of action the adversary would take against the populace, which are most dangerous to our goals, and which are most likely to occur.

Again, in looking to the conflict in Afghanistan, these adversary courses of action will include influence operations aimed at creating a negative view of U.S. or coalition forces and a positive view of the Taliban. These operations also include threats and intimidation of the populace to keep the populace from working with the U.S. or coalition forces. So, we are not just talking about operations aimed at destroying U.S. or coalition forces, although those are probable, but also those aimed at eroding our influence within the populace. Herein lies one of our vulnerabilities; in the past, we have been much slower than the Taliban at providing influencing information to the populace. We have been losing the information war.

Vulnerabilities are not always fixed and can be very fluid. Changes in circumstances, in operations, in populace perception, etc., can remake former vulnerabilities into strengths. The Taliban's use of intimidation, violence, and threats worked for them previously; however, they became a vulnerability as coalition forces entered areas formerly under Taliban control and treated the locals with respect and compassion. These formerly intimidated locals were giving coalition forces support and information on

Vulnerability:

Capable of or susceptible to being wounded or hurt; open to moral attack, criticism, etc.; open to assault; difficult to defend.

our adversaries. Identifying these vulnerabilities is a key intelligence consideration to winning the irregular war. One must also identify one's own vulnerabilities and either hide them or address them. Identify the population's vulnerabilities to the adversary and protect them. Identify the adversary's vulnerabilities and exploit them.

Opportunities

Most people would assume that vulnerabilities can lead to opportunities, and this is true—they may. However, there

are also opportunities we can use to our advantage that do not stem from vulnerabilities of our adversary or the population. Opportunities to further our cause and obtain our goals occur in abundance in our daily interactions with locals, with our coalition partners, and with the local Army and police, and may have no connection to vulnerabilities in any of these groups or the adversary. Civil-military operations can meet the needs or wants of the populace, providing positive messages to the local populace and influencing the local populace in favor of our cause. Buying local goods to meet our supply needs provides an input of cash into the local economy and influences local businesses in favor of our cause.

For example, security represents a key portion of the strategy of village stability operations. It addresses the vulnerability of the populace to the insurgents' use of violence and the threat of violence. The populace needs to be protected from threats and violent activities of the insurgents. One of the lines of operation in village stability operations is creating a security force of local villagers, which then answers to a regional commander. Thus, the opportunity presented by addressing a vulnerability of the populace also provides another opportunity to build a stronger regional, and by inclusion national, security force, which then influences the local villagers to see the regional, and by inclusion national, government in a better light.

A populace's vulnerability resulting from natural or man-made disasters offers an opportunity for the United States to provide humanitarian assistance, which is an opportunity to influence a populace favorably toward the United States.

Projects, such as building clinics, outhouses, or schools, also present opportunities to influence a populace favorably toward the United States without a specific populace vulnerability.

“The greatest productive force is human selfishness.”¹⁰

Finding common ground with an insurgent—such as reducing government corruption, ending ethnic favoritism, or stopping ethnic cleansing—can provide enough common ground to bring an insurgent force to the bargaining table, presenting an opportunity for dialogue and an end to further conflict. Appealing to a group's or individual's self-interest is much more compelling than using threats.

Methodology Note on Using IGIVO

Figure 1 shows a template for capturing an IGIVO analysis. Bear in mind, this is an analytic framework to ensure you are assessing all relevant actors in an irregular conflict. Therefore, the ways to capture and present such an analysis

are endless. A matrix, such as the one shown in the figure, is certainly one of the simplest ways. However, you could employ a variety of relationship diagrams, including maps or software, to take advantage of layering and geospatial associations. Whatever methodology you choose to employ, you should look at IGIVO

from the point of view of each of the parties involved.

Students of the Intelligence Support to Asymmetric Warfare Course at the NATO School Oberammergau created the example shown in Figure 2 (on the next page). They used the IGIVO matrix and applied NATO PMESII to the matrix. It immediately gives an overall perspective on which

Opportunity:
A situation or condition favorable for attainment of a goal; a good prospect, as for advancement or success.

IGIVO Matrix	Issues	Goals	Influence	Vulnerabilities	Opportunities
Population					
Adversary					
Village Governance					
District / National Government					
Other (external?) Government					
US Government Diplomatic / Military					
Allies/Coalition					

Figure 1. IGIVO Matrix

	Issues	Goals	Influence	Vulnerabilities	Opportunities
Russian Government/Military	<ul style="list-style-type: none"> • Black Sea Access • Desires control of Crimea • Fear of western influence 	<ul style="list-style-type: none"> • Buffer zone • Frozen conflict • Access to Mediterranean • Domestic political support • Ukraine joins EEU • Promote RUS narrative 	<ul style="list-style-type: none"> • Bases in Crimea • RUS owned enterprises • Media-favorable narrative • Cultural conservatism • Forces inside Crimea 	<ul style="list-style-type: none"> • Geostrategic relevance • Energy exportation • Sevastopol lease • Popular support 	<ul style="list-style-type: none"> • Keep UKR in SOI • Test IC resolve • Refine hybrid warfare • Credible foreign engagement • Improve popular support
Ukrainian Government/Military	<ul style="list-style-type: none"> • Territorial Integrity • Join EU or not • Pressure to join ECU • Displeasure w/ government 	<ul style="list-style-type: none"> • Economic growth /stability • Appease RUS • Join EU • NATO potential • Develop energy deposits 	<ul style="list-style-type: none"> • Energy deposits • Local government • Control of infrastructure 	<ul style="list-style-type: none"> • Political division • Limited legitimacy • Escalation • Lack of counter-strategy • Lack of IO • Russian presence • Ties to RUS 	<ul style="list-style-type: none"> • Garner western support • Unify against RUS
Ethnic Russian Population in Crimea	<ul style="list-style-type: none"> • Culture ID limbo • Marginalization 	<ul style="list-style-type: none"> • Stability • Quality of life • Status quo • Pro-RUS gov't 	<ul style="list-style-type: none"> • Pro-Russian militias • Vocal minority 	<ul style="list-style-type: none"> • Personal security • Manipulation • Need for stability 	<ul style="list-style-type: none"> • Aligned with RUS
International Community	<ul style="list-style-type: none"> • Russian revanchism • Avoid war 	<ul style="list-style-type: none"> • Status quo • Avoid war • Non-disruption • Stabilization • Promote democratic values • Counter RUS IO 	<ul style="list-style-type: none"> • International organizations • Ability to enforce sanctions 	<ul style="list-style-type: none"> • No narrative • Double standards • Escalation • Energy dependence • Credibility 	<ul style="list-style-type: none"> • Galvanize pro-western spt • Contain RUS • Develop hybrid warfare strategy
Legend: Political Military Economic Social Information Infrastructure					

Figure 2. NATO School's IGIVO Matrix with Color-Coded PMESII Elements Applied

elements of PMESII are preeminent in the conflict. For example, social concerns (purple) are dominant in the ethnic Russian population. However, political (red) and economic (green) are dominant throughout the whole of the matrix. The matrix shows at a glance that the conflict in Ukraine is about politics and economics for Ukraine, Russia, and the international community, but about social (or ethnic) divides for the local population.

This example shows the flexibility and applicability of the IGIVO model. You can use IGIVO on its own as a primer to quickly familiarize yourself with a conflict. You can also enhance other models by inserting IGIVO into the analysis or the model itself. As shown in the figure, the IGIVO model can include other models.

Conclusion

We hope others will see value in what we have presented here and that they will use (and modify) IGIVO for their own use in the varying manifestations of warfare. The IGIVO

model is used in courses run by Joint Special Operations University, U.S. Special Operations Command, and NATO School Oberammergau. Several other models and methods are useful in irregular warfare, such as the U.S. Marine Corps Intelligence Activity's cultural intelligence factors, the special forces area study, human terrain analysis, human geography, and human factors analysis. We believe that IGIVO could be useful as a guide during the use of those other models and methods. 🌟

Endnotes

1. Office of the Chairman of the Joint Chiefs of Staff, *DOD Dictionary of Military and Associated Terms* (Washington DC: The Joint Staff, January 2019), 120.
2. Department of Defense Directive 3000.07, *Irregular Warfare (IW)* (August 28, 2014), 1. Change 1 was issued on May 12, 2017.
3. Department of Defense Directive 3000.07; and Department of Defense, *Irregular Warfare: Countering Irregular Threats, Joint Operating Concept Version 2.0* (May 17, 2010).

4. Ibid., 11.

5. Konrad Trautman, Assistant Chief of Staff for Intelligence (J-2), U.S. Special Operations Command, 2010.

6. For example, the U.S. Marine Corps Intelligence Activity's cultural intelligence factors, the special forces area study, human terrain analysis, human geography, and human factors analysis.

7. Governance is used instead of government because government control or any government representation is not always present in some areas. But

some type of governance will always exist, such as a village chief, an elder, a religious or tribal leader, etc., providing similar public services that a government would provide if it were present.

8. Robert Heinlein, *The Notebooks of Lazarus Long* (New York: Ace Books, 1978).

9. Ibid.

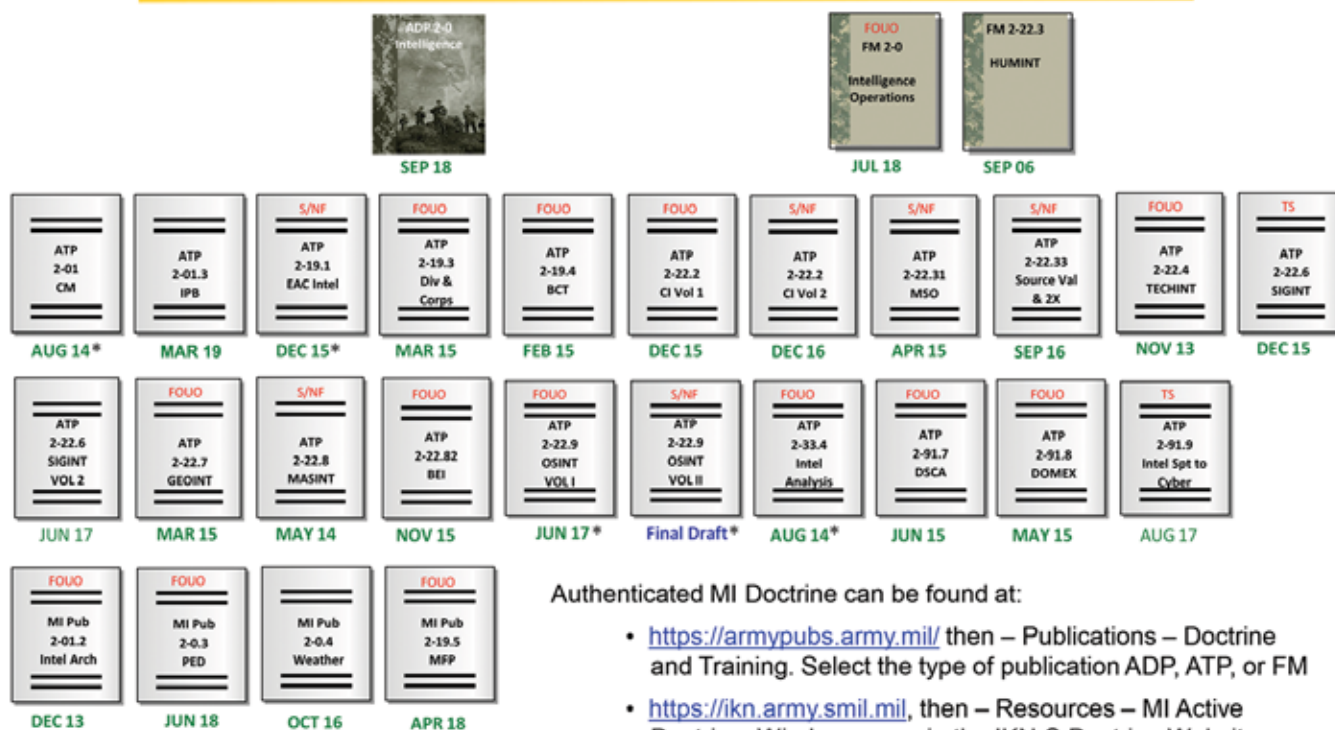
10. Ibid.

Marcus Canzoneri is a program manager and instructor in the Asymmetric Warfare Analysis Branch at the Joint Military Intelligence Training Center, Defense Intelligence Agency (DIA). He joined DIA in 2007 after serving 21 years of active duty and 2 years of reserve duty in the Marine Corps, Marine Corps Reserve, Army National Guard, and Army. His military experience was mostly as an all-source intelligence analyst and intelligence chief. His most recent operational experiences were overseas as a government civilian supporting special operations activities in Iraq and Afghanistan.

Richard Oakley is a course manager and instructor in the Asymmetric Warfare Analysis Branch at the Joint Military Intelligence Training Center, DIA. He served as a U.S. Army special forces officer in command and staff positions spanning the tactical, operational, and strategic levels with multiple operational deployments. He has also served as a contract civilian training special operations forces on a wide range of operations and intelligence topics specific to irregular warfare.

David Walther was an instructor in the Asymmetric Warfare Analysis Branch at the Joint Military Intelligence Training Center, DIA. He retired from the U.S. Army after 26 years of active duty. His military experience was as a cryptologic linguist and a special operator. His most recent operational experience was as a contract civilian supporting special operations activities overseas. He currently works for a Department of Defense contractor on special projects.

Are You Doctrinally Proficient?



* Key revision projects
Authenticated
Draft

Authenticated MI Doctrine can be found at:

- <https://armypubs.army.mil/> then – Publications – Doctrine and Training. Select the type of publication ADP, ATP, or FM
- <https://ikn.army.smil.mil>, then – Resources – MI Active Doctrine. Window opens in the IKN-S Doctrine Website. Select MI Active Doctrine from the left menu.
- <https://ikn.army.smil.mil>, then – Applications – IKN Applications – Document Management System – Doctrine – ADP, ADRP, FM, TC, ATP Series (Intelligence)

As of 8 March 2019

Intelligence Support to Unconventional Warfare

by Lieutenant Colonel Thomas J. McCarthy (Retired)

Challenge and Proposition

What does it mean to enable Army special operations forces (ARSOF) with intelligence in support of unconventional warfare (UW) operations? An interesting question to consider. The answer would likely gather informal responses involving the collection, analysis, and dissemination of data for operations affecting decision making. Fundamentally, this approach is not wrong. However, analytical support within special operations forces (SOF) formations to conduct UW entails particular requirements that may not be fully understood or executed. Investigation of the challenges and opportunities resulting from the intelligence functions is

vitaly important. Moreover, facilitating understanding within this domain strengthens the conventional forces and SOF integration, interoperability, and interdependence.¹ As ARSOF and conventional units operate and complement each other across all joint phases, each component may find special application within particular segments. Regardless of the element involved or the time and space occupied, it is still always necessary to facilitate situational understanding across the entire force.

This article offers recommendations for improving intelligence support to UW.² This focus is important given that U.S. Army Special Operations Command (USASOC) is the lead component organization within the U.S. Special Operations Command to execute these operations.³ The article is limited purposefully to address activities that may enable quick wins against a problem set vast in complexity. The list of potential issues surrounding this topic far exceeds what may be covered within this piece. Certain challenges will require senior-level action to remedy; however, the improvements discussed herein are not particularly resource-dependent and are achievable.



Photo by U.S. Army PFC Alexander Holmes

U.S. Special Forces conduct a downed pilot simulation for the Army Warfighting Assessment 17.1 exercise at Fort Bliss, TX, on Oct. 18, 2016; the first in a series of annual events to focus scarce resources where they will give Soldiers a true edge in the fight against a peer adversary.

No revolutionary concepts are discussed in this article. On the contrary, it reveals that resolution, in terms of using existing resources to improve UW-related intelligence functions, is within our reach. It occurs with greater understanding of, and adherence to, currently available UW doctrine and a genuine willingness to redress existing shortcomings. Two overarching approaches are provided:

- ◆ A discussion of UW principles.
- ◆ Challenges resulting from the application of intelligence support to UW within the current operational environment.

This article includes views and opinions garnered from subject matter experts within the U.S. Army John F. Kennedy Special Warfare Center and School, USASOC's Office of Special Warfare, and the Intelligence Advanced Research Projects Activity. Their feedback offers academic, operational, and experimental perspectives in evaluating the issues.

The article unfolds in three parts.

- ◆ **First—A discussion of the niche activities performed by SOF elements**, the bulk of which include functions readily known, but likely not well understood.
- ◆ **Second—An evaluation of lessons learned from the application of intelligence support to contemporary UW operations**—Human intelligence (HUMINT), signals intelligence (SIGINT), and open-source intelligence (OSINT) are expounded upon.
- ◆ **Third—The utility of automated frameworks potentially supportive to predictive human-centric analysis at the individual and societal level is recognized.**

Army Special Operations Forces Core Activities

As previously mentioned, it is important for intelligence practitioners to understand where UW falls within the ARSOF portfolio of missions. There is too much confusion within the intelligence community about what UW is and where it fits within the core ARSOF activities, as opposed to where it fits within irregular warfare (IW). The discussion that follows will help personnel speak about and understand UW within established frameworks. A secondary effect is achieving credibility within the ARSOF and intelligence communities by displaying subject matter expertise concerning UW.

There are 12 ARSOF core activities:⁴

- ◆ Unconventional warfare.
- ◆ Foreign internal defense.
- ◆ Security force assistance.
- ◆ Counterinsurgency.
- ◆ Direct action.
- ◆ Special reconnaissance.
- ◆ Counterterrorism.
- ◆ Preparation of the environment.
- ◆ Military information support operations.
- ◆ Civil affairs operations.
- ◆ Counter-proliferation of weapons of mass destruction.
- ◆ Humanitarian resistance/disaster relief.

UW is also an integral part of IW. The overarching concept of IW includes UW, counterinsurgency, counterterrorism, foreign internal defense, and stability operations, but is not a distinct activity within itself, as shown in Figure 1.⁵ As you can see from the figure, four of the five key IW functions are core ARSOF activities.⁶

UW involves activities “conducted to enable a resistance movement or insurgency to coerce, disrupt, or overthrow a government or occupying power by operating through or with an underground, auxiliary, and guerrilla force in a denied area.”⁷ The six core activities of UW include preparation of the environment, subversion, sabotage, personnel recovery, guerrilla warfare, and intelligence operations.

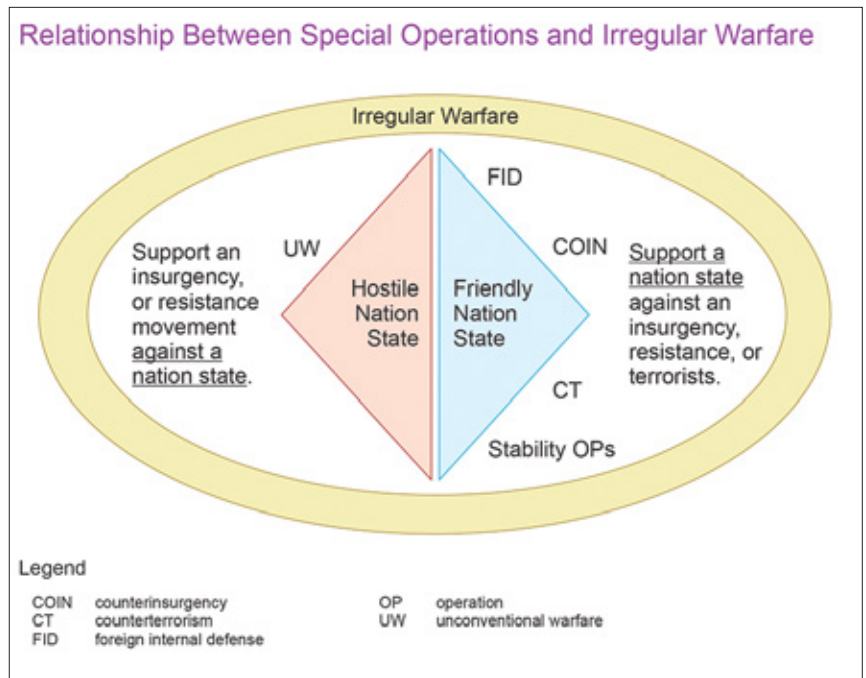


Figure 1. Relationship Between Special Operations and Irregular Warfare

Insurgent or resistance movements within UW may also undertake a multitude of activities—overt and clandestine—executed by public components, armed components, and underground forces.⁸

“There are three basic components of a resistance or an insurgency...guerrillas...underground... and insurgency... Although not basic components of a resistance, two other important organizational considerations are the area command and the mass base.”⁹ Each element can be assessed independently or in combination, depending on the primary UW objectives of coerce, disrupt, or overthrow. UW operations will also vary in their ways, means, and ends and entail armed and unarmed methods. These pathways are not mutually exclusive and analysts must be mindful of this fact when performing intelligence support functions.

An Appreciation of Fundamentals

The Special Forces Doctrine Division of the Special Operations Center of Excellence within the U.S. Army John F. Kennedy Special Warfare Center and School is the lead proponent for developing UW-related products. Faithful appreciation of doctrine and related literature is important—a critical step toward improving intelligence support to UW. However, this statement does not denote strict adherence, as doctrine is neither a panacea nor a means to address all ends. Rather, it establishes the fundamental principles that guide actions in support of objectives, which if followed, allows fulfillment in purpose.¹⁰ Moreover, it is the first step in the development of subject matter expertise and professional competence.

Discussion with personnel from the Special Forces Doctrine Division reveals the importance of effectually grasping UW fundamentals; it is a critical enabler to performing intelligence support activities. Chief, Special Forces Doctrine Division, states there has been “a loss of institutional knowledge” across the force.¹¹ This problem is neither unknown to nor impactful of ARSOF alone. Conventional force elements also face the challenge of rebuilding core competencies. A multi-decade commitment of forces in support of missions across the U.S. Central Command area of operations has inadvertently created the conditions enabling atrophy of some collective organizational tasks, the growth of expertise within the counterinsurgency and counterterrorism realms notwithstanding.

The Special Forces Doctrine Division representatives also highlight as a critical skill greater awareness and appreciation of partner force capabilities and integration into ARSOF planning and operations. An analyst in the Special Forces Doctrine Division notes in particular, “a thorough review of intelligence collection during UW operations entails a linkage between U.S. unilateral SOF intelligence capabilities and those of the partner force.”¹² He highlights TC 18-01.1, *Unconventional Warfare Mission Planning Guide for Special Forces Operational Detachment—Alpha Level*, as a great resource containing valuable information and graphics depicting potential resistance force intelligence capabilities, an example of which is shown in Figure 2.¹³ ATP 3-05.1, *Unconventional Warfare*, is noted for similar purposes in support of five additional SOF core activities. Additional doctrine is in development that will help professionals with UW activities especially ATP 3-18.1 and TC 18-08, *Underground Resistance*.

The U.S. Army Intelligence Center of Excellence is tackling a portion of skillset atrophy through publication and enforcement of its Military Intelligence Corps 2019-2020 Training Strategy. While this work seeks to gain efficiencies for intelligence instruction across conventional forces, it is

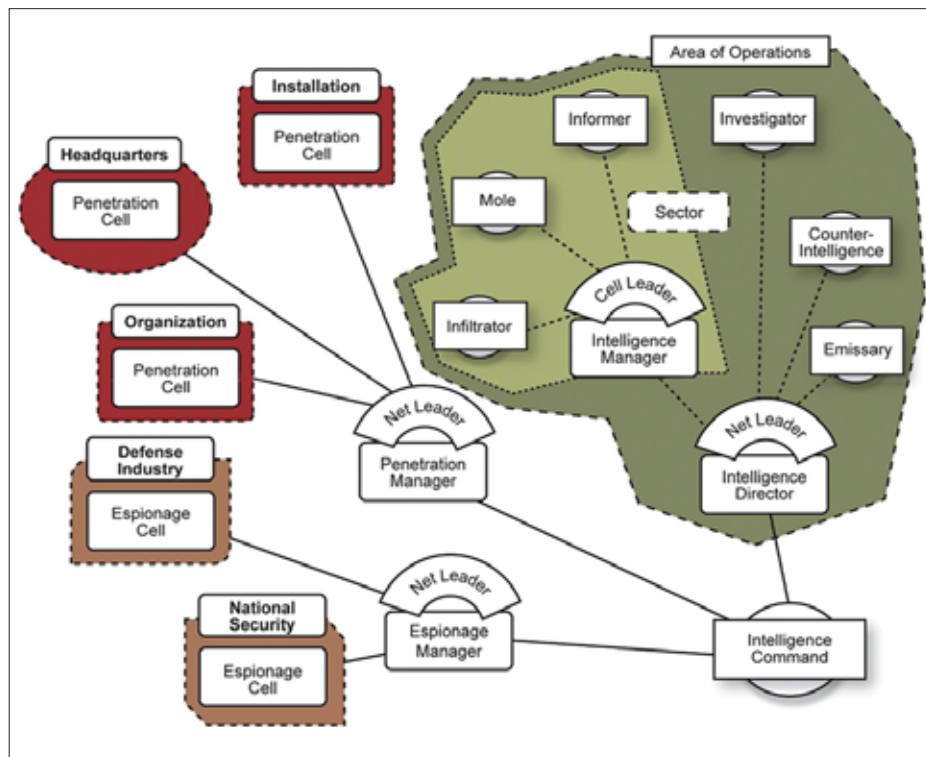


Figure 2. Underground Intelligence Command

highly applicable to ARSOF as well. The USASOC integration into the strategy involves publicizing ARSOF’s unique training opportunities while also allowing SOF formations to benefit from conventional forces’ training resources. These efforts are naturally supportive to the conventional forces

and SOF integration, interoperability, and interdependence and require broad use by personnel across all commands to enable symbiosis.

In a broad sense, institutional training allows for training of fundamental knowledge, while organizational training allows for growth into specific areas of expertise in line with unit mission requirements. Civilians and Soldiers who support SOF (and in particular UW operations) understand this statement to be acutely true. Indeed, according to the Special Forces Doctrine Team, what has been lost to a specific degree concerning UW is an appreciation of the difficulty involved in operating within denied areas.¹⁴ According to Chief, Special Forces Doctrine Division, “Denied areas offer the most difficult challenges with respect to nearly every aspect of the mission—from communications, to resupply, transportation, detection, etc.—all of which must be considered and trained [for].”¹⁵ However, ARSOF can operate within these denied areas when Soldiers sustain and improve their knowledge and training.

Improvement Opportunities

The contemporary operating environment offers numerous opportunities to improve intelligence support to UW. Engagement with representatives of the Office of Special Warfare reveals a general description of initiatives helpful to this process. The Office of Special Warfare is an element under 1st Special Forces Command, a component subordinate command within USASOC, and serves “as a focal point for all unconventional warfare capabilities, activities and interagency coordination across the [Special Warfare] SW spectrum.”¹⁶ Discussion with the Military Intelligence Integration Officer, Office of Special Warfare, involving observations and lessons learned highlight three disciplines of interest: HUMINT, SIGINT, and OSINT.

Human Intelligence. HUMINT is the coin of the realm when it comes to UW. Influence upon the individual and societal levels and within the cognitive domain enables success. As a principle of war, mass dictates the application of overwhelming capability at particular points in time to achieve ends. This concept is no different for HUMINT in support of UW. UW requires more HUMINT collectors (35M) than currently authorized to ensure mission success. The establishment of a joint manning document, employment of the Worldwide Individual Augmentation System, and a request

for forces have increased (temporarily) the 35M population support to ARSOF. However, long-term requirements warrant an evaluation of the permanent increase of 35Ms within SOF formations.

Signals Intelligence. SIGINT provides incredibly helpful intelligence to UW. Capabilities to discern “threat intentions, capabilities, compositions, and dispositions” by exploiting the electromagnetic spectrum provide “information for the delivery of fires.”¹⁷ As noted in ATP 3-05.1, *Unconventional Warfare*, “nonlethal methods of influence [are] crucial to the long-term conduct of UW.”¹⁸

The special operations team-alpha represents the SIGINT unit of action employed in support of ARSOF units worldwide. These teams conduct electronic reconnaissance and force protection, support to foreign internal defense operations, signals research, target development, and support to personnel recovery missions.¹⁹ Successful employment of organic ARSOF SIGINT capabilities requires sustainment of subject matter expertise. Although an obvious premise, it is routinely—but unintentionally—overlooked because of a myriad of conditions entailing operational tempo requirements, resource constraints, and personnel circumstances. To alleviate this problem, USASOC has implemented specialized training to increase SIGINT expertise throughout

[Special operations team-alpha] “SOT-As are low-level signals intelligence collection teams that intercept and report operational and technical information derived from tactical threat communications through prescribed communications paths. The mission of a SOT-A is to conduct signals intelligence and electronic warfare in support of cyber/electromagnetic activities, unilaterally or in conjunction with other SOF elements to support existing and emerging SOF missions.”²⁰

—FM 3-18, Special Forces Operations

its formations. Primarily, ARSOF personnel use the SIGINT course, but attendance is also open to conventional force Soldiers. Such integration and seeding of expertise enhances conventional forces and SOF integration, interoperability, and interdependence and provides for

continual development of subject matter expertise aligned against UW specific requirements. Personnel who successfully complete the course are well prepared to support ARSOF operations within all environments, including UW within denied areas.

Open Source Intelligence. The volume of publicly available information and its exploitation elevates OSINT to be on par with more traditional forms of intelligence like those already discussed. In many cases, OSINT provides greater environmental awareness than HUMINT or SIGINT. HUMINT requires time and validation to establish source reliability and data credibility. SIGINT often entails employment of systems and exploitation procedures not conducive to operations within denied areas. Admittedly, data derived from

OSINT cannot be accepted at face value. However, whether on the open, deep, or dark web, it is more accessible and available for immediate exploitation. Despite the data's morphology and episodic nature, it is surprisingly supportive to UW campaigns, which are of a long duration. ARSOF conducting UW must be adaptive to a society's changing dynamics, and OSINT enables operators and operational support personnel to react appropriately and in a timely manner to environmental shifts.

Current administrative and legal restrictions impede OSINT's full potential. Operation security risk via OSINT is inherent at the tactical level and grows exponentially at the operational and strategic levels, entailing potentially national-level impacts. However, ARSOF must have the freedom to assume appropriate levels of risk that enable the flexible use of capabilities within denied areas. These locales predominantly do not afford intelligence reachback via normal communications systems. Allowance of greater freedom within the OSINT domain, in line with authorities and approvals, expands ARSOF effectiveness in support of UW missions.

Utility of Frameworks

The amount of available OSINT data far exceeds an individual's processing capabilities. In particular, gaining situational awareness via social media exploitation is critical for understanding and influencing populations. A key component of this effort entails information superiority, which involves "operational advantage derived from the ability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same."²¹ The Information Dominance Detachment within 1st Special Forces Group is tackling this issue through research and testing of commercially available tools to establish effective analytical processes. The frameworks they offer derive from tactics, techniques, and procedures developed against real-world use cases within the U.S. Indo-Pacific Command's area of operation. Information Dominance Detachment-1's work is incredibly informative and offered for consideration in the establishment and refinement of intelligence support to UW.

Similar to Information Dominance Detachment-1's work, multiple governmental elements are working to improve human and machine capabilities to process and discern meaning from big data. One agency of note is the Intelligence Advanced Research Projects Activity (IARPA), which works under the direction of the Office of the Director of National Intelligence. The organization "invests in high-risk, high-pay-off research programs to tackle some of the most difficult challenges of the agencies and disciplines in the Intelligence

Community."²² Numerous projects are placed into four categories: analysis, anticipatory intelligence, collection, and computing. The intelligence community is able to leverage programs that IARPA produces, but adoptive organizations bear the cost to sustain and further develop transferred capabilities. To obtain more information about current and past research efforts, visit IARPA's webpage for contact information to program managers.²³

Machine learning, deep learning, forecasting, and the advent of artificial intelligence resonate through many IARPA projects. Successful applications, and equally informative failures, equate to delivery and employment of potentially supportive tools and functions enabling UW intelligence support. Regardless of which program is selected, the critical element of time remains the primary impediment to wide-scale adoption and utilization throughout SOF formations. Most IARPA projects require multiple developmental phases involving vendor solicitation and selection, trial runs, and repeatable achievements before transfer to end users. Condensing the acquisition timeline for innovative technologies without sacrificing attainment of qualitative milestones will better support ARSOF's busy operational tempo.

From an external perspective, a framework offered by the RAND Arroyo Center in its monograph published in 2008 titled *Assessing Irregular Warfare: A Framework for Intelligence Analysis* is worthy of note. The work proffered a framework made up of three activities comprised of eight distinct steps, shown in Figure 3.²⁴

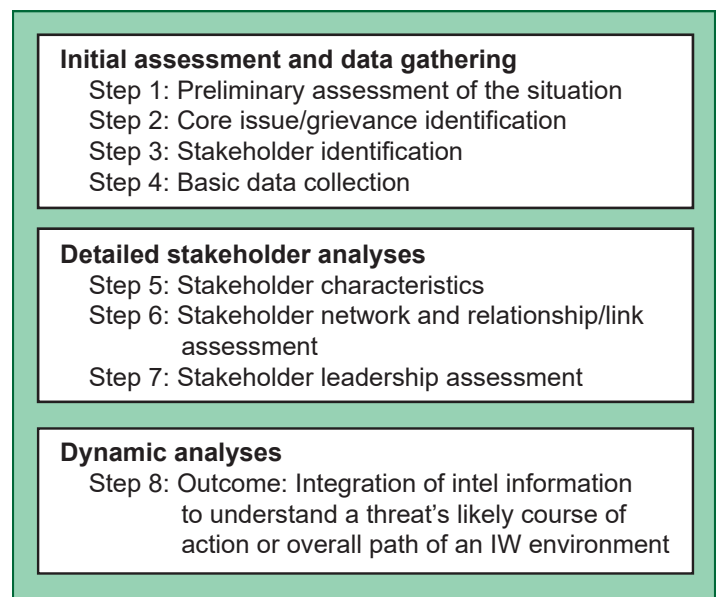


Figure 3. Analytic Framework for Irregular Warfare

The process guides analysts' activities as they evaluate the IW operational environment through either the population-centric or the counterterrorism lenses. The framework

provides an alternative method for addressing intelligence analytical support for all IW activities and complements the intelligence preparation of the battlefield process rather than working against it. This point is especially true when applied to ATP 2-01.3, *Intelligence Preparation of the Battlefield*, which is replete with examples of irregular and insurgent force analysis. The Special Forces Intelligence Sergeants Course heavily references ATP 2-01.3.

Numerous other commercial entities, research organizations, and governmental agencies are tackling the problems of developing processes supportive to intelligence functions. Awareness of applications along this front is paramount given ongoing and anticipated technological advancements within current and future operating environments. Recent guidance for the establishment of the Joint Artificial Intelligence Center and activation of the Army Futures Command illustrates the importance the Department of Defense has placed on remaining ahead of similar threat pursuits.²⁵

Conclusion

The recommendations in this article address the challenge of providing intelligence support to UW. First, the article presented a recommitment to understanding doctrine, which guides Army forces toward common knowledge and practice. Second, the article discussed peripheral challenges inherent with executing and applying HUMINT, SIGINT, and OSINT given the current operating environment. Third, we addressed frameworks, specifically in the form of developmental tactics, techniques, and procedures (1st Special Forces Group [Airborne]), experimental efforts (IARPA), and institutional research (RAND Corporation). An exploration and application of these frameworks may facilitate a continued drive toward excellence.

Outside observers who have never served in special operations units may find the SOF mystique intimidating, leading to a reluctance to learn more about ARSOF's many elements and functions. This effect is unintentional, and professionals should build a well-informed awareness of ARSOF operations. Knowledge of ARSOF operations will demonstrate that intelligence Soldiers and professionals are well equipped to support SOF; the recommendations discussed within this article will bolster their ability to succeed. ✨

Endnotes

1. Department of Defense established the policy and responsibilities to conduct and support "IW...to address irregular challenges or threats to national security." Department of Defense Directive 3000.07, *Irregular Warfare (IW)* (Washington, DC: U.S. Government Publishing Office [GPO], August 28, 2014), 1. Change 1 was issued on May 12, 2017.

2. Unconventional warfare is defined as "activities that are conducted to enable a resistance movement or insurgency to coerce, disrupt, or overthrow a government or occupying power by operating through or with an underground, auxiliary, and guerrilla force in a denied area." Office of the Chairman of the Joint Chiefs of Staff, Joint Publication (JP) 3-05, *Special Operations* (Washington, DC: U.S. GPO, 16 July 2014), xi.

3. "USSOCOM Directives 10-1cc (U) and 52589 (S//NF) establishes USASOC as the Lead Component for UW. This directive also describes the SOF service component capabilities and tasks for UW." U.S. Army Special Operations Command, *Unconventional Warfare Pocket Guide V1.0* (Washington, DC: U.S. GPO, 5 April 2016), 4.

4. Department of the Army, Field Manual (FM) 3-05, *Army Special Operations* (Washington, DC: U.S. GPO, 9 January 2014), 2-1.

5. Office of the Chairman of the Joint Chiefs of Staff, JP 3-05, *Special Operations*, II-2.

6. Irregular warfare is "a violent struggle among state and non-state actors for legitimacy and influence over the relevant population(s)." Department of Defense Directive 3000.07, *Irregular Warfare (IW)*, 14.

7. Office of the Chairman of the Joint Chiefs of Staff, JP 3-05, *Special Operations*, xi.

8. U.S. Army Special Operations Command, *Unconventional Warfare*, 9.

9. Department of the Army, FM 3-05, *Army Special Operations*, 2-3.

10. This sentence paraphrases wording from an article about Army doctrine. John Spencer, "What is Army Doctrine?" *Modern War Institute*, 21 March 2016, <https://mwi.usma.edu/what-is-army-doctrine/>.

11. Mr. Frank Hudson (Chief, Special Forces Doctrine Division, Special Operations Center of Excellence), in discussion with the author, 29 August 2018.

12. Mr. Daniel Banks (Analyst, Special Forces Doctrine Division, Special Operations Center of Excellence), in discussion with the author, 29 August 2018.

13. Department of the Army, Training Circular 18-01.1, *Unconventional Warfare Mission Planning Guide for the Special Forces Operational Detachment—Alpha Level* (Washington, DC: U.S. GPO, 27 October 2016), A-8.

14. For discussion herein, denied areas are those locations "under enemy or unfriendly control in which friendly forces cannot expect to operate successfully within existing operational constraints and force capabilities." Office of the Chairman of the Joint Chiefs of Staff, *DOD Dictionary of Military and Associated Terms* (Washington, DC: The Joint Staff, January 2019), 66.

15. Mr. Frank Hudson (Chief, Special Forces Doctrine Division, Special Operations Center of Excellence), in discussion with the author, 29 August 2018.

16. U.S. Army Special Operations Command, *ARSOF Next: A Return to First Principles* (2016), 8.

17. Department of the Army, Army Doctrine Publication 2-0, *Intelligence* (Washington, DC: U.S. GPO, 4 September 2018), 4-8.

18. Department of the Army, Army Techniques Publication (ATP) 3-05.1, *Unconventional Warfare* (6 September 2013), E-2. Change 1 was issued on 25 November 2015.

19. Department of the Army, ATP 3-05.20, *Special Operations Intelligence* (Washington, DC: U.S. GPO, 3 May 2013), 7-15.

20. Department of the Army, FM 3-18, *Special Forces Operations* (Washington, DC: U.S. GPO, 28 May 2014), 4-15.

21. Office of the Chairman of the Joint Chiefs of Staff, JP 3-13, *Information Operations* (Washington, DC: U.S. GPO, 27 November 2012), GL-3. Change 1 was issued on 20 November 2014.

22. Intelligence Advanced Research Projects Activity website, accessed 4 February 2019, <https://www.iarpa.gov/index.php/about-iarpa>.

23. Intelligence Advanced Research Projects Activity website, accessed 4 February 2019, <https://www.iarpa.gov/>.

24. Eric V. Larson, Derek Eaton, Brian Nichiporuk, and Thomas S. Szayna, *Assessing Irregular Warfare: A Framework for Intelligence Analysis* (Santa Monica, CA: RAND Corporation, 2008), xii.

25. Paul McLeary, "Pentagon, Intel Agencies Set Up New AI Joint Office," *Breaking Defense*, April 13, 2018, <https://breakingdefense.com/2018/04/pentagon-intel-agencies-set-up-new-ai-joint-office>.

LTC Thomas J. McCarthy (retired) currently serves as the senior intelligence analyst within the G-2, U.S. Army Special Operations Command (USASOC) and has more than 20 years of experience within both special operations forces and conventional organizations. Previous assignments include Intelligence Operations Division Chief (USASOC, G-2), intelligence planner at the Joint Special Operations Command, executive officer and operations officer for the 319th Military Intelligence Battalion, and Experimentation Chief for the Mounted Maneuver Battle Lab. He has three deployments to Afghanistan and two deployments to Iraq. Mr. McCarthy holds a master of science degree in strategic intelligence from the National Defense Intelligence College and graduated from West Virginia State University in 1997.



Photo by U.S. Army SSG Marcus Fichtl

Two U.S. Army Soldiers assigned to Special Operations Command-Europe, engage opposing forces at an objective during Jackal Stone 2016 in Tblisi, Georgia, August 15, 2016.



by Chief Warrant Officer 3 Brandon R. Mesa

U.S. Army Special Operations Command Soldiers participate in a weeklong capabilities exercise or CAPEX, June 13, 2018.

Addressing Army Aviation Intelligence Training

Obligation to Prepare

In recent years, the U.S. Army's military intelligence branch has been going through a transformation to prepare the next generation of intelligence professionals for large-scale combat operations in a complex operational environment. The 2018 National Defense Strategy underscores our emergence from a period of strategic atrophy, declaring, "inter-state strategic competition, not terrorism, is now the primary concern in U.S. national security."¹ Recently published Army doctrine confirms that a shift in strategic thinking has occurred among senior leaders—away from intra-state conflicts such as Iraq—and is the impetus behind the transformation across the force.

The contemporary operational environment is contested across every domain, with both current and emerging sophisticated threats from revisionist states and rogue regimes challenging the competitive military advantage the

United States has enjoyed for decades.² A prolonged fight using the counterinsurgency model dominated the focus of Army training for many years, leading to conventional operational deficiencies that demanded a shift in Soldiers' training to close these gaps.

Army aviation is a critical element that assists ground forces—including support for sensitive activities carried out by special operations forces—and it requires tailored, reliable, timely, and predictive intelligence to prevail in large-scale combat operations. However, despite the overhaul in Army training, intelligence professionals do not currently receive institutional training specific to aviation and support to rotary wing operations. The U.S. Army Training and Doctrine Command and other training venues, such as Foundry, do not provide formal courses on aviation intelligence. This is likely because assignments for Army intelligence professionals to aviation units are niche assignments,

and these training institutions have the challenge of determining what is trained and how it is trained, using the available resources of time, people, and equipment.

In a 2017 article in the Army's *Aviation Digest*, CPT Margaret Troxell highlighted the difficulties that combat aviation brigade (CAB) and battalion S-2s face in providing effective intelligence preparation of the battlefield and mission analysis support. She cited the lack of aviation-specific

intelligence training as the contributing factor to this problem.³ As a potential remedy to partially address this issue, CPT Troxell recommended sending CAB S-2s to the Aviation Mission Survivability Officers (AMSO) course at Fort Rucker, Alabama, to "bridge the gap between Intelligence and all aspects of Aviation mission planning."⁴ Although the AMSO course is for aviation officers and aviation warrant officers, military occupational specialty 35D (all-source intelligence) officers assigned to aviation units can attend the class on a case-by-case basis. The AMSO course goes into the technical aspects of airframe details, aircraft survivability, threats to aviation capabilities and vulnerabilities, mission planning, and personnel recovery support; all of which provide invaluable course material to intelligence professionals bound for aviation assignments.⁵

One major issue with the AMSO course administration, however, is that enlisted personnel cannot attend, leaving most of the aviation intelligence sections at a significant disadvantage. In today's operational environment, CAB S-2s are unlikely to have sufficient time to personally train their personnel on all the knowledge gained at the 5-week AMSO course. It is further doubtful that all CAB S-2s would be able to attend the AMSO course, because of either a lack of available seats or an inability to spend 5 weeks away from their duty positions. With this in mind, the time for designing an aviation-specific intelligence course to train all intelligence personnel, officers and enlisted, is long overdue.

A Note on Intelligence Training from USAICoE

While it is true that training institutions have the challenge of determining what is trained and how it is trained, the U.S. Army Intelligence Center of Excellence (USAICoE) trains intelligence professionals on the basics of intelligence planning, management, and execution that are the foundations of all intelligence procedures. USAICoE cannot and does not train technical aspects of any particular warfighting function, rather they provide the building blocks to which any technical aspects can be applied and transformed from information to intelligence. Intelligence supports the commander's requirements, answers the "so what" through intelligence preparation of the battlefield (IPB), and is applicable to all supporting organizations—aviation, sustainment, fires, maneuver, etc. An individual gains technical expertise by applying their understanding of the situation through the IPB process.

Solution Proposal

While the deficiency in aviation intelligence training is not a new problem, the mounting peer threats that may challenge U.S. air superiority in open armed conflict make the training matter more pressing than ever. A 2013 *Armed Forces Journal* article by MAJ Corby Koehler identified themes similar to CPT Troxell's and declared that the lack of formal training is the main problem.⁶ Contrasting Army intelligence training to other

services, MAJ Koehler highlights how the Marine Corps has addressed its aviation intelligence training deficiency by providing both a 12- and 4-week course for officers and enlisted personnel, respectively, both of which are tailored for intelligence support to aviation missions.⁷ In 2013, MAJ Koehler also discussed the topic in an article he co-authored for the *Military Intelligence Professional Bulletin*.⁸

The Army could use either the above courses or the Marine Corps' Squadron Intelligence Training Certification Course, which is specifically designed to train enlisted Marine personnel destined for an aviation assignment, as a model for training against its identified gaps.⁹ Army intelligence personnel assigned to aviation elements would significantly benefit from attendance at a 1- or 2-week course covering topics such as aviation airframes, airframe survivability, mission planning, operational tactics, threat detection capabilities, weapon systems, and electronic warfare.¹⁰

The U.S. Army Special Operations Aviation Command (SOAC)

SOAC was established in 2011 with the following subordinate units: 160th Special Operations Aviation Regiment (Airborne), U.S. Army Special Operations Command Flight Company, Special Operations Aviation Training Battalion, Systems Integration Management Office, and Technology Applications Program Office. SOAC's mission is to organize, man, train, resource, and equip the Army special operations aviation enterprise to provide responsive, special operations aviation support to special operations forces worldwide.

The Special Operations Aviation Training Battalion (SOATB), an element subordinate to the Special Operations Aviation Command, is currently taking the lead in formalizing the creation of an intelligence course tailored to train Army personnel to support the unique requirements of Special Operations Aviation. The SOATB has the


mission of conducting individual training and providing education to produce both crewmembers and support personnel with basic and advanced qualifications for the 160th Special Operations Aviation Regiment (SOAR), also known

as Night Stalkers. The proposed course aims to close identified training gaps by providing institutional follow-on intelligence training for newly assigned intelligence analyst Night Stalkers after the completion of combat skills assessment, also known as Green Platoon. Analysts will receive standardized training, and a professionalized course will drastically shorten the time it takes an analyst to become basic mission qualified, enabling the regiment to achieve improved military intelligence readiness more efficiently. The formalization of an Army aviation intelligence course, similar to the Marine Corps Squadron Intelligence Training Certification Course, would also provide intelligence personnel assigned to CAB S-2s the opportunity to cross-train with 160th SOAR intelligence personnel, allowing for an invaluable exchange of key lessons learned.

The 160th SOAR intelligence staff possess the preeminent expertise in supporting special operations aviation missions; they are among the Army's most talented intelligence professionals. Over the past several years, senior analysts and AMSO pilots from across the 160th SOAR have collectively codified years' worth of tacit knowledge derived from operational experience into standard operating procedures. More recently, 160th SOAR analysts have worked closely with the SOATB to translate the knowledge and tradecraft within these standard operating procedures into training tasks that will serve to form the foundation for the planned aviation intelligence course. While a formalized Army aviation intelligence course remains in development, in January 2019 the 160th SOAR's senior intelligence technician led an initial Analyst Academy, largely based on training tasks earlier mentioned, capturing valuable lessons learned to aid in future course development. With the Army's push to address force readiness requirements for large-scale ground combat operations, the Special Operations Aviation Command intelligence enterprise aims to promote aviation intelligence education across the force that will enable Army aviation to adapt and prevail in next-generation warfare.

Conclusion

The contemporary and future operational environments will be contested in every domain, presenting a far more significant challenge to Army aviation engaged in large-scale combat operations. Army aviation intelligence has been

neglected for too long and requires urgent attention to prepare the next generation of intelligence professionals with the adequate skills and knowledge to effectively support one of the Army's critical capabilities. Interim solutions such as leveraging AMSO training opportunities and cross-service schooling with the Marine Corps will not adequately contribute to building the more lethal force upon which our Nation depends. According to the 2018 National Defense Strategy, "the creativity and talent of the American warfighter is our greatest enduring strength,"¹¹ and our Soldiers deserve the training that allows them to operate at full capacity. Short of outpacing our competitors through advanced development in next-generation military equipment, focusing our efforts to enhance training can address operational deficiencies and give our forces both strategic advantage and tactical overmatch against our adversaries. 

Endnotes

1. Office of the Secretary of Defense, *Summary of the 2018 National Defense Strategy of the United States of America*, n.d., 1, <https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf>.
2. Ibid., 3.
3. Margaret-Elizabeth Troxell, "Educating the Aviation S-2 for Success," *Aviation Digest United States Army* 5, no. 4 (October-December 2017): 26-27, http://www.rucker.army.mil/aviationdigest/assets/archive/AVN_DIG_2017_11-15.pdf.
4. Ibid., 27.
5. Ibid., 26.
6. Corby Koehler, "Fixing aviation intel," *Armed Forces Journal* (June 1, 2013), <http://armedforcesjournal.com/fixing-aviation-intel/>.
7. Ibid.
8. Corby Koehler and Christopher Tatakra, "Intelligence Support to Combat Aviation Brigade," *Military Intelligence Professional Bulletin* 39, no. 2 (April-June 2013): 4-12.
9. Jason Jimenez, "SITCC teaches language of aviation to Intelligence Marines," United States Marine Corps website, February 27, 2016, <https://www.cherrypoint.marines.mil/News/Article/674724/sitcc-teaches-language-of-aviation-to-intelligence-marines/>.
10. Koehler, "Fixing aviation intel."
11. Office of the Secretary of Defense, *Summary of the 2018 National Defense Strategy*, 8.

CW3 Brandon Mesa is currently the senior intelligence chief for the Army Special Operations Aviation Command headquartered at Fort Bragg, NC. He has a bachelor of arts degree in intelligence studies from the American Military University and a graduate certificate in China geostrategic intelligence issues from the National Intelligence University. He is on track to finish his master of arts in military studies at the American Military University. CW3 Mesa is also a graduate of the Army Warrant Officer Intermediate Level Education.



U.S. Army Special Operations Forces Military Intelligence Training Strategy

by Master Sergeant Thad R. Heiges

Introduction

In 2016, U.S. Army special operations forces (ARSOF) intelligence leaders began assessing training requirements for the ARSOF military intelligence force. The goal was to ensure continued support to ongoing operations while preparing the force to support U.S. Army Special Operations Command (USASOC) Strategy-2035. This deliberate, collaborative process focused initially on the special forces groups and sought to develop an ARSOF Intelligence Training and Readiness Strategy. ARSOF intelligence leaders worked with subject matter experts from across ARSOF and within the U.S. Army Intelligence Center of Excellence, as well as with Department of the Army G-2 readiness and training representatives, to create a tiered certification plan for ARSOF that would be analogous to the Army's Military Intelligence Training Strategy (MITS).

ARSOF MITS was developed through several USASOC G-2 hosted working groups consisting of senior intelligence officers, warrant officers, and noncommissioned officers from 1st Special Forces Command and its subordinate organizations, 75th Ranger Regiment, U.S. Army Special Operations Center of Excellence, and U.S. Army Special Operations Aviation Command. These leaders conducted an in-depth analysis to determine the core capabilities for ARSOF's intelligence warfighting function. This analysis yielded 16 common-to-all platform (Tier 2) tasks. In addition to the 16 common tasks identified, if necessary, O6 level commanders can determine additional tasks that more closely support theater-specific requirements.

The Intent and Planning Process of ARSOF MITS

MITS was designed to ensure the readiness of assigned intelligence personnel to perform their intelligence support

functions. It ensures military intelligence Soldiers, team/crews, platforms, and staffs are trained to conduct established mission essential task lists (METL) tasks under realistic conditions and to required standards. This same standard applies to all USASOC formations, as well as U.S. Army National Guard and U.S. Army Reserve military intelligence personnel.

The Commanding General, USASOC, has endorsed ARSOF MITS. He has directed its expansion across the ARSOF formation and its incorporation into the command education and training guidance and USASOC Regulation 350-1, *Training and Leader Development*. Unit readiness reporting requirements and semiannual training briefings will include focused discussions on MITS-driven training and readiness requirements.



Figure 1. ARSOF MITS Purpose and End State

The following are key points about the intent of ARSOF MITS:

- ◆ ARSOF intelligence readiness is not a new training requirement, but rather a clarification and codification of commanders' requirements for intelligence warfighting function readiness, and a delineation of responsibilities for intelligence training, certification, and validation.
- ◆ The approach nests with the Army MITS and Objective-Task concepts. It facilitates P2 category funding, as well as resourcing and training opportunities for special operations forces and conventional forces integration, interoperability, and interdependence.
- ◆ Tasks were selected using a bottom-up approach. Military intelligence leaders from across the subordinate commands and units have voiced their command-

ers' vision for intelligence training and readiness to working groups.

- ◆ The strategy allows units to retain the flexibility to determine the right mix of live, virtual, constructive, and gaming training enablers to support training events that replicate the anticipated operating environment.
- ◆ Tasks have clearly defined performance measures that allow leaders to ensure that training is executed to standard. They enhance interoperability of ARSOF intelligence with other special operations forces, Service, and joint partners.
- ◆ The training model will ensure leaders focus on critical tasks to sustain proficiency, sustain core individual and collective skills and knowledge, train staff elements, and enhance leader oversight of intelligence training.
- ◆ The approach is easily adaptable to allow multi-echelon and concurrent training.
- ◆ This strategy creates a baseline standard across ARSOF intelligence and in no way restricts any additional training requirements that the commander or theater special operations command identifies.

MITS Certification

MITS provides guidelines, resources, certification standards, and evaluation processes to assist commanders, G-2s, S-2s, and military intelligence detachment commanders in determining and maintaining the combat readiness of their intelligence personnel. Commanders, G-2s, and S-2s will ensure that Soldiers within the intelligence warfighting function receive the training required to achieve and maintain MITS certification. Three primary components exist to achieve this goal:

- ◆ First—Implement the MITS individual, team/crew, platform, and staff training and certification program.
- ◆ Second—Ensure leaders provide sufficient resources, including training time and funding, to conduct all aspects of intelligence training.
- ◆ Third—Require that each organization publish a unit and/or section 18-month training calendar that synchronizes the training plans, known mission/exercise requirements, and training program of the next higher headquarters.

Each unit conducts MITS training as part of the overall unit-training program. This may include training in garrison, field training/exercises, staff exercises, and combat training center rotations. MITS certification must be evaluated, routinely and thoroughly, to determine shortfalls and

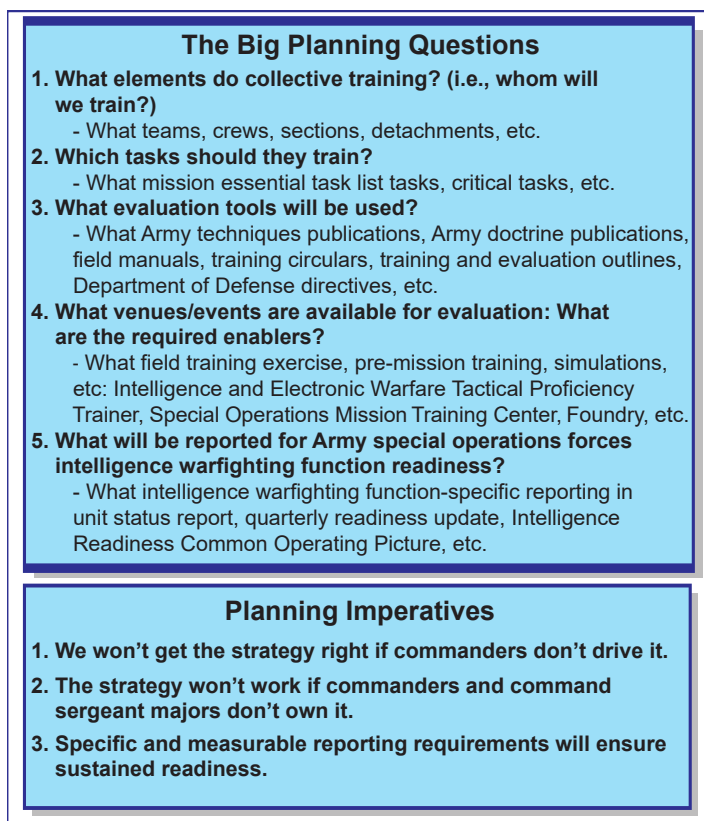


Figure 2. ARSOF MITS Planning Considerations

future training requirements, in addition to the unit's METL, Department of the Army/Department of Defense directives, and guidance from the supported theater special operations command. Sufficient resources and time are not available to train every collective task equally well. Commanders and other leaders ensure unit training plans prioritize training mission essential tasks first. Unit training priorities are based upon guidance from the higher commander, time, and available training resources. The commander manages their unit training toward proficiency in these collective tasks.

Months 1 through 3. ARSOF MITS is conducted with each unit on an 18-month, four-tier phased approach to certifying the individual (Tier 4), team/crew (Tier 3), platform (Tier 2), and intelligence warfighting function (Tier 1). Using an 18-month training timeline, the first 3 months are for individual certification. Individual training enables the mastery of fundamentals skills. Individual Soldier skills and proficiencies establish a solid foundation for units to train the more complex collective tasks at the unit level. Building this foundation at the Soldier level is key to the ability of the unit to ultimately perform its mission. Unit noncommissioned officers ensure Soldiers meet individual task proficiencies and work to ensure sustainment of those proficiencies. All 35-series Soldiers within the intelligence warfighting function will conduct Tier 4 training for their individual mili-

tary occupational specialty. This training is conducted at the section level within brigade and group, as well as at the battalion and detachment, and it is evaluated by section leadership (staff sergeant or above). The individual military occupational specialty tasks are those identified within the training and evaluation outline (T&EO) of the crew-level tasks (Tier 3).

Months 4 through 6. Continuing on the training timeline of events, months 4 through 6 focus on crew-level certification. Based on the accomplishment of task proficiencies at the individual level, units conduct collective training. This is done at home station, at maneuver combat training centers, during joint training exercises, and while deployed. Collective training is the essence of teamwork and develops mutual trust, which is essential to developing effective, cohesive teams. A military intelligence crew consists of two or more individuals who perform a specific set of critical intelligence collection or analytical tasks (e.g., counterintelligence team or special operations team-alpha) conducted at the level of battalion or below, which are evaluated by the leadership of similar crews from sister, or higher, units. The Tier 3 task list is derived from the supporting collective tasks identified within the T&EOs of the Tier 2 tasks.

Months 7 through 9. Months 7 through 9 are used to perform platform certification. A platform is the collaboration of two or more crews to perform a discipline activity (e.g., all-source production section) at the battalion level or above. Commanders must validate platforms while considering the following: the assigned mission, the unit level being supported (e.g., advanced operational base, special operations task force, or combined joint special operations task force), and the intelligence analysis capacity required to accomplish the mission. Military intelligence leadership from outside the unit conducts the evaluations of platforms; this leadership may be from higher headquarters; a sister organization; or special operations forces and conventional forces integration, interoperability, and interdependence with collocated military intelligence units. It is intended that the evaluated tasks be those 16 that are common to all and were yielded through the aforementioned working groups. The T&EOs are the Army's published standards for these tasks.

Months 10 through 18. Completing the training timeline through months 10 to 12 is Tier 1, an evaluation of the intelligence warfighting function. This is the combined evaluation of all platforms within a battalion/group/brigade. This is the ultimate evaluation of an organization's readiness before a combat training center rotation or 6-month deployment. The evaluation occurs at the battalion level, or above,

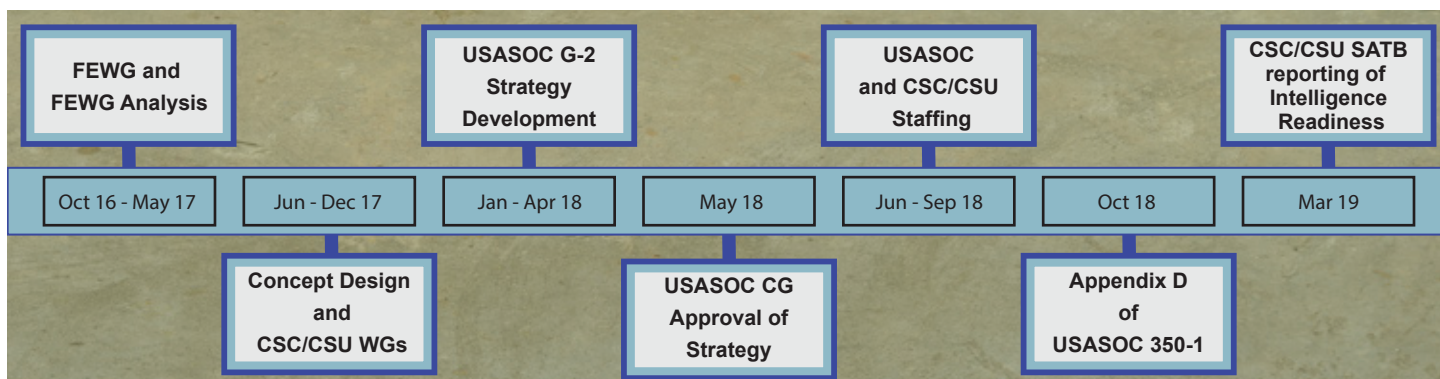



Figure 3. ARSOF MITS Strategy Development Timeline




in order to evaluate all intelligence platforms. The higher headquarters intelligence leadership evaluates the tasks (i.e., 1st Special Forces Command evaluates special forces groups, and groups evaluate battalions).

Conclusion

Like the Army's conventional force MITS, ARSOF MITS provides leaders at all levels clear guidance and expectations for the training and readiness of their intelligence force. It also drives the training management and resourcing pro-

cess, thus providing a framework and timeline for applying training resource management models specifically to intelligence training requirements. Once fully implemented and matured, and with transparent accountability requirements for intelligence force readiness, Army special operations intelligence Soldiers and elements will be trained and ready to meet national defense strategy, U.S. Special Operations Command, and theater requirements. 

MSG Thad Heiges is currently the U.S. Army Special Operations Command G-2 Sergeant Major. Previous assignments include 3rd Special Forces Group Analysis and Control Element noncommissioned officer in charge and Headquarters and Headquarters Company, 525th Expeditionary Military Intelligence Brigade, First Sergeant.

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 –


- Resident (TDY) or at a Foundry Site
- Live Environment Training
- 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



SGT Justin L. Bertoni, 3rd Brigade Combat Team, 10th Mountain Division, looks at his display as he prepares to launch the Black Hornet III during field testing at Fort A.P. Hill, VA.

Unstoppable Small Unmanned Aircraft Systems

by Captain Sean D. Hayball, Captain Peter L. Kerkhof, and Sergeant First Class Ryan K. Sarver

Introduction

"All the business of war, and indeed all the business of life, is to endeavour to find out what you don't know by what you do; that's what I called 'guessing what was at the other side of the hill.'"¹ Around 200 years ago, the Duke of Wellington said the whole art of war consisted of being able to see over the next hill. Today, units have the capability at the squadron and troop level to see the enemy with clarity beyond Wellington's wildest dreams. Using small unmanned aircraft systems (SUAS), units can now see over the hill, fully prepared to fight an enemy. U.S. Army formations can gain information and target the enemy with organic systems better than at any point in history. As a result, SUAS usage is a key enabler to unit lethality in the 21st century.

Units at the Joint Multinational Readiness Center (JMRC) that want to employ SUAS face several challenges when conducting operations to include:

- ◆ Maximizing use of SUAS with regard to their range, time flown, and priority intelligence requirements (PIRs) answered.
- ◆ Proficiency of operators.
- ◆ Effectiveness of staff processes for tasking SUAS collection in conjunction with the information collection matrix to answer the commander's PIR.

This article describes how rotational units at JMRC adapted elements of the opposition forces (OPFOR) tactics, techniques, and procedures (TTPs) to begin overcoming these

challenges. It also provides lessons learned for other units to implement an effective SUAS program.

Initial Opposition Forces Implementation at the Joint Multinational Readiness Center

In 2015, the JMRC OPFOR began a rapid expansion of SUAS use. The OPFOR consistently flies more than 50 hours per rotation using a mix of Puma, Raven, and quadcopter flights. At times, the 1st Battalion of the 4th Infantry Regiment SUAS use seems unstoppable. For each exercise, OPFOR SUAS collection exceeds that of rotational unit's Shadow and SUAS flight hours combined. OPFOR does this through daily operations and intelligence working groups, dedicated SUAS teams, and a capable, enduring battalion master trainer program.

Rotational Unit Analysis

JMRC observer-coach-trainers followed the evolution of one rotational unit's (Cougar Squadron or 2nd Squadron, 2nd Cavalry Regiment [2/2 CR]) progress as it developed its SUAS program over several training exercises. This squadron noticed the OPFOR's SUAS dominance and developed a good squadron program through JMRC exercises Allied Spirit IV and V. Later, while in the Baltics for exercise Atlantic Resolve North and serving as the headquarters for the North Atlantic Treaty Organization's first Enhanced Forward Presence battle group in Poland, the unit implemented lessons learned from its rotations at Hohenfels, Germany, pooling teams of pilots at the squadron level with Pumas, Ravens, and quadcopters on a real-world, deployed mission. The 2/2 CR also shared ideas and TTPs with members of the United Kingdom's Princess of Wales Royal Regiment

and the Norwegian SUAS operators. This cross-pollination of ideas is a success story of multinational interoperability.

As part of developing the SUAS program, the squadron consolidated operators and the squadron's master (Raven) trainer under the S-3 and S-2 to maximize the use and focus of assets, track flight hours and training, and answer the commander's PIR through information collection planning. They also improved and further developed operators' call for fire skills and information collection capabilities, proving in numerous exercises and force-on-force events that they could effectively communicate targeting information from sensor-to-shooter and provide timely effects. This allowed the unit to synchronize assets at the squadron level and leveraged those assets employed in support of the squadron's decisive operation. The unit conducted several very successful fires missions while watching the Raven feed on the One System Remote Video Terminal (OSRVT) during exercise Puma in Orzysz, Poland, in May 2017. The unit then fully appreciated SUAS as an asset that offered a significant advantage as an intelligence, surveillance, and reconnaissance (ISR) and fire-support capability.

Beginning with exercise Allied Spirit V at the JMRC (September to October 2017), the unit continued to restructure its task organization of Raven and Puma systems and operators. Cougar Squadron (2/2 CR) built on this initial concept and effectively collected information with SUAS. They accomplished this by employing the Pumas deep and the Ravens in closer during exercises in Poland and exercise Saber Strike 17 in Poland and Lithuania. The squadron added SUAS tasks to the information collection matrix in order to answer PIRs and managed assets at the squadron level. The unit successfully identified targets and called for fire on enemy BMP infantry fighting vehicles, by tasking the Puma system to cover deeper named areas of interest (NAIs), while Ravens covered close-range NAIs. In exercise Saber Strike 17, the unit adopted techniques that the OPFOR and multinational partners used with their SUAS. The unit did this by—

- ◆ Dedicating vehicles for the SUAS team with power inverters and battery chargers to ensure continuous flight capacity.
- ◆ Adding vehicle-mounted antenna masts to improve line of sight/range.
- ◆ Mounting Ground Control Station monitors.

In Poland and Lithuania, 2/2 CR conducted a multinational fire support coordination



Photo by U.S. Army SSG David Overson

U.S. Army SGT Christopher Curley, an infantryman with small unmanned aircraft systems operator duties, with 1st Battalion, 4th Infantry Regiment, Joint Multinational Readiness Center, Hohenfels, Germany, prepares to launch an RQ-11 Raven unmanned aerial vehicle for reconnaissance purposes during training.

exercise, with the battle group's British cavalry company and organic troops integrating fire support officers who watched the live Raven feed on the OSRVT. The call for fire missions were successful, and this exercise showed the unit how to develop a synergistic relationship and sensor-to-shooter linkage between the British reconnaissance units, organic troops, fires, and intelligence sections.

With one SUAS team deployed, the unit clocked 19.4 flight hours, or 31 sorties, including two at night. These flights supported 13 fires missions, answered the commander's PIR for the identification of the enemy main body, and enabled the destruction of more than 20 BMP infantry fighting vehicles. This exercise became a live-fire benchmark because most units fly fewer than 3 hours during a live-fire exercise (if they use their SUAS at all). Synchronizing targeting over the fires net while each troop watched on the OSRVT allowed the troops to see the battlefield and gain an appreciation of the tangible benefit of using SUAS in support of their operations. As the squadron assumed the training and management of the SUAS, troop-level commanders were able to fight and, when needed, request UAS capabilities from the squadron while the burdens of management of pilots, restricted operating zones, and security for the Ravens were taken off their busy task list while in contact.

For the unit's live-fire exercises in Poland, the squadron successfully integrated SUAS within a troop's maneuver and air plan. The squadron deconflicted airspace between SUAS and AH-64 Apaches. Using SUAS to identify the enemy counterattack, the unit cued the AH-64s in support of the troop, enabling the AH-64s to destroy a significant number of enemy forces in a support-by-fire role.

These successes led the squadron to adjust its model for conducting SUAS operations. The squadron commander, working with the S-2, formally consolidated the master trainers and SUAS operators in the headquarters troop under the S-2 section. A squadron master trainer and two additional individual team master trainers are now with each of the two permanent teams. The teams conduct assigned missions, tasked by the operations officer, in order to enable the squadron commander and S-3 section to drive future operations and answer the commander's PIR.

Execution and Implementation

SUAS operators work in a four-man section with one dedicated vehicle per team. One team acts as the launch and recovery team for the Raven or Puma, depending on mission requirements, while the other team operates as the forward station. During missions, the launch and recovery team launches the SUAS and flies it until the forward team takes control of the asset. The teams conduct an electronic

handoff, and the forward team flies the SUAS mission. When the battery is low or weather no longer permits the flight, the forward team returns the SUAS to the launch and recovery team. At this point, the recovery team lands the asset in a safe or more secure area to mitigate risk.

The launch and recovery team maintains all aircraft except when the forward team has control. Therefore, while one air vehicle is operating, the rear team can prepare the next SUAS and have it launch-ready before landing the first aircraft. This method allows the squadron to maintain near-continuous ISR coverage of the operational area using organic capacity. It also allows greater flexibility for dynamic re-tasking as the two teams handover aircraft control and bound as necessary to support different missions. The vehicles consist of two modified high mobility multipurpose wheeled vehicles (HMMWVs), allowing the SUAS teams to conduct operations with minimal exposure outside the vehicle. The added benefit of employing multiple teams is the ability to use multiple SUAS systems simultaneously in different configurations, depending on mission requirements. The unit can employ Puma and Raven, Puma and quadcopter, or Raven and quadcopter. Units can potentially use this TTP to conduct launch, recovery, and SUAS handover from the SUAS team to scout observation posts, forward observers, etc.

Based on the lessons learned from the JMRC and observations from the OPFOR's success, as well as multinational TTPs identified while deployed to the Baltics in 2016 and Northeastern Poland in 2017, Cougar Squadron's SUAS program adjusted and experimented with several different configurations that merit the capture of important lessons and TTPs for other Army units.

Lessons Learned

This unit's lessons include moving SUAS management to the squadron level for better focus on NAIs, having the ability to answer the squadron commander's PIRs, and improving understanding of the situation across the unit's frontage. The ability to conduct almost continuous SUAS operations at critical times was an obvious battlefield advantage for the squadron. By emphasizing the importance of SUAS, investing in training, and allocating resources to a battalion SUAS master trainer program, the squadron commander, S-3, and S-2 were able to increase lethality and survivability by integrating information collection, maneuver, aviation, and fires with its organic systems.

A problem unintentionally solved by managing the master trainers and pilots at the squadron level was that near-continuous collection can occur and personnel shortfalls due to

turnover are overcome by maintaining a strong program of trained operators with longevity.

Tactics, Techniques, and Procedures

The 2/2 CR adopted TTPs from the JMRC's OPFOR and developed additional TTPs through real-world deployments to the Baltics and JMRC rotations during exercises Allied Spirit IV, V, and VIII. These TTPs are now a large part of what 2/2 CR and other units are doing to enhance their SUAS programs. The 2/2 CR improved in the following areas:

- ◆ Conducting collection management.
- ◆ Utilizing an organic SUAS advantage through Puma, Raven, and quadcopter use.
- ◆ Equipping and task organizing teams to echelon systems.
- ◆ Accepting and mitigating risk.
- ◆ Employing fires and reconnaissance TTPs through an iterative training process.

These TTPs greatly increased the unit's effectiveness, continuing to improve the unit's performance through each exercise. The following is a brief description of the TTPs that others can apply to their SUAS program.

Collection Management. Two key elements of collection management are cueing (when one asset triggers the use of another) and mixing (using two or more different assets to refine collection). Collection managers use SUAS for quick target identification. Whether using a Puma's longer loiter time, infrared capability of the Puma and Raven, or hover capability of a quadcopter, an SUAS team can quickly identify targets. Using SUAS for target acquisition can be faster than ground movement, can support maneuver with a mitigated risk of observation, and can provide greater refinement to ground observation. By using SUAS, a commander has the ability to rapidly acquire a target, leverage higher-level fires, and implement combined arms maneuver techniques to achieve dominance on the battlefield.

Organic Advantage. SUAS has the added advantage of rapid employment. In 15 minutes or less, a troop has access to an organic ISR asset with trained crews, in comparison to requesting a Shadow or higher-level assets. SUAS are significantly faster and more agile to employ, with few of the technical challenges of establishing communications with nonorganic enablers. Several units at the JMRC achieved enough proficiency to launch and recover SUAS on the move

(i.e., from an HMMWV, Stryker, or Bradley), adding mobility and survivability to the Ground Control Station team. Doing this requires the operator of the Ground Control Station's home location to perform consistent system updates to recover the SUAS if the data link is lost. However, this technique also allows overhead observation ahead of a moving unit.

Puma Use. The Puma system has the advantage of longer station time and range than either a Raven or a quadcopter system. Units tend to use the system at longer range or for objectives requiring greater loiter time for better target refinement. The Puma's 20-kilometer range and almost double battery life (as opposed to the Raven's 10-kilometer range) allows for layered information collection planning in coordination with Raven systems and other collection platforms.



PVT Jonathan Jackson, a cannon crew member assigned to 82nd Brigade Engineer Battalion, 2nd Brigade, 1st Infantry Division, Fort Riley, KS, launches a Puma small unmanned aerial system during a multinational joint equipment training brief April 2, 2018, in Grafenwoehr, Germany.

Quadcopter Use. Commercially available quadcopters operate from 15 minutes to 1 hour. The advantages of a quadcopter are—

- ◆ Rapid employment.
- ◆ Hover capability (along or in tree lines and towns).
- ◆ Capacity to drop small munitions.
- ◆ Reduced signal signature (lower power output than Puma or Raven systems).

These advantages enable small teams to quickly employ the collection asset forward, scan routes, acquire targets, and move. As a result, OPFOR reconnaissance elements prefer this method of using SUAS, whether in the close fight or in deep reconnaissance. As units refine their TTPs, adopting this method can greatly increase situational awareness forward.

Resource Allocation. For units maintaining SUAS at the battalion or squadron level, a successful technique is to provide a dedicated vehicle with communications equipment allocated for each SUAS team. This allows direct communication from the battalion tactical operations center to the collection asset. When the SUAS team is enabled with a vehicle and radios, the team can relay PIRs directly and the battalion ensures refined reporting. The team can also be tasked to other requirements quickly, or when possible, the properly and well-trained team can conduct a call for fire.

Echeloning Systems. The proliferation of SUAS assets at the battalion or squadron level allows the echeloning or layering of systems throughout the formation. Based on the advantages and capabilities of each system, a method of echeloning SUAS is to use Pumas at the battalion or squadron level, Ravens in the area closer to company and troops, and quadcopters along the forward line of own troops. Critical to this is investing in an increased number of trained operators. Echeloning SUAS maximizes a unit's ability to ensure continuous reconnaissance, increasing overall capacity rather than re-allocating teams throughout the battlespace. By increasing overall capacity, the unit can acquire targets and clear NAIs faster, quickly conduct battle damage assessment, scan routes, and decrease the need to move brigade or regimental SUAS assets throughout the battlespace. This has the added advantage of enabling the regiment to focus collection efforts forward of the front line of troops or more consistently in support of the regimental decisive operation.

Risk. To employ SUAS teams effectively, forward units must accept some level of risk. Units mitigate risk through training, proper employment, and cost-benefit analysis. The following benefits consistently outweigh the risk associated for a single team:

- ◆ Answering the PIR.
- ◆ Determining the trafficability of routes.
- ◆ Screening a flank.
- ◆ Acquiring and engaging a high-payoff target with fires.
- ◆ Performing accurate battle damage assessments.

Risk mitigation occurs because SUAS enables greater lethality, battlefield visualization, and survivability for the entire unit. Using the forward teams in combination with forward reconnaissance elements will provide some security for these valuable assets while allowing them the best possible terrain to conduct operations.

Risk Mitigation. With the current reconnaissance/counter-reconnaissance, unmanned aircraft system (UAS)/counter-UAS environment and with the possible peer capabilities, one risk mitigation technique to use is SUAS password protection. Units using simple passwords often risk compromise of the system's data link or risk adversaries taking control of the SUAS asset. Developing strong passwords can prevent the enemy from live-feed observation or prevent the enemy's control of the asset. Units employing strong passwords prevent enemy forces from observing the live feed, identifying the return location of the system, or capturing the system.



U.S. Army PVT Brandon Ruehl (right) and U.S. Army SGT Jesse Moore, infantrymen with small unmanned aircraft systems operator duties, with 1st Battalion, 4th Infantry Regiment, Joint Multinational Readiness Center, Hohenfels, Germany, prepare to fly a quadcopter for reconnaissance purposes during training.

Photo by U.S. Army SSG David Overton

Fires Integration. Fires integration increases for units using SUAS in two areas. When units use SUAS in direct support to operations, they more effectively acquire and target in depth and deliver greater effects than when they rely solely on direct observation from an observation post or within an engagement area, especially in hilly or varied terrain. In cases where units use SUAS in support of upcoming operations, units identify and refine targets earlier, enabling pre-plotted fires to support rapid maneuver.

Employment. Some effective TTPs for SUAS include the SUAS team identifying the trafficability of a route or trail, conducting observation over the hill and target identification, and cueing a reconnaissance element. The reconnaissance element maneuvers to gain direct observation of the target from a concealed position. The reconnaissance element identifies indicators to answer the commander's PIR, conducts calls for fire, and attrits the enemy force. Additionally, the element either enables the forward passage of lines of follow-on forces or maneuvers to the next

NAI. The JMRC OPFOR in the offense consistently and effectively uses this TTP, and now observers/coaches are seeing units with multiple rotations at the JMRC use these tactics in training and while deployed.

Training Integration. The 2/2 CR's, OPFOR's, and other rotational units' training development at the JMRC shows that many opportunities exist for units attempting to maximize SUAS training. Training opportunities at home station are squadron, platoon, or company situational training exercise lanes; live-fire exercises; or troop-level force-on-force exercises. Taking these opportunities refines a Soldier's proficiency, TTPs, and best practices. Through command emphasis, planning, and continuous incorporation into normal training events, any unit can develop a dominant SUAS program.

Program Management

The 2/2 CR implemented several key changes to improve its SUAS program management. Beginning with the command team's increased emphasis, the unit developed a master trainer and operator training program at the squadron level, which it then used to track proficiency and maintain the aircrew training program. By implementing this program, 2/2 CR greatly increased information collection capacity to answer the commander's PIRs and support targeting. What follows is an explanation of how program management can sustain proficiency and the publications that can help other units develop a strong SUAS program.

Command Emphasis. Battalion/squadron leadership should invest in the SUAS program and provide input to junior leaders. The incorporation of SUAS tasks into home-station training, as well as their use in the combat training center environment, is necessary to build qualified and competent operators who are confident in employing their systems. The battalion/squadron commander establishes the commander's critical information requirements; therefore, he or she has a vested interest in seeing SUAS employed to their maximum capability in order to answer those requirements. Commanders who understand the capability and reinforce SUAS usage gain an information collection capacity up to 20 kilometers from the forward line of own troops and the ability to gain targeting information using that capability.

Squadron/Battalion and Regiment/Brigade Master Trainers. The importance of having a master trainer at the battalion and brigade level cannot be overstated. According to TC 3-04.62, *Small Unmanned Aircraft System Aircrew Training Program*, master trainers conducting initial qualification training must be designated by the first O6 in the

chain of the command. The training circular states, "Those [master trainers] MTs selected to conduct initial qualification training [in accordance with] IAW an [U.S. Army Aviation Center of Excellence] USAACE-approved program of instruction, and appendix will be designated by the first colonel in the chain of command. Initial qualification training will be managed at brigade level or higher by a designated MT that is a qualified graduate of the MT course, current and [mission qualified] MQ."² Squadron master trainers should align concurrent training for operators, tracking and logging flight hours by using the SUAS Manager system. These master trainers can also leverage SUAS assets to support operations regardless of whether a unit decides to consolidate its SUAS teams at the battalion/squadron level or to keep them integrated at the company/troop level. The key to this is the flexibility of the SUAS teams to move and communicate with higher and adjacent unit headquarters. Master trainers help manage collected information and should be an integral link between intelligence and operations sections. The 2/2 CR did this effectively by incorporating sergeants to oversee individual aircrew teams, as well as a staff sergeant at the squadron level who manages the program and provides guidance for crew evaluations and qualifications to the aircrew team sergeants.

Requirements. Each operator must attend the 10-day SUAS initial qualification course. The operator then receives a status of mission preparation following graduation from the course. Subsequent home-station SUAS training must be conducted in accordance with the established aircrew training program of the unit under the supervision of the master trainer(s). When they complete all 10- and 20-level tasks associated with their unit and any 30-level tasks required by the unit's particular mission set, operators gain mission qualified status. Two mission-qualified operators can operate the SUAS without the supervision of a unit master trainer. Chapter 4 of TC 3-04.62 gives examples of how to create unit-specific tasks for operators.³ Unit master trainers should work closely with commanders to develop these tasks. Chapter 3 of ATP 3-04.64, *Multi-Service Tactics, Techniques, and Procedures for the Tactical Employment of Unmanned Aircraft Systems*, gives good examples of SUAS techniques employed during various missions for surveillance and reconnaissance that translate into tasks for a unit to train operators on improving their proficiency.⁴ The 2/2 CR's establishment of its aircrew training program consisted of additional 30-level tasks; for example, identification of enemy forces, assessment of their size and composition, conduct a call for fire, and set up and maintain communications.

Currency and Operator Proficiency. Mission qualified operators must complete a simulator flight every 30 days and a live flight every 150 days. They must also complete the Semi-Annual Proficiency and Readiness Test in order to maintain active currency on their assigned system; however, this mandatory training is not enough to develop proficient operators. The key to developing proficiency is the incorporation of SUAS activities into ordinary home-station unit-level training, as well as dedicating times to conduct live flights. This allows operators to use the systems in a variety of scenarios and environments to better prepare for

exercises, SUAS use has the added benefit of reinforcing a Soldier's need to implement camouflage, cover, concealment, and deception techniques to avoid SUAS detection.

Maintaining the Aircrew Training Program. It is important to develop SUAS operations and train new operators as a battle rhythm event. Identifying key personnel with unit longevity to attend the master trainer course is necessary to maintain the program and a substantial pool of qualified operators through times of high unit turnover. Doing this ensures program continuity and enables SUAS operational readiness without having to focus on a massive buildup before key events. Maintaining a depth of both master trainers and current, qualified operators allows the unit to focus on developing operator proficiency on TTPs rather than focusing on developing operator currency.

Way Ahead

The 2/2 CR conducted more than 20 hours of SUAS flights during the 8-day exercise Allied Spirit VIII in January 2018, supporting targeting and answering the commander's PIR. That is a dramatic increase from where the unit started. The average battalion at the JMRC conducts fewer than 3 hours of SUAS flights per rotation. The German winter played a role in preventing full use, including weather such as snow, ice, rain, and low cloud

cover. The 20-hour figure also stands out because of the airspace deconfliction challenges associated with working through a multinational brigade headquarters. To underscore the importance of this accomplishment, if a United States brigade employed the full use of SUAS assets at its disposal across three maneuver battalions and a reconnaissance battalion, the brigade would fly more than 80 hours of SUAS coverage without using a Shadow or higher-level asset during the German winter.

This accomplishment also shows that dominant SUAS is not just an OPFOR capability, but that any unit can develop a successful battalion/squadron-level SUAS program. Until recently, OPFOR provided unstoppable SUAS support to their maneuver forces, which greatly affected units without this capability. Other units, such as the 4th Squadron of the 10th Cavalry Regiment, 3rd Armored Brigade Combat Team, 4th Infantry Division, displayed a high degree of prowess during their 2017 Grafenwoehr live-fire exercise, when they incorporated the Raven SUAS by launching and using the system from one of their Bradley fighting vehicles while



Photo by U.S. Army CPT Joshua B. Good

CW4 Ralph Stroup, left, a student with the small unmanned aerial system course, teaches recruits from D Company, 2nd Battalion, 58th Infantry Regiment, about various drone aircrafts.

conducting SUAS operations in support of combat training center events. For currency purposes TC 3-04.62 states, "Currency in one series SUAS will satisfy the requirement for all SUAS within the series or group; separate currency is required for all other SUAS." ⁵ This means for operators to maintain currency on the Raven, they can fly any subsequent system within that set, ranging in size from the Puma down to the Wasp. Additionally, for a flight to count toward proficiency, the crew must launch, fly for a minimum of 15 minutes, and successfully recover the air vehicle.

Observation of the more successful units at the JMRC indicates they focus on developing aircrew proficiency during home-station training events and use their systems regularly. The 2/2 CR incorporates SUAS section training into all squadron, troop, and platoon situational training exercise training by conducting weekly crew training flights in their local training area. Implementing live-fire exercise and troop force-on-force SUAS training increases training opportunities for SUAS operators and supports a Soldier's SUAS awareness and reporting of SUAS. During force-on-force

on the move. The motivation of their command team, staff, and troop commanders enabled this progress. Observer/coaches saw several multinational partners, including the British Princess of Wales Royal Regiment and Norwegian forces, displaying similar prowess and motivation during exercise Saber Strike 17 in their employment and execution of SUAS tasks. The incorporation of British reconnaissance elements and SUAS teams in coordination with U.S. fire support officers highlights opportunities for multinational SUAS interoperability.

To capitalize on training opportunities, units can achieve rapid improvement using SUAS simultaneously with each training lane. This can include live-fire exercises, situational training exercises, or force-on-force iterations. Since the program allows for virtual training every 30 days and live training every 150 days, units can achieve proficiency by adding SUAS to normal training. Through disciplined repetition, the program will grow a cadre of trained operators.

The master trainer program is the critical factor for developing enduring SUAS capability. This program requires depth. The unit master trainer should train as many mission-qualified operators as possible that have longevity at the unit. The unit should also ensure continuity in training by consistently rotating its best operators through the master trainer course.


To ensure the battalion employs assets at the right place and time, the battalion should work on three key areas:

- ◆ Ensuring readiness by providing the necessary assets, enabling qualified SUAS teams to move through the battlespace and reach the correct NAI, with the ability to reach back to the battalion.
- ◆ Training operators at each of the troops. A broad distribution of assets will limit travel time and minimize the risk of losing one or even two teams.
- ◆ Ensuring the battalion evaluates and updates its information collection and tasking process through a nightly operations and intelligence working group. Covering SUAS collection tasks and priorities each night or phase allows operations to focus tasking, troops to orient on the reconnaissance objective, fires to develop updated target areas of interest, and the battalion to ensure continuous reconnaissance.

The easiest way to develop motivation for the SUAS program at the squadron level is to ensure squadron and troop commanders understand they are using an organic ISR platform that will enable fires integration in direct support of maneuver. Once the fire support officer uses SUAS to tar-

get enemy forces successfully for the squadron and troops, the record will show the effort is worth the outcome. With added command emphasis, a battalion can develop a master trainer program that enables effective use of SUAS in a decisive action fight.

As units develop a battalion master training program, creating a core of trained talent is critical to the success of the program. Giving teams the necessary assets for success will enable organic ISR collection immediately when needed. Refining staff standard operating procedures and working groups is key to ensuring those assets get to the right place at the right time to enable combined arms maneuver. Once a trained team of operators and staff members builds a high degree of proficiency, the next step is to expand the program across the entire formation. By doing this, the battalion will be able to echelon, or layer, SUAS collection throughout the formation, from the forward line of own troops to the battalion. As SUAS enables fires and maneuver across the formation, units attrit enemy forces faster with less risk to forces through indirect fires and they achieve a more rapid destruction of the enemy through well-informed maneuver. This type of SUAS utilization will increase the lethality and survivability of troops with each training event. The advantages gained will make SUAS at the battalion, once proven, unstoppable.

Battalions have at their fingertips the capability to employ more information collection assets immediately—seeing over the hill—better than ever before. The rapid expansion and proliferation of SUAS on the modern battlefield enables rapid targeting. Other nations and non-state actors now use their own SUAS to employ munitions and fires, enabling their own targeting and maneuver. Units employing organic SUAS gain the advantage by employing SUAS faster, rapidly collecting information, and putting steel on target. While higher-level assets are nice to have, waiting for them is not. As commanders add emphasis to SUAS programs, their ability to identify enemies and destroy them will increase exponentially. Once units train teams, allocate resources, and synchronize staff, the unit's lethality will increase. By implementing a broad program with capability across the formation, the unit can employ SUAS in any direction, at will against any opponent unable to field SUAS. This is what it means to have unstoppable SUAS. 

Endnotes

1. Arthur Wellesley, 1st Duke of Wellington, quoted in Louis J. Jennings, ed., *The Croker Papers: The Correspondence and Diaries of the Late Right Honourable John Wilson Croker, LL.D., F.R.S., Secretary of the Admiralty from 1809 to 1830, Volume III* (London: John Murray, 1884), 276. Statement in conversation with John Croker and Croker's wife (4 September 1852).

(Continued on page 93)

Preparing the Redesigned Company Intelligence Support Team for Decisive Action Employment

by Lieutenant Colonel Anthony Barbina, Captain Alex Reinwald, and Captain Michael Heim

Introduction

In May 2017, the modified table of organization and equipment (MTOE) for the brigade combat team (BCT) military intelligence (MI) company changed to add 21 intelligence analysts—with military occupational specialty (MOS) 35F—to serve as the company intelligence support team (COIST) for the BCT. The change to the MTOE did not come with changes to ATP 2-19.4, *Brigade Combat Team Intelligence Techniques*; TC 2-19.400, *MI Gunnery for the Military Intelligence Company of the Brigade Engineer Battalion 1.0* [inactive];¹ or specific implementation guidance for distribution within a BCT. As a result, the MI company has 21 additional intelligence analysts but no doctrine on how to prepare, train, or employ them throughout the brigade.

Although the Army's original intent for the MI company COIST concept was for commanders within BCTs to allocate their COIST support to companies according to changing mission requirements, 1st Stryker Brigade Combat Team, 25th Infantry Division (1/25th SBCT) habitually aligns one COIST Soldier per maneuver company. This is done to form a lasting intelligence relationship at battalion and company levels that will allow for greater efficiency, cross-training, and support. This article describes the course of action that D Company, 70th Brigade Engineer Battalion, 1/25th SBCT, took to man, equip, and train the COIST for the brigade. It also highlights the lessons learned from COIST employment during decisive action operations.



U.S. Air Force photo by Alejandro Peña

Soldiers assigned to Charger Company, 1st Battalion, 5th Infantry Regiment, 1st Stryker Brigade Combat Team, 25th Infantry Division, U.S. Army Alaska, march to their next objective during Operation Punchbowl at Joint Base Elmendorf-Richardson, AK, February 10, 2018.

Background

The Army's original COIST concept called for intelligence support teams at the company level, consisting of one non-commissioned officer (NCO) and one junior enlisted Soldier. Doctrine describes a COIST as a team that "provides an analytical, production, and dissemination capability at the company level, providing the commander with options to exploit enemy vulnerabilities."²

As shown in Figure 1, these COIST Soldiers were assigned to their respective maneuver battalions. During deployment, especially during counterinsurgency operations, the COIST would train non-MI personnel to augment them, allowing for 24-hour operations and more rapid answers to the company commander's intelligence requirements.³ However, because of a grade plate and force reduction for the MI Branch, the Army reduced the number of MI NCOs within maneuver units. The result for the SBCT maneuver battalions was a reduction to only two 35F20s and four 35F10s to serve in the COIST role in addition to the intelligence analysts designated to fill the battalion/squadron S-2

positions. The battalions were only able to field two COISTs with an NCO, while the third COIST had only two junior enlisted Soldiers. This hindered the ability of the COIST to meet the requirement of training non-MI Soldiers to provide augmentation.⁴

In order to address the Armywide intelligence force reductions, the Army began looking for options to optimize the COIST capability within the BCT. The option that emerged removed some intelligence analysts from maneuver units and centralized them in the BCT's MI company, also shown in Figure 1. In the 1/25th SBCT's MTOE, each of the three infantry battalions lost three 35F20s and four 35F10s while the cavalry squadron lost two 35F20 and six 35F10s. For the SBCT, this means a total loss of twenty-nine 35Fs at the battalion level, consisting of eleven 35F20s and eighteen 35F10s.

To replace this loss of 35Fs within the SBCT, the Army added 21 intelligence analysts to the MI company, consisting of one 35F40, two 35F30s, four 35F20s, and four-

teen 35F10s. Additionally, the cavalry squadron gained one 35F30. The intent of this reallocation is to retain a COIST capability for the BCT commander that the commander can allocate according to priorities. The MI company commander prepares and trains the COIST and then pushes the COIST members out to supported units during missions. This new allocation of COIST Soldiers provides the BCT commander ten COIST teams for allocation, with seven of those containing an NCO. The different NCO grades can be distributed according to priorities of support and mission requirements.⁵

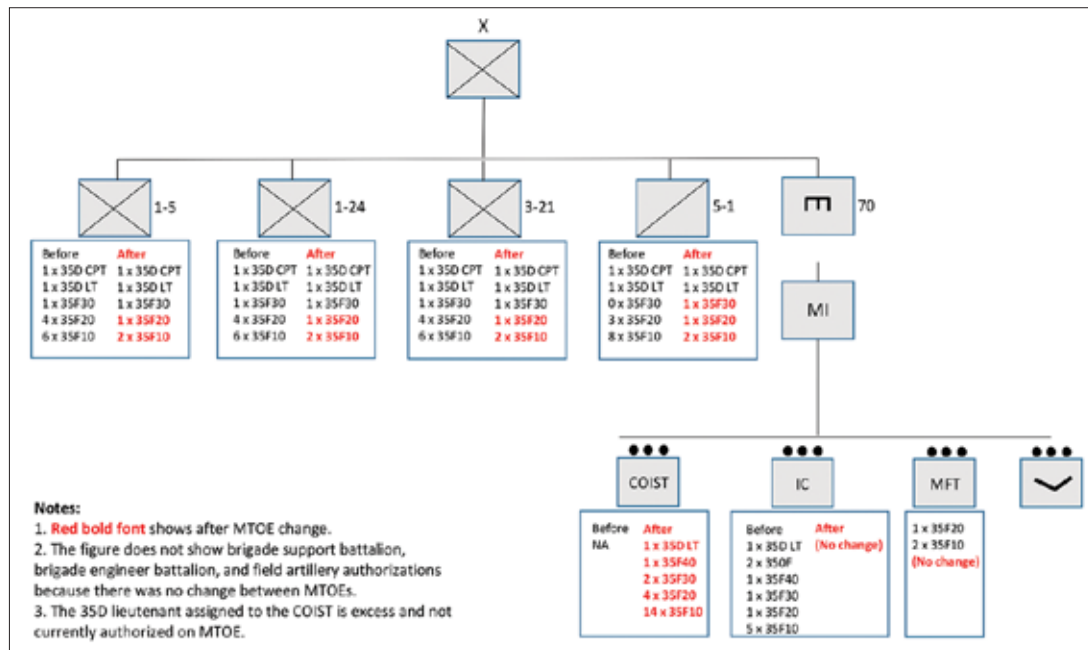


Figure 1. MOS 35F/35D Allocation within 1/25th SBCT Before and After MTOE Change

Man the Company Intelligence Support Team for the Brigade

Instead of following the Army's model of providing only ten COISTs for the BCT to allocate based on mission requirements, leaders of 1/25th SBCT focused on—

- ◆ Building relationships before training.
- ◆ Having intelligence experts certify COIST capabilities.
- ◆ Integrating COISTs with companies and battalions for all major training events.

The brigade followed the model of forward observers—artillery observers who carry the MOS 13F, Fire Support Specialist—when training and allocating Soldiers to a COIST. The 1/25th SBCT developed a plan to provide one intelligence analyst to the company and battalion levels to serve as the intelligence support for each maneuver company and maneuver battalion within the brigade. Much like the 13F model, each COIST habitually aligns with a supported company to build an enduring relationship and learn their

supported unit’s standard operating procedure. Similar to the relationship between companies and their fire supporters, 1/25th SBCT establishes a weekly battle rhythm between the supported companies, their battalion S-2s, and each COIST in order to build rapport, integrate into training, and gain the trust of their supported commander.

As shown in Figure 2, the 1/25th SBCT’s COIST concept maximizes NCO analysts at the battalion level to—

- ◆ Integrate with the battalion S-2.
- ◆ Manage information requirements.
- ◆ Support junior analysts within the companies.

The cavalry squadron receives the 35F30 because of its importance in the brigade’s information collection plan, and the brigade engineer battalion receives COIST augmentation enabling intelligence analysis and support to the SBCT’s consolidation area fight and wide area security operations. To leverage penetration of intelligence capability in every company, 1/25th SBCT aligns one 35F10 analyst with every maneuver company in the BCT. The MI company and brigade engineer battalion trains and develops these young Soldiers, habitually aligns their relationship, and pushes them down to the maneuver companies for all major training events. The intent of the COIST allocated to the mobile gun system (MGS) troop within the cavalry squadron is to augment the squadron if the MGS troop is task-organized elsewhere in the brigade. The brigade support battalion and field artillery battalion do not receive a COIST allocation. Significantly, the MI company exchanged the second authorized COIST 35F30 to the brigade intelligence support element for an additional 35F20 in order to properly man companies.

PL									
PSG									
35D					35F40				
5-1 CAV		1-5 IN		1-24 IN		3-21 IN		BEB (CIED/WAS)	
TRP	Name	COs	Name	COs	Name	COs	Name	COs	Name
SQDN	1x 35F30	BN	1x 35F20	BN	1x 35F20	BN	1x 35F20	BN	1x 35F20
SQDN/MGS	1x 35F20	A CO	1x 35F10	A CO	1x 35F10	A CO	1x 35F10	A CO	1x 35F10
A TRP	1x 35F10	B CO	1x 35F10	B CO	1x 35F10	B CO	1x 35F10	B CO	1x 35F10
B TRP	1x 35F10	C CO	1x 35F10	C CO	1x 35F10	C CO	1x 35F10		
C TRP	1x 35F10								

Figure 2. 1/25th SBCT COIST Allocation

During employment in a training cycle, the COIST Soldiers are typically under tactical control of their supported companies 2 weeks prior to any training exercise in order to integrate into the planning process and provide intelligence support prior to execution. As missions dictate, earlier integration is an option. As mentioned earlier, the MI company and brigade engineer battalion generally parallel the field artillery battalion’s training cycle for 13Fs and push the COIST over to the supported battalions around the same time.

As a critical component of the 1/25th SBCT COIST concept, the brigade authorized the MI company an additional lieutenant to serve as the platoon leader for a separate COIST platoon. While the MTOE identifies the COIST as part of the information collection platoon, the creation of a separate COIST platoon enables the company to focus on a specific training plan designed for COIST Soldiers and facilitates integration with supported battalions. This also allows the information collection platoon leader to focus on the brigade intelligence support element and geospatial intelligence operations.

Equip the Company Intelligence Support Team for the Brigade

With the change to the MTOE, the COIST platoon received ten Distributed Common Ground System-Army (DCGS–A) multifunction workstations and no other additional equipment. To ensure the COIST moves out to supported maneuver units with the correct equipment, the 1/25th SBCT MI company provided these DCGS–A multifunction workstations to the battalion COIST elements to enable their detailed analysis and enemy common operational picture at a location where the upper tactical internet is available. This

allocation requires creating analog capabilities at the company COISTs. All COIST Soldiers built map boards and unit-based tracking charts to assist in analog battle tracking. The MI company also reallocated and prioritized its night vision goggles and AN/PEQ-15 Advanced Target Pointer Illuminator Aiming Lights for each company COIST Soldier in order to support maneuver in any condition. Additionally, the COIST platoon received two high mobility multipurpose wheeled vehicles (Humvees) and associated radios to facilitate garrison training and allow movement for the COIST

platoon leadership during training and combat operations. Overall, the 1/25th SBCT's equipping plan for COISTs focuses on integration with maneuver and on the development of the right capabilities at the right level.

Train the Company Intelligence Support Team for the Brigade

A critical portion of the 1/25th SBCT COIST concept relies on the MI company and brigade engineer battalion commanders to train and certify the COIST before employment in any training cycle. Because of this change, the MI company needed to build a training concept that met this intent. When developing the COIST training plan after the MTOE was changed, the MI company consulted ATP 2-19.4 and TC 2-19.400. ATP 2-19.4 states the responsibilities of the COIST are to develop and maintain situational understanding of the area of operations and to facilitate the flow of information between the company and battalion S-2.⁶ In order to accomplish this intent, the MI company focused on three main areas:

- ◆ Intelligence preparation of the battlefield (IPB).
- ◆ Enemy common operational picture.
- ◆ Frequency modulation (FM) and Joint Capabilities Release (JCR) proficiency.

For training Soldiers on IPB, the MI company trained and certified all COIST analysts on information collection Table I tasks from TC 2-19.400.⁷ Although designed for the brigade intelligence support element, the tasks lend themselves to the COIST with their focus on IPB and map-reading skills.

To train the COIST on maintaining an enemy common operational picture, the company developed its own Table III team certification. This certification consists of each battalion COIST team, consisting of an NCO and three Soldiers, conducting IPB together followed by a battle-tracking exercise. Critical to this exercise is the COIST's ability to make assessments from templated courses of action and reporting that it receives. A white cell replicates platoon-level reporting to the company COIST and brigade and battalion scout reporting to the battalion COIST team leader. This allows the team to exercise "pushing" and "pulling" information. Each COIST member has radios that monitor company and battalion frequencies, as well as a JCR. The intent of the exercise is to stress the COIST's reporting process and to develop each team's standard operating procedure.

Due to the absence of the upper tactical internet at the company level in a decisive action fight, the company chose to focus training on the lower tactical internet and the development of analog products. Each COIST member is required to certify on JCR and FM radios. The company leveraged the

Mission Training Center for JCR training and conducted internal training on operating the FM radio and establishing an OE-254 communications antenna group.

To round out the COIST's capability in support of maneuver commanders, the MI company identified some other areas that require training and preparation before employment in the decisive action fight. The COIST should train on the One System Remote Video Terminal in order to assist its commander in pulling full motion video feeds. COIST Soldiers should also become familiar with tactical questioning and site exploitation in order to advise the commander on those missions.

The employment of the COIST to train 11-series and 19-series Soldiers and NCOs on intelligence tasks within each company command post continues to be a company commander-level decision. Within 1/25th SBCT, each company commander tends to execute this cross-training a little differently, with more aggressive commanders training their entire headquarters element on intelligence tasks and tracking to enable 24-hour operations and increased intelligence understanding.

Employment of the Company Intelligence Support Team in Decisive Action Operations

The brigade was able to test the COIST concept in February 2018 during 1-5 Infantry Battalion's exercise, Arctic Thrust, a battalion emergency deployment exercise followed by a battalion live fire at Joint Base Elmendorf-Richardson, Alaska. The COIST had given a capabilities briefing on the COIST roles and responsibilities to supported maneuver commanders prior to Arctic Thrust. Upon alert, the COIST immediately integrated with the supported maneuver battalion and companies to assist with IPB and recommend named areas of interest and priority intelligence requirements. Once integrated, the COIST confirmed battalion communication cards, JCR role names, key leaders in the company and battalion, and reporting timelines and formats.

During the exercise, the best results for COIST implementation came when the supported commander brought his COIST to the battalion for all operation orders, rehearsals, and battlefield update briefs. Bringing the COIST to battalion allows the COIST to receive the latest intelligence from the battalion S-2 and fully understand the current battalion common operational picture. An identified best practice was to have each COIST brief their company's enemy situation during the battalion combined arms rehearsal.

During training, COIST Soldiers provided the most benefit when fully integrated into command post operations. COIST

teams had access to FM/high frequency/satellite communications radios and a JCR. This allowed the COIST to push and pull information from the platoons and battalion. The COIST also maintained the common operational picture on its issued map board. It assisted the commander in battle tracking, battle damage assessments, and updated enemy assessments as the situation developed. A JCR chatroom for COIST analysts and battalion S-2 was identified as a best practice to facilitate rapid intelligence dissemination within the battalion.

Conclusion

With the implementation of 35F force reduction and the change to MTOE in effect, the optimization of COIST support across the brigade—

- ◆ Allowed 1/25th SBCT to build relationships.
- ◆ Increased emphasis on intelligence leaders generating intelligence capacity.
- ◆ Optimized support to maneuver commanders at echelon.

Much as the 13F concept built before it, the 1/25th SBCT COIST plan outlined here enabled the brigade to develop a functioning COIST program in approximately 6 months. Moving the COIST from the battalion S-2 to the MI company enables the BCT to more effectively train the COIST prior to execution. The COIST concept has already demonstrated value to its supported battalions. By establishing a habit-

ual relationship, properly equipping Soldiers to operate in an austere environment, and focusing intelligence training on developing analog products through the lower tactical internet, the MI company developed a critical intelligence enabler that provided company commanders greater situational awareness. Vital to the success of the COIST program is integrating the COIST early and often with its supported companies. Additionally, the authorization of an additional lieutenant to serve as the COIST platoon leader allowed the MI company to tailor a specific training plan that focused on IPB and current operations at the company level. ✨

Endnotes

1. Training Circular (TC) 2-19.400, *MI Gunnery for the Military Intelligence Company of the Brigade Engineer Battalion 1.0*, dated 29 July 2016, is inactive. The development strategy for MI Gunnery is in revision with a planned update titled *Military Intelligence Training Strategy for the Brigade Combat Team*.
2. Department of the Army, Army Techniques Publication (ATP) 2-19.4, *Brigade Combat Team Intelligence Techniques* (Washington, DC: U.S. Government Publishing Office, 10 February 2015), 2-14.
3. Department of the Army, *Operational and Organizational Concept Paper, Company Intelligence Team (COIST) FDU Junior* (December 2014).
4. Ibid.
5. Ibid.
6. Department of the Army, ATP 2-19.4, *Brigade Combat Team*, 2-14.
7. Department of the Army, TC 2-19.400, *MI Gunnery*.

LTC Anthony Barbina is the former 70th Brigade Engineer Battalion Commander. He provided the guidance and intent for the 1st Stryker Brigade Combat Team (SBCT), 25th Infantry Division company intelligence support team (COIST) implementation plan. He has led formations from the platoon through battalion level and previously served as a brigade engineer, brigade troops battalion executive officer, airborne brigade combat team executive officer, and the Chief, Facilities and Construction for U.S. Army Africa.

CPT Alex Reinwald was the former platoon leader for the COIST platoon. He was responsible for the implementation of the 1/25th SBCT COIST certification plan. He previously served as a cavalry squadron assistant S-2, cavalry squadron S-2, and information collection platoon leader.

CPT Michael Heim was the Company D, 70th Brigade Engineer Battalion Commander. He developed the 1/25th SBCT COIST certification plan. He previously served as a battalion S-2 and brigade assistant S-2.

Military Intelligence Professional Bulletin (MIPB) presents information designed to keep intelligence professionals informed of current and emerging developments within intelligence.

MIPB mobile APP is now AVAILABLE for Android and iPhone

The APP can be accessed by going to <https://play.google.com> (for Android) or the Apple App Store (for iPhone) and searching for MIPB.



4th Infantry Division Military Intelligence Training Strategy

by Lieutenant Colonel Thomas Spahr and Captain Michael Weiss

Background

In 2016, U.S. Army Forces Command published an operation order directing brigade combat team (BCT) commanders to develop a military intelligence (MI) home-station training and certification plan in accordance with TC 2-19.400, *MI Gunnery for the Military Intelligence Company of the Brigade Engineer Battalion 1.0*.¹ The order directed corps, division, and U.S. Army Reserve Command to oversee “the development of a holistic training and certification strategy to ensure all intelligence warfighting function teams meet the readiness levels supporting operational mission sets and culminating training events.”² This order was in response to the disturbing statistic that during fiscal year 2015, 12 brigade-level S-2s were relieved or removed early from their position. The order was also in response to observations at the combat training centers that S-2 sections and MI companies were arriving at combat training centers inadequately trained on their essential tasks and unfamiliar with their equipment.³

Our observation in the 4th Infantry Division is that BCT S-2 sections lack the expertise and/or time to put together adequate intelligence collective training. The cost of a BCT S-2 section leading this kind of collective training is that the most experienced noncommissioned officers, warrant officers, and officers have to build a scenario and fill exercise control roles, precluding them from conducting the needed training themselves.

The division G-2 section shares responsibility with commanders to ensure BCT intelligence professionals are trained and ready for combat and major training exercises, including the combat training center rotations. The divisions possess comparatively senior intelligence professionals in each intelligence discipline (all-source, human intelligence [HUMINT], geospatial intelligence, and signals intelligence [SIGINT]). At posts where the division is the highest level of command, divisions can prioritize the Foundry trainers and the Intelligence and Electronic Warfare Tactical

Proficiency Trainer (IEWTPT) team to focus on collective training events for the BCT S-2 sections and MI companies. By taking the lead on the collective training portions of the Military Intelligence Training Strategy (MITS), formerly MI Gunnery, the division provides the BCT leadership the flexibility to focus on training rather than exercise control. By directing the collective portion of MITS, the division assists the BCT S-2 and MI company commander in blocking time on the brigade’s training calendar to ensure the necessary training repetitions before deployment or combat training center rotation.

MITS provides a vehicle to execute an adequate BCT S-2 and MI company training plan. The goal of MITS is to provide a standardized training strategy for commanders to assess, train, and evaluate their tactical intelligence warfighting function in an objective and quantifiable manner. MITS follows the Integrated Weapons Training Strategy philosophy, enabling a series of progressive tiers that build from individual to collective tasks and, in the process, build muscle memory through repetition. MITS includes four tiers:

- ◆ Tier 4 for individual military occupational specialty certification.
- ◆ Tier 3 for team/crew certification.
- ◆ Tier 2 for brigade S-2 and brigade intelligence support element certification.
- ◆ Tier 1 for the entire BCT intelligence warfighting function incorporated with the rest of the BCT staff.⁴

Certification of all four tiers should occur at every echelon of a BCT’s intelligence warfighting function before a combat training center rotation.

The Initial Planning Phase

At the 4th Infantry Division, we divided MITS into two phases. Phase 1 included Tiers 4 and 3, with the brigade planning, resourcing, and leading while the division provided oversight and external evaluator support upon

request. Phase 2 included Tiers 2 and 1, with division leading the planning and exercise control of the training events. To ensure consistency with Objective-Task standards for outside observers, we defined—

- ◆ MI company and brigade S-2 noncommissioned officers as evaluators for Tier 4.
- ◆ MI company, brigade S-2, and Foundry as evaluators for Tier 3.
- ◆ Division or a sister brigade as evaluators for Tier 2.
- ◆ Division, corps, or a sister brigade as outside evaluators for Tier 1.

The 4th Infantry Division already had a program in place that defined the division as the lead for the brigade field training exercise and a system for providing external evaluators. We used this exercise at the Tier 1 event for MITS. Within the BCTs, the MI company commonly ran a field training exercise that served well as the Tier 3 event. What was lacking was the Tier 2 collective training event for the BCT S-2 section and MI company before the brigade field training exercise. Our Tier 2 training event enabled the BCT S-2 and MI company commander to test their intelligence team and to solidify their planning and tactical standard operating procedures before complete integration with the BCT staff. We identified that the BCTs needed assistance/support from division at Tier 2. The remainder of this article will focus on how we developed the Tier 2 program that currently exists in the 4th Infantry Division.

Formulating a Plan Specific to the Tier 2 Exercise

The first step to developing the Tier 2 exercise was formulating a plan. We gathered lessons from other division G-2 sections, notably the 1st Armored Division, which recently conducted an MI Gunnery competition. While a great training event, the 1st Armored Division G-2 highlighted the challenge of scheduling this event at a time when two of their BCT S-2 sections were at a similar point in their training progression. Based upon this experience, we decided to focus on one BCT at a time.

Next, we gathered lessons learned from a senior brigade S-2 and two senior MI company commanders in the 4th Infantry Division who had recently conducted a successful field training exercise. These lessons included the technique of pushing an IEWTPT-simulated scenario through our division’s tactical network to a field location. The IEWTPT was not originally designed to push data outside of the mission training complex or Foundry facility, but we believed it was necessary to test the brigade’s intelligence architecture in a field environment using the training audiences’ communications systems as much as possible. Working closely with our Fort Carson Foundry director, our mission training complex leadership, and our G-6, we were able to relatively easily access the IEWTPT on our division tactical network. This enabled IEWTPT to push U.S. message text format (USMTF) information, ground moving target indicator data, and a simulated unmanned aerial vehicle feed to the brigade tactical operations center in the field.

One of our brigade MI companies recently had success using the U.S. Army Intelligence and Security Command-funded Digital SIGINT Training System-Mobile (DSTS–M) to train their SIGINT and HUMINT collectors and analysts. By partnering with DSTS–M, we were able to create an environment to train our HUMINT and SIGINT collectors by adapting prefabricated roles for role players and pushing low-level and complex communications that were relevant to our scenario for our Prophets and low-level voice intercepts to collect against.

Getting Buy-In at the Right Level was Essential

Once our initial plan was in place, we set about gaining buy-in at the division, brigade, and brigade engineer battalion (BEB) level. The BEB was essential because this command was able to block time for the MI company and allocate the resources to conduct a Tier 2 training event. We found that our engineer teammates were more than willing to accept the division support. The BEB leadership also carried the weight of gaining the BCT commander’s support

Training Week 21-14	T - 13	T- 12	T - 11
Unit Tasks <ul style="list-style-type: none"> • Issue training guidance • Review intelligence certifications • Initial planning for Tier 3 • Update manning roster Unit SME <ul style="list-style-type: none"> • Request training areas for Tiers 2 & 3 • Certify Tier 4 evaluators • Conduct TCE training for Tier 3 	Unit Tasks <ul style="list-style-type: none"> • Determine STT focus topics • Finalize manning roster • Issue Tier 3 OPOD Unit SME <ul style="list-style-type: none"> • Identify STT topics • Develop Tier 3 scenario 	Unit Tasks <ul style="list-style-type: none"> • Attend Tier 2 in process review • Conduct retraining • Conduct intelligence system maintenance Unit SME <ul style="list-style-type: none"> • Develop STT • Supervise retraining • Confirm Tier 2 external evaluator support 	Unit Tasks <ul style="list-style-type: none"> • Conduct intelligence COMDEX • Validate IEWTPT scenario • Issue Road to War Unit SME <ul style="list-style-type: none"> • Verify all training area requests are complete • Confirm crew rosters

Military Intelligence Training Strategy 21-Week Training Cycle

Acronym legend on page 86

by including the Tier 2 exercise in their training progression during the brigade’s quarterly training brief.

With backing from brigade leadership, earning the 4th Infantry Division commanding general’s buy-in was relatively easy. After the initial brief to the 4th Infantry Division commander, the general asked the G-2 team to—

- ◆ Better refine the standard for the BCT S-2 section and MI company to progress through each tier (i.e., 80 per cent certified).
- ◆ Lay out a doctrinal training timeline for each tier.
- ◆ Clearly define the division versus the brigade role at each stage of the training plan.

Once we answered these requirements, the commanding general authorized us to publish a division order directing the execution of the Tier 2 exercise and tasking a sister brigade to provide role players for HUMINT training and outside observers. The division order instructing the BCT to conduct the Tier 2 exercise proved critical to the success of our MITS program. This order helped ensure that the BCT did not schedule over the intelligence warfighting function training plan and helped secure the necessary resources to conduct the training.

Refining the Plan

Next, we set about refining the plan. An article titled “MI Gunnery: Why and How?” in the January-March 2017 issue of *Military Intelligence Professional Bulletin* was an important resource in helping us understand MITS during its development.⁵ The authors of the article advised not to “reinvent the wheel”; they also advised the importance of “speaking the maneuver commander’s language.” Thus, the 4th Infantry Division G-2 team coordinated early on with the division master gunners to integrate MITS into a similar training plan and sequence as the Integrated Weapons Training Strategy. This coordination helped us create a 21-week training cycle from the receipt of a division warning order to a BCT field training exercise. Our training cycle be-

gan with an initial planning conference that outlined the training requirements for the entire BCT intelligence warfighting function. The initial planning conference should include the BEB commander, senior warrant officers from the G-2, the BCT S-2 and S-3, the MI company commander, and the G-2 planning team. Outputs from the planning conference should be the mission essential tasks that need to be practiced and certified (individual and collective), training dates and locations, external resources required, and the initial scenario design. This planning conference also ensured that both phases of MITS were nested in the scenario design and mission essential tasks.

Following the planning conference, the G-2 team built a decisive action training environment scenario nested with the BCT field training exercise and upcoming combat training center rotations. By using the same scenario that the analysts would experience during their upcoming combat training center rotation, the intelligence Soldiers were forced to learn the threat early on in their training cycle, ensuring familiarity when they went to the national training center or joint readiness training center. Additionally, the training audience was able to continually refine their intelligence preparation of the battlefield products, which improved the product and saved valuable time in a compressed training cycle. This methodology is beneficial because it puts the intelligence warfighting function ahead of the operating tempo, ensuring both the BCT S-2 and battalion S-2s provide maneuver leaders with information on the threat they will face early in the training cycle.

Putting it Together

After the G-2 approved the overall scenario for MITS, the team began to work with the operators of the IEWTPT to build their simulation. The IEWTPT provides the training audience with USMTF messages on enemy activity inside corps, division, and brigade named areas of interest directly to their Distributed Common Ground System-Army. The IEWTPT also simulates full motion video and ground moving target indicators. To ensure the SIGINT and HUMINT

T - 10	T - 9	T - 8	T - 7
Unit Tasks <ul style="list-style-type: none"> • Conduct intelligence ROC drill • Conduct intelligence systems PCC/PCI • Conduct TLP • Publish updated unit SOP • Tier 3 rehearsal Unit SME <ul style="list-style-type: none"> • Verify 80% of intelligence Soldiers are Tier 4 certified 	Military Intelligence Training Strategy Tier 3	Unit Tasks <ul style="list-style-type: none"> • Conduct retraining • Conduct maintenance on intelligence systems • Update unit SOP Unit SME <ul style="list-style-type: none"> • Supervise retraining • Consolidate unit after action report 	Unit Tasks <ul style="list-style-type: none"> • Conduct retraining • Conduct intelligence systems maintenance • Update unit SOP Unit SME <ul style="list-style-type: none"> • Supervise retraining

Acronym legend on page 86

Military Intelligence Training Strategy 21-Week Training Cycle (cont.)

collectors were trained, the G-2 team resourced external support from DSTS–M. Combining both DSTS–M and IEWTPT simulated the BCT’s organic SIGINT assets with simple and complex communications. DSTS–M created role-player characters tied into the decisive action training environment scenario that ensured the HUMINT Soldiers were able to conduct interrogations, screenings, and military source operations, which produced reports relevant to the overall scenario. Finally, the division G-2 SIGINT section provided simulated theater-level reporting injects over the Joint Worldwide Intelligence Communications System to the BCT’s Trojan SPIRIT for the BCT SIGINT cell to process and disseminate into the overall intelligence picture.

Observer-coach-trainers (OC/T) and HUMINT role players came from another BCT or were volunteers from other units in the Fort Carson region. Once the external support was resourced, we conducted two training academies—one for the OC/Ts and one for the HUMINT role players. The academy for OC/Ts focused on the scenario and ensured the OC/Ts understood their roles; these individuals also needed to understand how to evaluate MI training using training and evaluation outlines compiled for each intelligence discipline from the Army Training Network. The senior HUMINT warrant officer from the G-2X ran the opposing force academy. Both academies covered the scenario, the training audiences’ training objectives, and the role players’ expectations from HUMINT screenings, interrogations, and source operations.

The last requirement before execution was defining the higher command and exercise control support. We decided to—

- ◆ Establish a combined higher command/exercise control element capable of providing responses to requests for information.
- ◆ Conduct G-2 and S-2 coordination meetings on Command Post of the Future.

- ◆ Conduct collection management synchronization meetings on Command Post of the Future.
- ◆ Publish daily intelligence summaries to the training audience.

Additionally, during times of limited connectivity, exercise control was prepared to send message traffic to the training audience in ZIP files or using Virtual Cabinet from the Distributed Common Ground System-Army. The minimum manning requirements for this element are an officer in charge, an all-source Soldier, an all-source senior noncommissioned officer, a SIGINT warrant officer to serve as an oversight officer and coordinate placement of the DSTS–M team, and a senior HUMINT warrant officer to coordinate movement of the HUMINT role players and serve as an oversight officer. When possible, this element should also include a geospatial noncommissioned officer or warrant officer to provide processing, exploitation, and dissemination to the training audience from corps and division named areas of interest. It should also include a more robust team of all-source Soldiers and noncommissioned officers to increase the production capability of exercise control.

Lessons Learned from the Two MITS Training Cycles

As of May 2018, 4th Infantry Division executed two MITS training cycles from Tier 4 to Tier 1—first with 2nd Infantry BCT, 4th Infantry Division, and then with 1st Stryker BCT, 4th Infantry Division. Both training events followed the concept outlined above. There were many lessons learned from these two iterations.

We learned that training OC/Ts and opposing force role players requires its own detailed training plan. The Soldiers we received from the tasked unit were motivated and had a great attitude, but had virtually no experience with intelligence operations. Even with a more elaborate training plan, oversight from the division HUMINT officers and noncommissioned officers is critical.

T - 6	T - 5	T - 4	T - 3
Unit Tasks <ul style="list-style-type: none"> • Conduct retraining evaluation • Conduct intelligence systems maintenance • Conduct TLP Unit SME <ul style="list-style-type: none"> • Certify retrained Soldiers • Conduct training evaluation (as necessary) 	Unit Tasks <ul style="list-style-type: none"> • Conduct intelligence ROC drill • Conduct intelligence systems PCC/PCI • Update manning roster • Conduct TLP • Conduct intelligence COMDEX • Validate IEWTPT scenario • Publish updated unit SOP • Issue Road to War Unit SME <ul style="list-style-type: none"> • Verify 80% of intelligence crews are Tier 3 certified 	Military Intelligence Training Strategy Tier 2	Unit Tasks <ul style="list-style-type: none"> • Conduct retraining • Conduct intelligence systems maintenance • Update unit SOP Unit SME <ul style="list-style-type: none"> • Supervise retraining

Acronym legend on page 86

Military Intelligence Training Strategy 21-Week Training Cycle (cont.)

We also learned the importance of incorporating at least one maneuver planner to provide the basics of a friendly course of action in the simulated scenario. Although we understood how critical it was for the intelligence team to understand the friendly forces’ maneuver plan in order to predict the enemy response, we did not dedicate enough effort into developing the friendly plan.

A key sustain to the MITS Tier 2 exercise was the inclusion of a weeklong communications exercise the week before the training event. By surging the BCT, Foundry, and division subject matter experts on the BCT systems before the exercise, we were able to ensure no training time was lost because of system maintenance. This also ensured the BCT S-2 systems were fully functional as they began their brigade field training exercise.

Another key sustain was coordination with the G-3 to publish a MITS Tier 2 order early and to identify and coordinate for external evaluation and scenario support as soon as possible. We found that to block time on a BCT training calendar, we needed to publish a division warning order 6 months out and the operations order 90 days before the exercise.

Conclusion

The MITS program described here focuses on the BCT S-2; however, most of these principles also apply to the division G-2 section. In preparation for Warfighter Exercise 18-04, the 4th Infantry Division ran a Tier 2 collective training exercise, leveraging the IEWTPT and U.S. Army Training and

Doctrine Command G-27 to build the scenario. This exercise was critical to our success during the division’s final command post exercise, serving as our Tier 1 certification event.

The MITS program has great promise and can increase our tactical Army’s overall readiness. At the 4th Infantry Division, we were able to leverage the foundation established by U.S. Army Forces Command, U.S. Army Intelligence Center of Excellence, and our fellow divisions to build a program that is helping our BCT S-2s and division G-2 to achieve success at the combat training centers and, ultimately, in combat. 🌟

Endnotes

1. In June 2018, U.S. Army Training and Doctrine Command rescinded Training Circular (TC) 2-19.400, *MI Gunnery for the Military Intelligence Company of the Brigade Engineer Battalion 1.0*. Current training circulars that address tier certification are TC 2-19.403, *Military Intelligence Training Strategy for the Brigade Combat Team Tier 3*, and TC 2-19.404, *Military Intelligence Training Strategy for the Brigade Combat Team Tier 4*.
2. U.S. Army Forces Command, Operation Order 160423, “FORSCOM order ISO development of MI home station training and assessment/certification strategy,” 4 April 2016.
3. Nathan Adams, “Observations from a Year as the Brigade S-2 Observer-Coach-Trainer at the Joint Readiness Training Center,” *Military Intelligence Professional Bulletin* 43, no.2 (April-June 2017): 6-14.
4. Department of the Army, TC 2-19.400, *MI Gunnery for the Military Intelligence Company of the Brigade Engineer Battalion 1.0* (Washington, DC: U.S. Government Publishing Office, 29 July 2016 [obsolete]).
5. Michael Works and Martin Schwerzler, “MI Gunnery: Why and How?” *Military Intelligence Professional Bulletin* 43, no. 1 (January-March 2017): 15-20.

LTC Thomas Spahr served as the division G-2 for the 4th Infantry Division from June 2016 to June 2018. His prior assignments include speechwriter for the Vice Chief of Staff of the Army; brigade combat team S-2, 4th Brigade Combat Team, 82nd Airborne Division; and S-3 of the Army Geospatial Intelligence Battalion. He has a Ph.D. in history from The Ohio State University and taught history at West Point and the U.S. Air Force Academy. LTC Spahr is currently a student at the Army War College.

CPT Michael Weiss is the battalion S-2 for 1st Battalion, 66th Armor Regiment, 3rd Armored Brigade Combat Team, 4th Infantry Division. His previous assignments include 4th Infantry Division G-2 Operations Officer, Battalion Scout Platoon Leader, and Mechanized Infantry Platoon Leader in 1st Battalion, 77th Armor Regiment, 3rd Armored Brigade Combat Team, 1st Armored Division. CPT Weiss commissioned in 2012 from the University of Colorado Denver with a bachelor of arts in political science. He holds a graduate certificate in Advanced International Affairs from the Bush School of Government and Public Service at Texas A&M University.

T - 2		T - 1		T - Week		T + 1	
Unit Tasks <ul style="list-style-type: none"> • Conduct retraining evaluation • Conduct intelligence systems maintenance • Publish updated unit SOP Unit SME <ul style="list-style-type: none"> • Certify retrained Soldiers 		Unit Tasks <ul style="list-style-type: none"> • Conduct intelligence systems PCC/PCI • Conduct final coordination with division OC/T Unit SME <ul style="list-style-type: none"> • Verify 80% of intelligence warfighting function is Tier 2 certified 		Brigade Field Training Exercise Military Intelligence Training Strategy Tier 1		Unit SME <ul style="list-style-type: none"> • Provide Tier 1 results analysis to the brigade commander • Develop after action report for external use • Update manning roster • Provide training roll-up to division G-2 and G-3 • Develop IRCOP/QTB comments for training 	
COMMEX	communications exercise	OC/T	observer-coach-trainer	SOP	standard operating procedure		
IEWTPT	Intelligence and Electronic Warfare Tactical Proficiency Trainer	OPORD	operation order	STT	sergeants time training		
		PCC/PCI	pre-combat checks/inspection	TCE	training center evaluator		
IRCOP/QTB	Intelligence Readiness Common Operational Picture/Quarterly Training Brief	ROC	rehearsal of concept	TLP	troop leading procedures		
		SME	subject matter expert				

Military Intelligence Training Strategy 21-Week Training Cycle (cont.)

Brigade Combat Team Intelligence Transformation for High-Intensity Peer Conflict

by Captain Kyle Hanratty

Photo by U.S. Army SGT William Gore, 40th Public Affairs Division



Falcon Brigade at JRTC; a U.S. Air Force C-17 delivers supplies to 2nd Brigade Combat Team, 82nd Airborne Division, during a training exercise at the Fort Polk, LA, Joint Readiness Training Center.

Introduction

Army intelligence doctrine clearly states that operations and intelligence are closely linked and that intelligence directly drives and supports the operations process.¹ Army operations doctrine concurs by stating that the successful execution of unified land operations requires aggressive information collection and intelligence analysis.² Yet despite this concurrence, the intelligence structure at the brigade combat team (BCT) is ill-postured to provide the support required for a high-intensity peer conflict. The solution is a simple, but significant, twofold transformation requiring buy-in from the intelligence and operations disciplines.

First, the BCT staff must examine its command post composition; namely, how it organizes and connects its wealth of intelligence capabilities to better promote survivability and sustain the pace of operations, while adequately distributing its forces as required in a peer conflict. Second, the BCT intelligence warfighting function must gain efficiencies by dissecting the constructs of counterinsurgency—multi-function teams and company intelligence support teams (COISTs)—for their base capabilities and reallocate these capabilities to better support this faster, more mobile and lethal style of conflict. The 2nd BCT, 82nd Airborne Division's (2/82) intelligence warfighting function—informed by lessons learned from its high-intensity conflict against the so-called Islamic State of Iraq and Syria in Mosul and Tal Afar from December 2016 to September 2017—proofed a concept of this transformation during the Joint Readiness Training Center (JRTC) Rotation 18-06. This article illustrates this tangible transformation in three elements—

- ◆ Theory.
- ◆ Vignettes.
- ◆ Lessons learned.

The Theory: Why is Transformation Necessary?

"The Army must be ready to conduct the full range of military operations...Intelligence...is integral to operations, as the theater army competes with peer threats below the level of armed conflict...Intelligence enables mission command, facilitates initiative, and allows commanders and staffs to execute tailored solutions for complex problems in the fast-paced environments of the future."³

After more than 15 years of continuous, successful deployments, why must a BCT now dramatically change how it operates? Simply put, the threat is dramatically different. It is a discussion of risk management⁴ by way of task organization⁵—both mission-specific and broader institutional changes. The 2/82 agrees that BCTs have made tremendous progress in maximizing their potential; however, this is largely for a static (forward-operating, base-centric) counterinsurgency/stability operations-style conflict. A high-intensity conflict against a peer adversary brings a new breadth of challenges to bear. Principal among these challenges are—

- ◆ Numerous and accurate long-range artillery.
- ◆ Increased mechanized and armored forces.
- ◆ Significant chemical, biological, radiological, nuclear, and high-yield explosives (CBRNE).
- ◆ Persistent unmanned aircraft system surveillance.
- ◆ Contested cyberspace electromagnetic activity.

While well understood, the Army has never had to successfully counter the composite of these five threats.

As we seek to crack the code on this new threat model, we must return to the basics of mission command—specifically, command posts’ composition.⁶ Doctrine highlights five factors for “[command post] CP effectiveness: design and layout, standardization, continuity, deployability, and capability and range.”⁷ While all are relevant, 2/82 is particularly concerned with *deployability*—“determining the capabilities, size, and sequence of CPs.”⁸ And yet, through this discussion we must remember that while “CP survivability is vital to mission success, CPs often gain survivability at the price of effectiveness.”⁹ These concepts, guided by the subsequent brigade commander’s intent, will guide our discussion of 2/82’s model.

With this threat model in mind, the 2/82 brigade commander provided an enduring, four-faceted intent for the duration of the JRTC Rotation 18-06 operations. The changes recommended below focus on getting tenants one and four right to achieve the effects desired in tenants two and three:

1. Build and sustain combat power.
2. Mass fires to kill the enemy.
3. Attack and exploit at every opportunity.
4. Protect the force, with an emphasis on artillery and CBRNE threats.

Before examining the 2/82’s model, we must understand, according to the modified table of organization and equipment (MTOE), precisely what capabilities the BCT intelligence warfighting function brings to bear. According to ATP 2-19.4, *Brigade Combat Team Intelligence Techniques*, the BCT intelligence warfighting function has an—

- ◆ “Intelligence cell [BCT S-2]. To assist the commander and staff in understanding the situation and in decision-making, the intelligence cell provides timely, relevant, accurate, predictive, and tailored intelligence analysis.
- ◆ Organic [military intelligence] MI company. The MI company supports the BCT and subordinate commands through collection, analysis, and dissemination of infor-

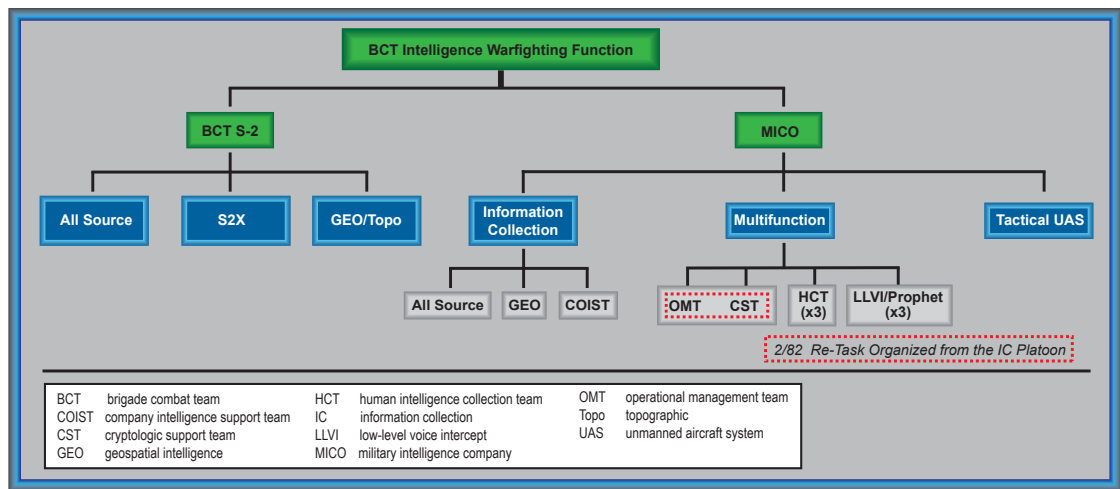


Figure 1. BCT Intelligence Warfighting Function Task Organization

mation and intelligence...[through] full-motion video, signals intelligence (SIGINT), and human intelligence (HUMINT) collection.”¹⁰

Figure 1 shows the task organization of the BCT intelligence warfighting function.

The Vignettes (How 2/82 Transformed) and Lessons Learned

To show how the 2/82 transformed, two vignettes are presented here, with their corresponding lessons learned: (1) the 2/82 distributed intelligence mission command model and (2) dissecting the constructs of counterinsurgency (multifunction teams/COISTs).

2/82 Distributed Intelligence Mission Command Model

The reemergence of high-intensity peer conflict demands the departure of the behemoth “TOC Mahal”¹¹ brigade intelligence support element (BISE) consisting of 50 or more analysts.¹² No longer can the BISE, collocated with the BCT Main command post, dwarf it in both physical and electromagnetic signature. Instead, the BISE must divide into forward and rear/sanctuary elements. It is a matter of mobility and survivability. This split configuration is the basis of the first 2/82 transformation we will discuss. For reference, we will discuss this model from a perspective of what 2/82 had on hand—not necessarily the MTOE allocation.

The 2/82 developed the following model to achieve the brigade commander’s intent to remain as small, mobile, and lethal as possible. The model draws heavily upon applying the doctrinal understanding of intelligence reach¹³ to “support distributed analysis.” The difference, however, is that typically “intelligence reach” has a connotation of leveraging the greater intelligence community¹⁴ and not establishing one’s own reach capability.

Instead of relying on a potentially overburdened higher headquarters and/or national agency, the 2/82 BCT chose to establish a small, scalable, forward-deployable (by either ground or air) cell of the BISE (henceforth referred to as BISE Lite) intended to self-sustain intelligence support to current operations and BCT plans for a period of approximately 48 hours. The remainder of the BISE (henceforth referred to as BISE Main) would

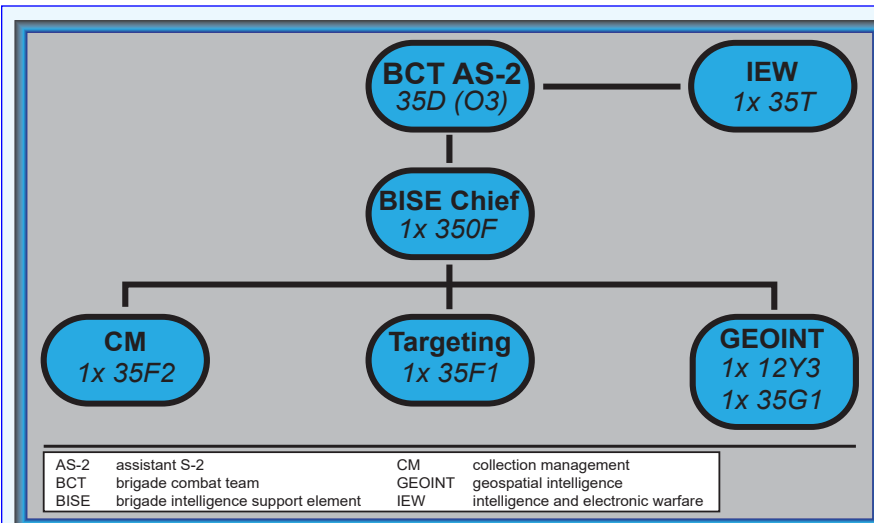


Figure 2. 2/82 BISE Lite

remain in sanctuary—out of range of the aforementioned artillery, armored, CBRNE, unmanned aircraft system surveillance, and cyberspace electromagnetic activity threats—to support the BCT in a reach capability.

It is elementary, however, to discuss the BISE Lite in a vacuum. Instead, we must view it as an intermediate stepping-stone in the build of combat power as dictated in the first tenant of the brigade commander's intent. The build progresses from the assault command post (ACP), to the tactical command post (TAC), and to the tactical operations center/BCT main command post.

The BCT ACPs are a two-piece element designed to promote redundancy and control the fight throughout the onset of the assault. For 2/82, ACP 1 consisted of the BCT S-2, the BCT collection manager, and a SIGINT-qualified analyst as a radio-telephone operator—to operate the Digital Network Kit.¹⁵ ACP 2 consisted of the BCT S-2 noncommissioned officer in charge (NCOIC) and the One Station Remote Video Terminal operator/radio-telephone

operator, typically a 35F (Intelligence Analyst). The purpose of ACP 1 is to control the fight until the ACPs can collapse into the TAC. The purpose of ACP 2 is to establish the TAC to enable a seamless transition, while simultaneously providing a redundant command and control element.

When the ACPs collapse into one formation, they become the TAC. This five-man formation is the first time the BCT intelligence warfighting function can reasonably sustain 24-hour operations. Despite this increased capability, for the BCT this is merely a stopgap until air-land operations can introduce the BISE Lite formation and establish its portion of the tactical operations center/BCT main command post.

The BISE Lite's core package (Figure 2) consists of a seven-paratrooper team, including the BCT AS-2, the BISE chief, an information collection sergeant, a targeting analyst, a two-man geospatial/topographic cell, and one intelligence system maintainer. The package is supported by a three-truck formation—one four-seat high mobility multipurpose wheeled vehicle (HMMWV) with a Joint Capabilities Release (JCR) (towing a trailer), one shelter HMMWV, and one mine-resistant ambush-protected all-terrain vehicle (M-ATV) (HUMINT variant). With the addition of a second SIGINT-variant M-ATV, the base package can be augmented to include a two-man all-source cell, a Prophet collection crew, and an additional maintainer or staff weather officer. The 2/82 chose the former, lighter model for its rotation.

BISE Main consists of several all-source officers, an additional BISE chief, the all-source production cell, a geospatial intelligence cell, the operational management team, the cryptologic support team, the remainder of the intelligence system maintainers, and the staff weather officer(s). The military intelligence company headquarters collocates with the BISE Main (Figure 3).¹⁶

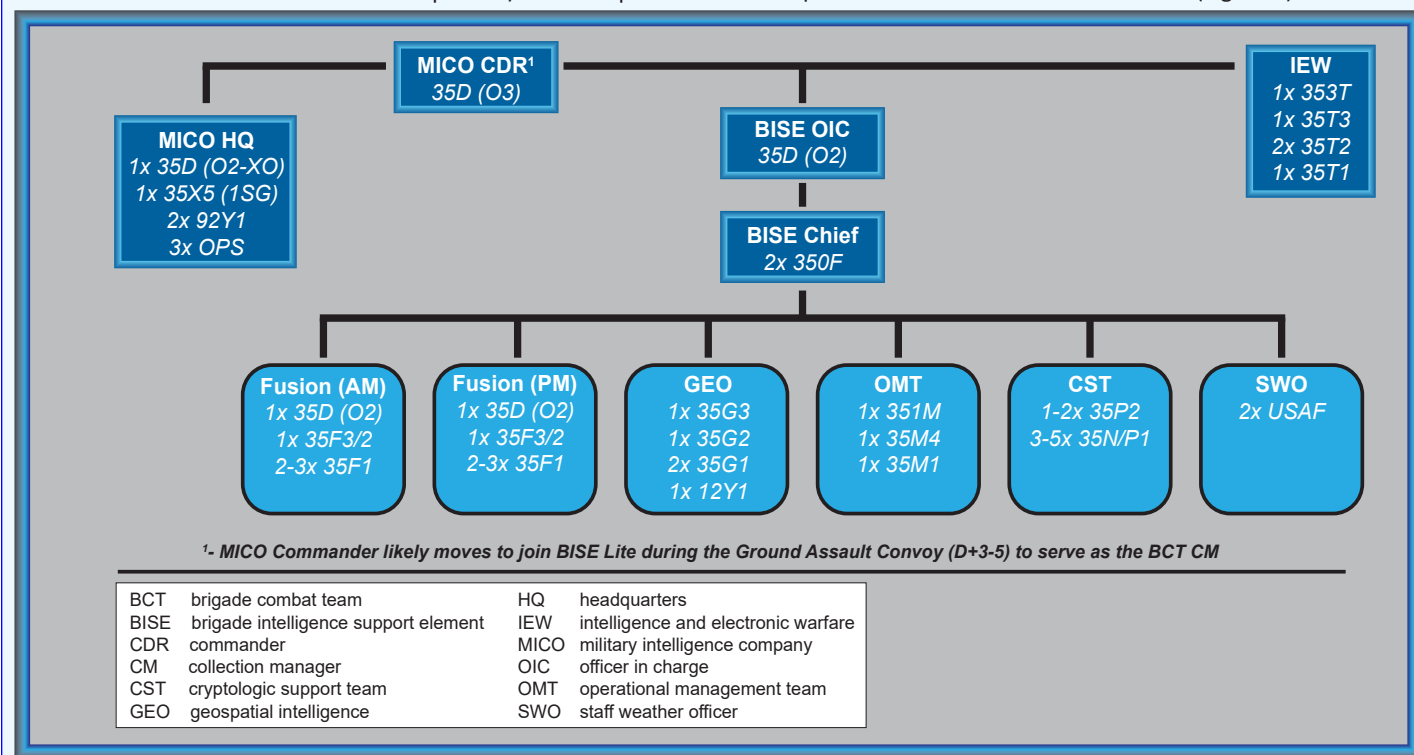


Figure 3. 2/82 BISE Main

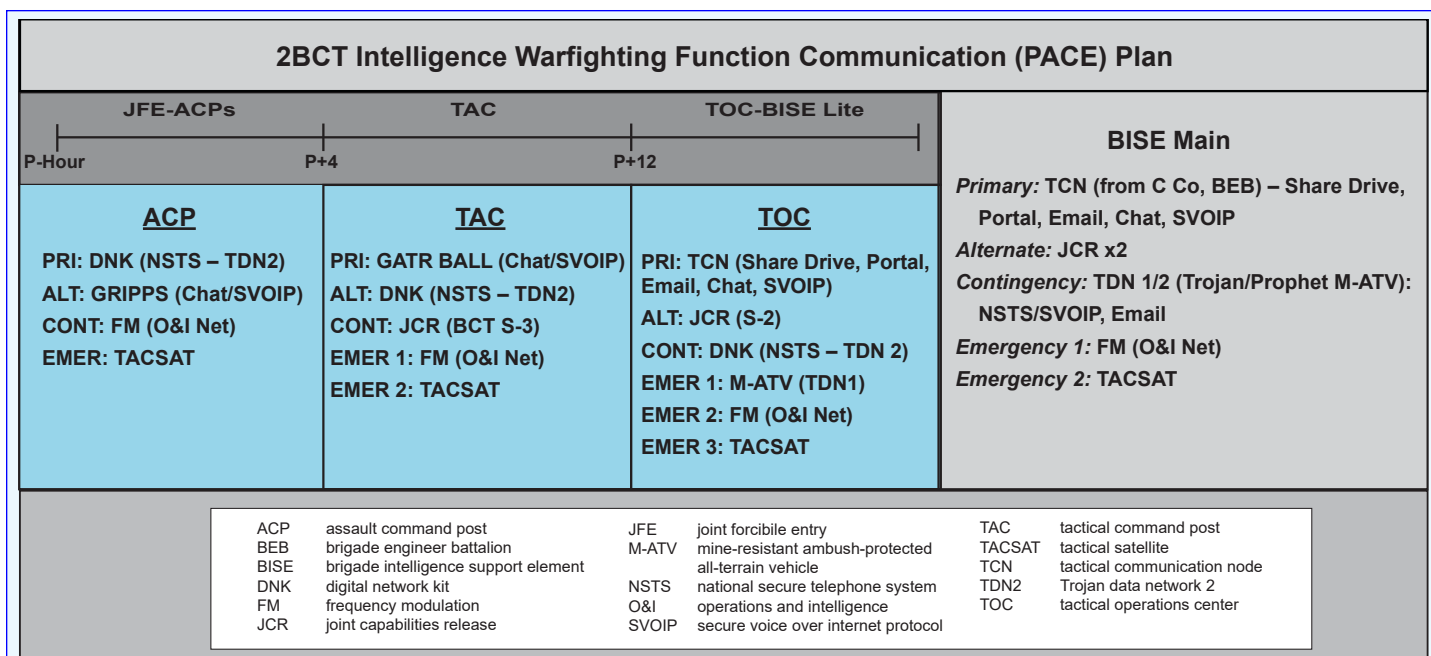


Figure 4. Key Elements of 2/82 PACE Plan

The challenge with any intelligence reach capability, let alone one organic to a BCT, is connecting the elements. The challenge becomes more complex for a BCT because the communication plan

(often referred to as the primary, alternate, contingency, emergency [PACE]) changes not only over space but also over time, as well as combat power builds (Figure 4.)

Lessons Learned: 2/82 Distributed Intelligence Mission Command Model

While the after action reviews indicate that 2/82's distributed intelligence mission command model successfully achieved the desired ends, several areas exist to refine techniques and/or gain efficiencies going forward.

The first change is systematic. The BCT prioritized the introduction of all command, control, communications, computers, and intelligence (C4I) vehicles in order to establish the command posts. However, the BCT did not consider the three-truck BISE Lite package as being C4I. Going forward, these trucks must be similarly front-loaded. For 2/82, the package arrived between P+48-72, which left the TAC undermanned nearly 24 hours longer than anticipated. [82nd uses P-hour as an equivalent to H-hour. It represents the time when the first parachute-suspended object exits the aircraft.]

The second recommendation is personnel-based. The BCT collection manager should not jump in with the ACP. Rather, they should remain with BISE Main where they can coordinate collection for D+4/5. Instead, a noncommissioned officer should jump in to relay the relevant information until the officer in charge can enter the fight.

Likewise, doctrine recommends that the military intelligence company commander collocate "with the BCT main command post to facilitate control of the company assets and maximize support to the BCT intelligence cell."¹⁷ The

2/82 recommends a step further: the BCT military intelligence company commander should serve as the BCT collection manager. Why condemn a lieutenant to attempt to understand and employ the assets best understood by the commander? In a deployed environment, a knowledgeable executive officer and/or first sergeant can resource and "run" the company. By doing so, the BCT keeps one of its most senior intelligence minds in the fight. In many cases, the commander could even serve as a current operations officer in charge to ensure a shared understanding among the asset, indicator, and BCT operations cell.

Additionally regarding personnel, 2/82 prioritized the S-2 NCOIC for ACP 2. In hindsight, we recommend the BISE chief jump in place of the NCOIC. The bottom line is that, with the formation of TAC, the BCT S-2 requires the expertise of the BCT's senior all-source intelligence technician to plan the next operation, while the BCT S-2 is likely consumed by TAC operations—potentially dislocated from the tactical operations center/BCT main command post.

The 2/82 further recommends considering the augmented version of the BISE Lite—more aptly described as BISE Forward (Figure 5, on the next page). Although this footprint requires an additional air-land slot (one M-ATV-Prophet Sensor), the five additional slots provide the following:

- ◆ one 35T (Military Intelligence Systems Maintainer/Integrator);
- ◆ one 35P (Cryptologic Linguist)/35N (SIGINT Analyst);

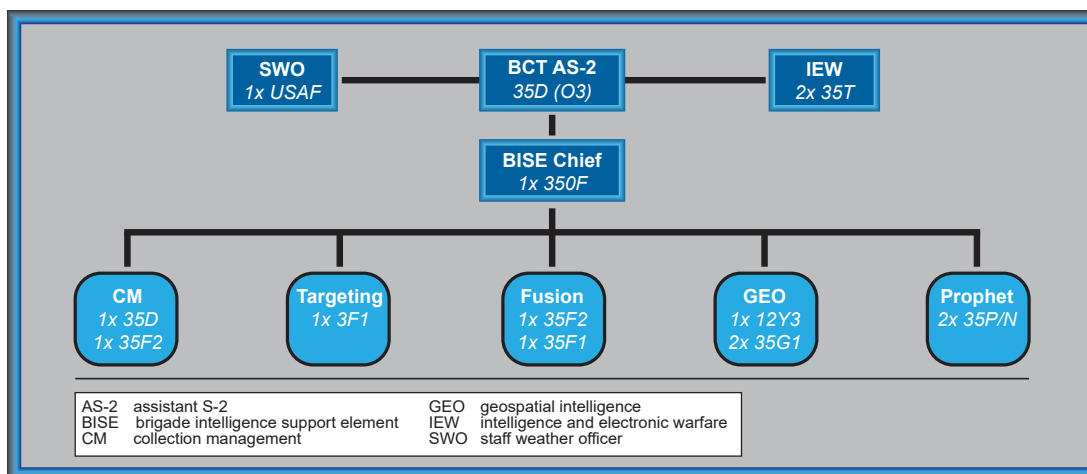


Figure 5. 2/82 BISE Forward (Recommendation)

- ♦ two 35Fs (Intelligence Analyst); and
- ♦ one 35G (Geospatial Intelligence Imagery Analyst).

Alternatively, these could also be substituted for a staff weather officer, depending on the availability of personnel and equipment. Ultimately, this change accounts not only for additional analytic output but also for security requirements and expected losses during the initial assault.

The next set of recommendations are communications-based. First, the BCT must continue to allocate at least one SIGINT-qualified individual to the ACPs to operate the Digital Network Kit. This jumpable, satellite-based communications suite provided the most consistent communications between BISEs throughout the 14-day operation. Second, 2/82 recommends prioritizing the use of the JCR or an equivalent vehicle-mounted satellite communications system higher on the PACE plan. The ability to establish intelligence (S-2) and operations (commander) chat rooms simultaneously resulted in rapidly shared information across the battlespace. Additionally, BISE Main received (and relayed) countless reflections from forward scout/maneuver elements because of its ability to maintain connectivity in sanctuary versus the challenges encountered by battalion/squadron headquarters in contact. Lastly, 2/82 largely struggled to fully employ satellite and high frequency radio communication platforms. This intelligence reach model can markedly bolster its PACE plan with additional training on AN/PRC-117 and AN/PRC-150 radios.

In addition to these platform-based recommendations, the importance of *rehearsing* the PACE plan cannot be overstated. The increased cyberspace electromagnetic activity threat presented by a peer adversary, combined with the tyranny of distance imposed by this distributed intelligence mission command model, makes these rehearsals pivotal to the success or failure of the intelligence warfight-

ing function in a high-intensity conflict. Numerous methods exist to achieve the shared understanding necessary, but 2/82 particularly recommends a two-prong approach.

First, during mission planning the BCT intelligence warfighting function (including collector teams and reconnaissance elements) should conduct a tabletop or terrain model rehearsal

during which each element explains its communication abilities over the phases of the operation. Key to this rehearsal are elements back briefing the timing/method of key reporting requirements and their understanding of adjacent elements capabilities throughout the build of combat power.

Second is the role of training. The decade and a half of counterinsurgency-conflict established a trust in and reliance on the upper-tactical internet, including but not limited to Secure Voice over Internet Protocol, email, share drives/portals, and Transverse chat or MIRC chat. It is imperative that the BCT stress its use of lower-tactical internet communications capabilities at every opportunity: frequency modulation, high frequency, and tactical satellite radios and JCR. Maintenance training presents an ideal opportunity to train these systems simultaneously.

Dissecting the Constructs of Counterinsurgency (Multifunction Teams/Company Intelligence Support Teams)

The Army's MTOE historically lags behind the pace of operations; the transition to defeat a peer competitor in high-intensity conflict is no exception. As such, BCTs must think in terms of base capabilities, not necessarily the teams given by the MTOE. Specifically, between redeployment from Operation Inherent Resolve through JRTC Rotation 18-06, 2/82 restructured how it considered its multifunction teams and its COISTs. Unlike the above transformation, necessitated by survivability, this one is more a discussion of efficiency.

Doctrine describes the multifunction platoon as flexible by design to permit it to be employed in various ways for SIGINT and HUMINT tasks.¹⁸ However, the MTOE-combination of HUMINT and SIGINT collectors inherently suggests use in a SIGINT terminal guidance model—a model very familiar to counterinsurgency veterans but arguably not nearly as useful in a high-intensity conflict. Moreover, according to the MTOE, the operational management team and cryptologic support team, including 351Ms (HUMINT Collection Technicians) and 353Ns (SIGINT Analysis Technicians), are in the information collection platoon. Why separate the subject matter experts from the collectors?

The 2/82 identified this as an opportunity to gain increased flexibility and formed a “ground collection platoon” (akin to a combination of yesteryear’s HUMINT and SIGINT collection platoons—still highlighted in ATP 2-19.4, *Brigade Combat Team Intelligence Techniques*, Figure 2-2).¹⁹ By task-organizing all SIGINT and HUMINT professionals into this ground collection platoon, 2/82 streamlined training and established an environment conducive to training all collectors on the entirety of their critical military occupational specialty tasks.

On the other hand, 2/82 did not identify the need to reorganize its COIST analysts until during JRTC Rotation 18-06. Throughout the operation, the BCT intelligence warfighting function supported each maneuver battalion with one or two 35F COIST analysts. The COIST analysts augmented the battalion intelligence section, though, and were not pushed to a company as recommended by doctrine. While this increased the capability of subordinate commands, these analysts can likely be better used to collocate an exploitation cell with the tactical unmanned aircraft system element.

Lessons Learned: Dissecting the Constructs of Counterinsurgency (Multifunction Teams/Company Intelligence Support Teams)

The task organization of HUMINT and SIGINT collectors into a ground collection platoon proved an overwhelming success for 2/82. First, this consolidation set the stage for leaders to easily task-organize collectors into separate SIGINT and HUMINT collection teams. In application during JRTC Rotation 18-06, this enabled 2/82 to task-organize an individual SIGINT collector to support a dismounted reconnaissance team and gather more than 70 SIGINT intercepts/lines of bearing and inform the greater brigade understanding of the enemy. Additionally, the ground collection platoon leader’s training plans benefited incredibly from the collocation of the warrant officer expertise.

As a former battalion S-2, I would never turn down the opportunity for increased analytic brainpower. As the intelligence company commander, though, I recommend otherwise. The analysts that the BCT military intelligence company attached to battalions produced marginal results—not because of a lack of proficiency but rather a lack of opportunity. The ideal opportunity for successful employment of COIST analysts occurs in a wide-area security style conflict in which companies are decentralized and operate with increased autonomy. High-intensity peer conflict relies heavily on combined arms maneuver and thus limits the opportunities for this company-level autonomy.²⁰

As a result, 2/82 recommends repurposing the COIST analysts to form a BCT exploitation cell (and potentially a strike cell integrated with fires representatives) at the tactical unmanned aircraft system headquarters. While this may sound like another good idea without empirical support, 2/82 proofed a similar concept during the BCT defense module at JRTC Rotation 18-06. They allocated one 35F sergeant to

augment the tactical unmanned aircraft system during the defense. This single, collocated analyst markedly increased the fidelity of exploitation and enabled multiple dynamic kinetic engagements. While an admittedly small sample size, one can only imagine the potential lethality increase by enabling 24-hour exploitation at the point of collection and streamlining the sensor-to-shooter chain.

Conclusion: Transform or Risk Irrelevance

The BCT intelligence warfighting function is designed to be the intelligence collection and production hub for unified land operations. The BCT intelligence warfighting function capabilities far outstrip those of its division headquarters. Yet, this wealth of capability is increasingly at risk of irrelevance. If BCTs attempt to fight future high-intensity conflicts against peer adversaries, in the same manner they fought counterinsurgency conflicts of the past generation, they risk being rendered too large and/or too slow or, worse yet, simply becoming a casualty of this violent, fast-paced style of conflict. However, if BCTs reexamine how they consider, organize, and connect these capabilities, they can establish the conditions to continue driving operations and thus winning on any battlefield against any adversary for years to come. ✨

Endnotes

1. Department of the Army, Army Doctrine Publication (ADP) 2-0, *Intelligence* (Washington, DC: U.S. Government Publishing Office [GPO], 4 September 2018), vii.
2. Department of the Army, Army Doctrine Reference Publication (ADRP) 3-0, *Operations* (Washington, DC: U.S. GPO, 6 October 2017), 3-14.
3. Department of the Army, ADP 2-0, foreword.
4. “The process to identifying and assessing hazards arising from operational factors and making decisions that balance risk cost with mission benefits.” Joint Chiefs of Staff, Joint Publication 3-0, *Joint Operations* (Washington, DC: U.S. GPO, 17 January 2017), III-16. Change 1 was issued on 22 October 2018.
5. “The act of designing a force, support staff, or sustainment package of specific size and composition to meet a unique task or mission.” Department of the Army, ADRP 3-0, 5-7.
6. As outlined in Department of the Army Field Manual (FM) 6-0, *Commander and Staff Organization and Operations* (Washington, DC: U.S. GPO, 5 May 2014). Change 1 was issued on 11 May 2015. Change 2 was issued on 22 April 2016; and in Department of the Army, FM 3-96, *Brigade Combat Team* (Washington, DC: U.S. GPO, 8 October 2015).
7. Department of the Army, FM 6-0, 1-3.
8. Ibid., 1-4.
9. Ibid., 1-4; and Department of the Army, FM 3-96, 3-23.
10. Department of the Army, Army Techniques Publication (ATP) 2-19.4, *Brigade Combat Team Intelligence Techniques* (Washington, DC: U.S. GPO, 10 February 2015) 1-1.

11. The “TOC Mahal” is of course a humorous comparison to the large, lavish Taj Mahal in India.

12. “A current technique used by [brigade combat teams] BCTs is the establishment of a [brigade intelligence support element] BISE by task-organizing personnel from the BCT intelligence cell and [military intelligence] MI company. The BISE is the BCT S-2’s main analytic organization for all-source analysis and production.” Department of the Army, ATP 2-19.4, 2-10.

13. “The activity by which intelligence organizations proactively and rapidly access information from, receive support from, and conduct direct collaboration and information sharing with other units and agencies, both within and outside the area of operations, unconstrained by geographic proximity, echelon, or command.” Department of the Army, ADP 2-0, 3-5.

14. “All departments or agencies of a government that are concerned with intelligence activity, either in an oversight, managerial, support, or participatory role.” Office of the Chairman of the Joint Chiefs of Staff, *DOD*

Dictionary of Military and Associated Terms (Washington, DC: The Joint Staff, January 2019), 116.

15. The Digital Network Kit is a jumpable satellite communication suite capable of accessing Trojan Data Network 2–National Security Agency Network.

16. The military intelligence company’s BISE Lite personnel are under operational control to the BCT headquarters, and collector teams become general support, reinforcing to their parent battalion headquarters.

17. Department of the Army, ATP 2-19.4, 2-6.

18. *Ibid.*, 2-10.

19. *Ibid.*, 2-6.

20. “COIST analysis focuses on the company area of operations...[to enable the company commander to] perform basic intelligence tasks associated with planning, directing, coordinating, and controlling forces and operations...[and serve as] the primary filter and analysis center for raw data.” *Ibid.*, 2-14.

CPT Kyle Hanratty is an active duty military intelligence officer with operational deployments to Afghanistan and Iraq, most recently as the 2nd Brigade Combat Team (BCT), 82nd Airborne Division, Military Intelligence Company Commander, during the liberation of Mosul and Tal Afar in 2017. His previous assignments include the 2nd Battalion, 325th Airborne Infantry Regiment S-2, and 2/82 BCT assistant S-2. He holds bachelor’s degrees in political science and Chinese from the University of Notre Dame.

Unstoppable Small Unmanned Aircraft Systems

(Continued from page 76)

2. Department of the Army, Training Circular (TC) 3-04.62, *Small Unmanned Aircraft System Aircrew Training Program* (Washington, DC: U.S. Government Publishing Office [GPO], 19 August 2013), 1-1.

3. *Ibid.*, 4-1–4-7.

4. Department of the Army, Army Techniques Publication 3-04.64, *Multi-Service Tactics, Techniques, and Procedures for the Tactical Employment of*

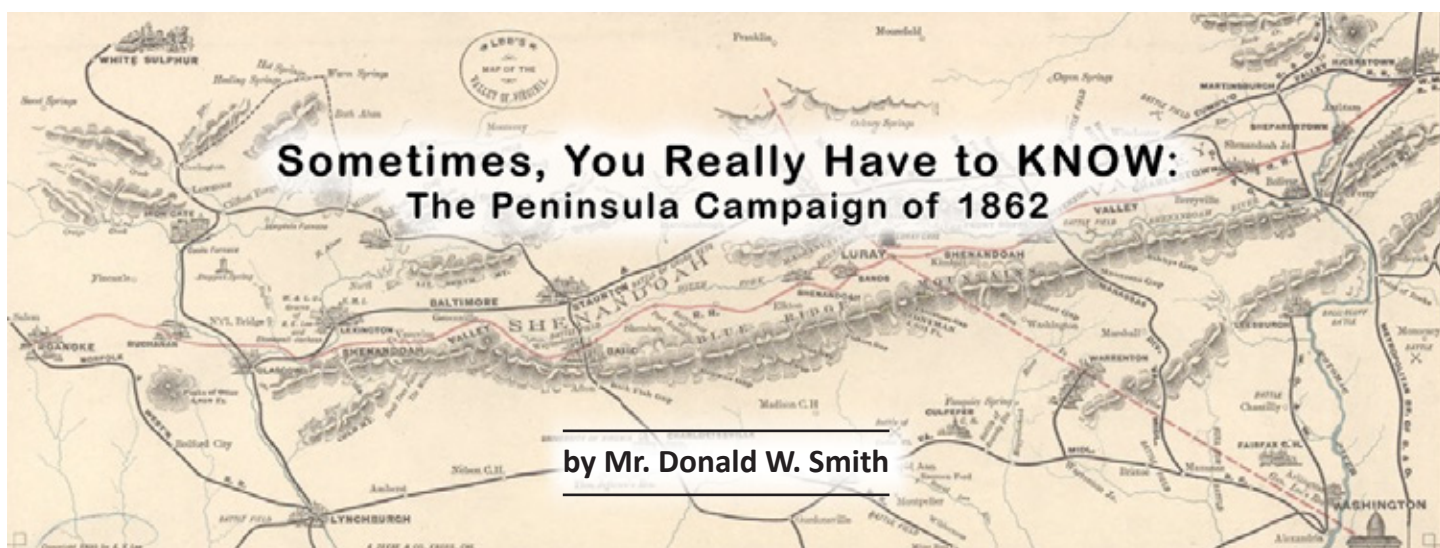
Unmanned Aircraft Systems (Washington, DC: U.S. GPO, 22 January 2015), 33-53.

5. Department of the Army, TC 3-04.62, *Small Unmanned Aircraft System*, 2-5.

CPT Sean Hayball is the Grizzly Team Intelligence observer-coach-trainer, Operations Group, Joint Multinational Readiness Center (JMRC), Hohenfels, Germany. His previous assignments include the 1-4 Infantry Battalion intelligence officer, JMRC; the Security Force Advisory and Assistance Team intelligence advisor Corps G-2 and Operational Coordination Center-Regional, Headquarters and Headquarters Troop (HHT), 3rd Cavalry Regiment, Fort Hood, TX; the Reconnaissance Squadron intelligence officer, HHT/4/3rd Cavalry Regiment, Fort Hood, TX; and the Regional Deconfliction Cell officer in charge, 10th Mountain Division, Kandahar Intelligence Fusion Center, Regional Command South, Afghanistan. CPT Hayball has a bachelor of science in international studies from the University of St. Thomas, Houston.

CPT Peter Kerkhof is the S-2, 2nd Squadron, 2nd Cavalry Regiment, Vilseck, Germany, with deployment as S-2 for the North Atlantic Treaty Organization Enhanced Forward Presence Battle Group, Poland. His previous assignments were as the Regimental assistant S-2, 2nd Cavalry Regiment; assistant S-2, 3rd Ranger Battalion, 75th Ranger Regiment; Regimental assistant S-2, 3rd Ranger Battalion; and Military Intelligence Company executive officer, 524th Military Intelligence Battalion, 501st Military Intelligence Brigade, Camp Carroll, South Korea. CPT Kerkhof has a bachelor of science in mathematics and economics from the U.S. Military Academy.

SFC Ryan Sarver is the Grizzly Team Fire Support observer-coach-trainer, Operations Group, JMRC, Hohenfels, Germany. He has served at the 1-187 Infantry Battalion, 3rd Brigade Combat Team, 101st Airborne Division, Fort Campbell, KY, and at Bravo Company, 2-7 Infantry Battalion, Fort Stewart, GA. SFC Sarver is completing his bachelor of science in history from Liberty University.



Tell me what you know. Tell me what you don't know. Then tell me what you think. Always distinguish which is which.

—GEN Colin Powell

Introduction

GEN Colin Powell's "rules" for intelligence personnel are thought-provoking: "Tell me what you know. Tell me what you don't know. Then tell me what you think. Always distinguish which is which." They force analysts to distinguish between verified information ("what you know") and assumptions ("what you think"). GEN Powell explained his rules in a 2012 *Newsweek* article. " 'What you know' means you are reasonably sure that your facts are corroborated. At best, you know where they came from, and you can confirm them with multiple sources." He acknowledges that intelligence analysts cannot always provide "facts." "At times you will not have this level of assurance, but you're still pretty sure that your analysis is correct. It's OK to go with that if it's all you have, but in every case, tell me why you are sure and your level of assurance."¹

Evaluate the Risk

Intelligence officers have to be sure their boss *knows* the difference between "what you know" and "what you think." In some situations, if you underestimate your opponent, the results can be catastrophic. The boss always has to ask, "But what if your intelligence estimate is wrong? What happens if the enemy is stronger than you think? And, can I deal with the consequences?"

Commanders can only accept a certain level of risk. Sometimes, the enemy really is strong enough to defeat you—or even annihilate you. In those high-risk situations, the boss cannot afford for you to be wrong. They need to **KNOW** where the enemy *really* is or is not, what they *really* can or cannot do. If you can't tell them that, with a high level of confidence, then the commander may have

to choose friendly courses of action that are less optimal but also less risky. They may have to pass up opportunities. When the risks of being wrong are too great, sometimes the boss has to play it safe.

We have all heard the phrase "intelligence drives operations." In order to drive operations that have high levels of risk, the intelligence has to be especially good. "What you think" may not be good enough. You may have to *know* where the enemy is and how badly they can hurt you. In some situations, if intelligence officers cannot provide intelligence that is good enough, their commanders will not be able to act aggressively—or not act at all.

A Lesson from the Civil War

President Abraham Lincoln found himself facing this kind of high-risk situation in June 1862. The Union Army (also known as the Federal Army or Northern Army) was just a few miles from Richmond, Virginia (capital of the Confederate States of America for most of the Civil War). It was about to fight a battle that could force the Confederacy to its knees. The Union commander kept asking Lincoln for reinforcements. Specifically, he wanted the President to release troops that were being held back to defend Washington. Lincoln wanted to release those troops, but he also feared for the safety of the Union capital.

Lincoln, in other words, was risk-averse and needed exceptionally good intelligence on the enemy's whereabouts, with a very high level of assurance, in order to release those reinforcements. In June 1862, it was not realistically possible for the Union Army to collect and report the amount of reliable information on the location and actions of the key Confederate forces necessary to give Lincoln the verification he needed. This article will explain the factors that prevented that intelligence collection and reporting.

The upcoming battle would culminate the Union Army's Peninsula Campaign. General George B. McClellan had taken more than 100,000 Union troops into Virginia. By late June, he was only a few miles east of Richmond. The Confederate commander, Robert E. Lee, had only 65,000 troops to oppose him.²

McClellan continued asking Lincoln and Secretary of War, Edwin Stanton, for reinforcements. In particular, he wanted General Irvin McDowell's command, known as the "Department of the Rappahannock." Deployed around Fredericksburg and Manassas and charged with defending Washington and Maryland, the Department of Rappahannock had between 20,000 and 30,000 soldiers.³ A major move south by McDowell would have put Lee in a bind. It would force him to defend in two directions: to the east, against McClellan, and to the north, against McDowell.

However, Lincoln never released the vast majority of McDowell's forces. They instead stayed in Northern Virginia, which let Lee focus on McClellan and defeat him in the Seven Days' Battles, a series of engagements in late June and early July 1862. McClellan's will broke, he withdrew his forces, and Richmond was saved.

Why couldn't Lincoln release McDowell? Two words: Stonewall Jackson. In May and June 1862, as McClellan's forces approached Richmond, Confederate general T. J. "Stonewall" Jackson commanded approximately 13,000 Confederate soldiers in Virginia's Shenandoah Valley. From there he menaced Washington in what came to be known as the "Valley Campaign." Jackson's troops marched up and down the Shenandoah Valley, attacking (and usually defeating) several different Union forces chasing him. "In thirty days," writes the National Park Service in its history of the Valley Campaign, "Jackson's men covered 350 miles, defeated three Union commands in five battles, caused 5,000 casualties at a loss of only 2,000 men, and captured much needed supplies."⁴

Jackson's troops also prevented thousands of Federal soldiers in Northern

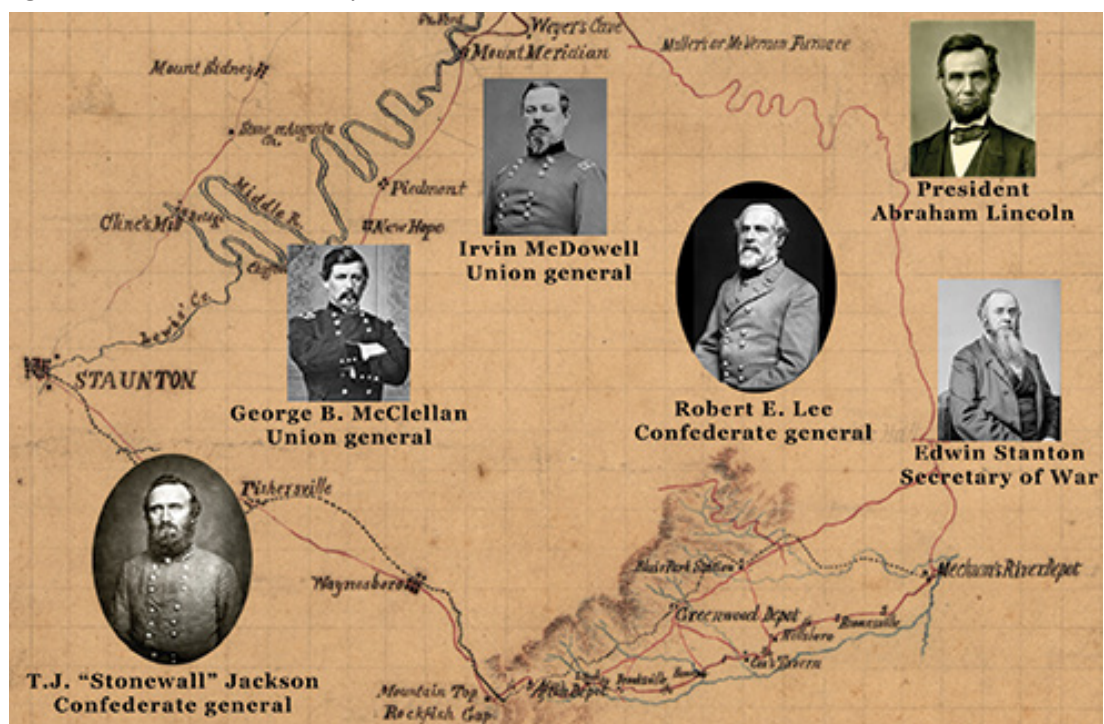
Virginia—McDowell's among them—from going south to help McClellan. Jackson's successes rattled Lincoln and his government. Less than a year had passed since the First Battle of Bull Run, and everyone remembered Union soldiers and civilians stampeding back into Washington after that catastrophe; no one wanted a repeat performance. So McDowell stayed up north, and McClellan fumed.

Telegrams from McDowell, Lincoln, Stanton, and several Union generals show that, in June 1862, they still worried about Jackson. Where was he? What would he do? Would he strike toward the Union capital? Might he enter Maryland? (At this early stage of the Civil War, the Union government still worried about Confederate sympathies in Maryland.) If Jackson was still a threat to Washington, then Lincoln and Stanton would want McDowell to stay close by. Just in case.

In modern-day terminology, Lincoln and Stanton had two commander's critical information requirements.

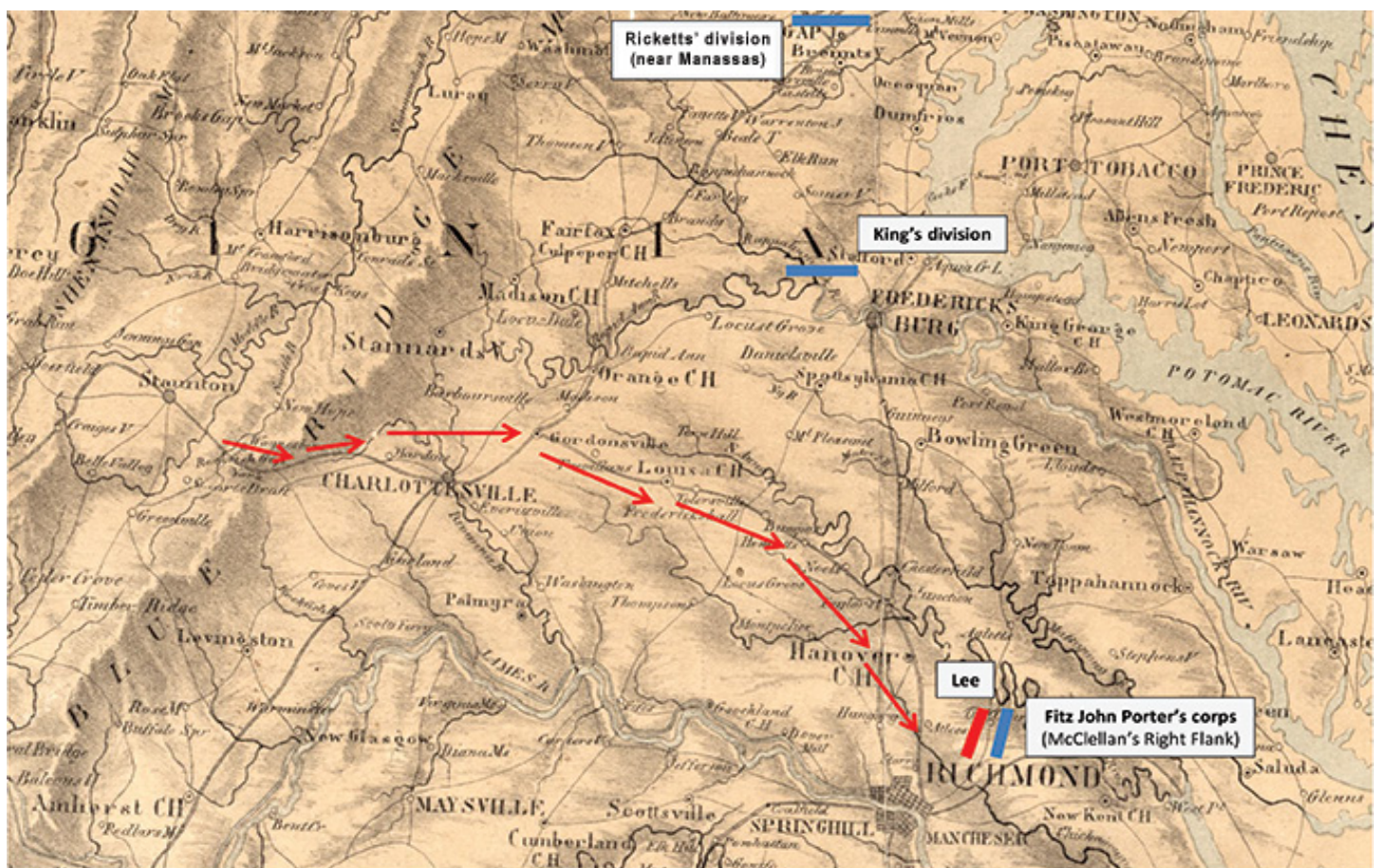
- ◆ Where is Jackson's main force?
- ◆ What is the objective of Jackson's main force? (Does it plan to stay in the Shenandoah Valley? Threaten Washington? Go to Richmond and join up with Lee?)

Before Lincoln and Stanton could be comfortable enough to release McDowell, they had to know that Jackson did not threaten Washington. That meant they had to know where Jackson was AND where he was going. Most important of



A map from the collection of Jedidiah Hotchkiss, Stonewall Jackson's mapmaker. It shows the route from Waynesboro, through Rockfish Gap to Mechum's River Depot. At Mechum's, Jackson's column turned northeast, toward Gordonsville. Overlaying the map are photographs of key decision makers.

Map courtesy of the Library of Congress; photo overlays courtesy of Wikipedia



A map of central Virginia, believed to have been published in 1861. The red arrows show Jackson's approximate route of march from the Shenandoah Valley to Richmond.

Map courtesy of the Library of Congress

all, they had to KNOW. They had to be certain. The risks of being wrong were significant.

What intelligence would Washington have needed? Multiple reports, updated over time, on the exact position and direction of travel of Jackson's main force. Federal intelligence elements would have had to be able to find Jackson's army, see it at regular intervals, and then get reports back to the Union lines at Fredericksburg.

If Jackson left the Valley, the Federals presumed he would go to one of two places: east toward Richmond or northeast toward Manassas and Washington. Although going to help Lee defend Richmond seemed the most likely course of action, Union leaders could not rule out the possibility that Jackson might strike into northern Virginia. In mid-June, McDowell raised concerns that Jackson might strike him in his current positions near Fredericksburg. On 14 June, McDowell telegraphed Stanton that "the forces of my command [are] too divided to support each other and give that protection to the capital which it is made my duty to afford." That left him "exposed to be attacked in detail, if Jackson acts offensively."⁵

Jackson's army went to Richmond. On 18 June, they left the Valley moving east from the town of Waynesboro

and crossed the mountains on the eastern side of the valley at Rockfish Gap. On 19 June, they reached the railroad station at Meachum's River, west of Charlottesville. They then moved northeast to the town of Gordonsville by 21 June. Jackson then moved east-southeast, toward Louisa and then Fredrickshall (near the modern-day Lake Anna Recreation Area). From Fredrickshall they moved south-east, and by the evening of 25 June, they reached Ashland, a town about 10 miles north of McClellan's forward lines outside of Richmond. The next day, they marched south and joined Lee's army.⁶ Jackson arrived just as the first of the Seven Days' Battles, the battle of Beaver Dam Creek, was finishing.

Thus, Jackson was in transit, east of (and clearly out of) the Shenandoah Valley from 19 to 26 June 1862. But it wasn't enough just to detect Jackson leaving the Shenandoah. Jackson had previously proven that he was willing (and able) to deceive his opponents. In early May, he marched part of his army out of the Valley to the east, to Meachum's River. There, wrote Confederate general John Imboden, "Jackson had collected, from Charlottesville and other stations on the Virginia Central Railroad, enough railway trains to transport all of his little army. That it was to be taken to Richmond when the troops were all embarked no one doubted."⁷

But Jackson had other plans. Once loaded, the trains headed west, back into the Valley. A few days later, on 8 May, Jackson won the first of his victories in the Valley Campaign, at the Battle of McDowell. So, it wasn't enough to know that Jackson left the Valley. Union Army intelligence would have to know that Jackson had not gone *back over* the mountains.

In his *Newsweek* article, GEN Powell defined “facts” as “verified information, which is then presented as objective reality.” He then elaborated: “The rub here is the verified. How do you verify verified? Facts are slippery, and so is verification. Today’s verification may not be tomorrow’s.” He said that facts “can change as the verification changes.”⁸ In late June 1862, the Union Army would have had to verify—not just once, but continuously—where Jackson’s army was. That would have required surveillance, or at least regular reconnaissance, of his force.

If Union Army intelligence analysts had prepared an event template of central Virginia, a good place for a named area of interest would have been the town of Gordonsville. From Gordonsville, Confederate troops could move either on Richmond (50 miles away) or on Fredericksburg (30 miles away). Observers watching Jackson’s army would not have a clear indication of his objective until they saw which way his troops headed as they left that town. Jackson left Gordonsville on 22 June. Throughout that day, his troops trudged along the roads heading southeast toward Louisa and then Fredrickshall.⁹ By the end of that day, there was enough evidence to indicate where Jackson was going.

Therefore, if Federal observers had been watching a Gordonsville “named area of interest,” they could have collected strong indications that Jackson was going to Richmond, but not until 22 June. The Seven Days’ Battles began on the evening of 26 June. Was 4 days enough time for Union scouts to transmit enough information through Union Army channels to convince Lincoln and Stanton that Jackson was heading for Richmond, in enough time for them to send McDowell to Richmond and still influence the upcoming fight?

That larger question raises several smaller ones. Did the Union Army even have the ability to collect such information? Probably not with its cavalry—at least, the cavalry



Sketch from the book *The Soldier in our Civil War: A Pictorial History of the Conflict, 1861-1865*, illustrating the valor of the soldier as displayed on the battlefield, from sketches drawn by Forbes, Waud, Taylor, Beard, Becker, Lovie, Schell, Crane, and numerous other eye-witnesses to the strife.

Photo courtesy of Wikimedia Commons

it had on hand. Once Jackson was out of the Shenandoah Valley, the Federal force most likely to detect his move across central Virginia was McDowell’s Department of the Rappahannock. Each of McDowell’s divisions had cavalry—approximately one regiment’s worth.¹⁰ Cavalry was the army’s traditional scouting arm. But it also performed local security. McDowell’s cavalry regiments spent much of their time on security patrol, and guarding railroads and supply routes. Louisa and Fredrickshall were more than 30 miles from Fredericksburg, the southernmost portion of McDowell’s lines. This was beyond the range that division-level cavalry normally covered. For example, a cavalry reconnaissance mission launched by one of McDowell’s brigade commanders near Fredericksburg “examined the country for 18 miles.”¹¹

McDowell did have an independent cavalry force—a brigade commanded by Colonel George Bayard. Bayard’s command, however, was in no position or shape to perform long-range reconnaissance in central Virginia in late June 1862. Bayard had spent the month of May chasing Jackson in the Shenandoah Valley. By June, his force was worn out. “We have had the advance ever since we have been here,” he said in a telegram from Harrisonburg, a town in the middle of the Valley, on 7 June. “We are utterly used up.”¹² In mid-June, Bayard did leave the Valley, arriving at Manassas by 20 June. Eight days later, his command was still in poor shape. “My brigade is in no condition to move at present,” he said in a telegram on 28 June. “We have only three kegs of horseshoes to shoe 500 horses.”¹³ 28 June was 2 days after the Seven Days’ Battles began.

What about scouts—observers moving alone or in small groups deep within enemy lines? *The War of the Rebellion: a Compilation of the Official Records of the Union and Confederate Armies* (also known as *The Official Records* or *OR*) contains several reports from groups of Union scouts in the Shenandoah Valley and northern Virginia. On 10 May, for example, three scouts working for General Robert Milroy returned to headquarters and gave a detailed and accurate report on Jackson's location and strength.¹⁴ Civil War intelligence historian Edwin Fishel identifies several men who worked directly for specific Union generals in Virginia, scouting miles beyond enemy lines.

Plenty of Union sympathizers lived in Virginia. It was not uncommon for civilians to move between the lines, especially in the war's early years. The war had been going on for nearly a year, which was enough time for the Union to recruit sympathizers in central Virginia who lived near areas of intelligence significance like Gordonsville. By no later than May, the Federals knew that Jackson might try to slip out of the Valley and head for Richmond. That left more than a month for the Union Army to infiltrate scouts into Virginia (or find Unionist locals) who could watch the mountain passes that Jackson would need to use, were he to try to join Lee.

So, the Union Army DID have the ability to collect the raw data necessary to detect Jackson's location and direction of travel. Individual scouts from McDowell's command, or Union sympathizers along Jackson's route of march, could have counted the troops passing by and noted their direction of march. Those reports could have provided the detailed information needed to reassure Lincoln and Stanton that Jackson was marching to Richmond—IF there had been enough of those reports, AND if they'd arrived in time.

Many Civil War scouts had to deliver their reports themselves. They did not have courier services, and they certainly had no long-range communications. Once they had gathered their information, they had to leave their area of operations, return to their headquarters, and report. They could not stay on station and constantly watch their targets. This caused gaps in coverage.

That travel time was often measured in days. Milroy's scouts, for example, took 5 days to complete their mission.¹⁵ Jackson's cavalry screened his route of march, and he placed pickets on the roads to interdict civilian travelers. Any Union observer heading north had to elude those security forces; that lengthened the trip, at the very least. At worst, the observer might be caught. Historian Edwin Fishel tells of several Union scouts who were captured during the Valley Campaign and spent months in Confederate prisons.

As for timeliness—how soon was “soon enough?” How quickly did the information on Jackson's move to Richmond need to get into the hands of Union decision makers? Or to use modern military intelligence terminology, what was the “latest time intelligence is of value”?

Lincoln and Stanton would not have been satisfied with just one or two reports, or “observations,” of Jackson's move. They would have sought more reports for corroboration. As GEN Colin Powell said, verification can be fleeting. (“Today's verification may not be tomorrow's.”¹⁶) Washington needed a steady stream of reports, from multiple sources. Collecting enough reports to satisfy Washington could easily have taken several days.

To make matters worse, McDowell was not ready to step off for Richmond on a moment's notice. In late June, his command was still scattered across Northern Virginia. McDowell had three divisions. One, commanded by General James Shields, had just returned from chasing Jackson in the Valley. It was as worn out as Bayard's cavalry brigade. It probably could not have moved on short notice, especially to pursue a target as potent as Jackson's army. That left McDowell with two divisions. One, under General Rufus King, was at Fredericksburg. The other, under General James Ricketts, was at Manassas.¹⁷ Manassas is more than 30 miles from Fredericksburg. If McDowell wanted to have a force large enough to fight Jackson, he would have needed Ricketts to march to Fredericksburg and join King. That would have given McDowell almost 20,000 men.

How long would that march have taken? Fortunately, we have someone to tell us—McDowell himself. On 26 June, he sent a telegram to Stanton, who had apparently asked him how long it would take to consolidate his forces. McDowell replied that it was “a three days' march” from Manassas to Fredericksburg.¹⁸ By 26 June, it was already too late. The Seven Days' Battles would start that night.

Intelligence can (and should) drive operations, but that intelligence has to be strong enough to answer decision makers' key concerns and arrive in time for leaders to act on it. In June 1862, the Union Army lacked the ability to report enough information on Jackson's operations to build a verified assessment of his objective, which was convincing enough to soothe Washington's concerns for the safety of the nation's capital, in enough time to enable McDowell's troops to make a difference outside Richmond. The ability to collect existed; the ability to report and assess enough information quickly enough did not.

In a telegram to McClellan on 20 June, Abraham Lincoln himself summed up the frustrations of tracking 19th century

enemy armies. The president referenced a report from a Union commander in the Valley, which said that Jackson was not only still in the Valley but also had received reinforcements from Lee. "This may be reality," said Lincoln, "and yet may only be contrivance for deception, and to determine which is perplexing." Lincoln had to play the safe hand. "If we knew [the report] was not true, we could send you some more force, but as the case now stands we do not think we safely can."¹⁹ Lincoln may have thought Jackson was not heading for Washington. But given the constraints he faced, that wasn't good enough. He needed to know, for sure.

You Will Really Have to "Know"

McClellan wildly and routinely overestimated the strength of the Confederates facing him. That helped make him a "figure of fun" among Civil War historians. But the Union Army did face real challenges in tracking and assessing one of the most wily generals of the whole war. Catching Stonewall Jackson before he reached Richmond would have required a high volume of reliable and updated information, delivered very quickly. That was too much to ask of the Union Army—and probably any army—in the early summer of 1862. Modern-day decision makers will also find themselves in positions where they cannot afford to be wrong about their enemy. For the intelligence staffs supporting those decision makers, telling the boss "what you think" will not be enough. You will really have to "know." 🌟

Epigraph

Colin Powell, "Colin Powell on the Bush Administration's Iraq War Mistakes," *Newsweek*, 13 May 2012, <https://www.newsweek.com/colin-powell-bush-administrations-iraq-war-mistakes-65023>.

Endnotes

1. Colin Powell, "Colin Powell on the Bush Administration's Iraq War Mistakes," *Newsweek*, 13 May 2012, <https://www.newsweek.com/colin-powell-bush-administrations-iraq-war-mistakes-65023>.

2. "1862 Seven Days' Battles," Richmond National Battlefield Park, National Park Service website, accessed December 24, 2018, <https://www.nps.gov/rich/learn/historyculture/sevendays.htm>.

3. U.S. War Department, *The War of the Rebellion: a Compilation of the Official Records of the Union and Confederate Armies* (Washington, DC: U.S. Government Publishing Office, 1885), ser. I, vol. XII, part I, 326.

4. "Overview of the 1862 Stonewall Jackson Valley Campaign," Cedar Creek & Belle Grove National Historical Site website, National Park Service, accessed December 24, 2018, <https://www.nps.gov/cebe/learn/historyculture/overview-of-the-1862-stonewall-jackson-valley-campaign.htm>.

5. U.S. War Department, *The War of the Rebellion*, ser. I, vol. XII, part I, 286.

6. Timeline information courtesy of Jeff Driscoll (Cedar Creek & Belle Grove National Historical Site) and Robert Krick (Richmond National Battlefield Park).

7. John D. Imboden, "Stonewall Jackson in the Shenandoah," in *Battles and Leaders of the Civil War*, vol. 2 (New York: The Century Co., 1887-1888), 286.

8. Powell, "Colin Powell."

9. Timeline information courtesy of Robert Krick (Richmond National Battlefield Park).

10. U.S. War Department, *The War of the Rebellion*, ser. I, vol. XII, part III, 309.

11. *Ibid.*, 390.

12. *Ibid.*, 365.

13. *Ibid.*, 439.

14. *Ibid.*, 163.

15. *Ibid.*

16. Powell, "Colin Powell."

17. General McDowell gives the position of General King's division in a telegram on 26 June. U.S. War Department, *The War of the Rebellion*, ser. I, vol. XII, part III, 433. Robert Krick (Richmond National Battlefield Park) determined the position of Ricketts' division by reading monthly reports in the *The War of the Rebellion* from regiments assigned to that division. Those regiments reported they were at Manassas in late June 1862.

18. *Ibid.*, 433-434.

19. John Nicolay and John Hay, *Complete Works of Abraham Lincoln* (New York: The Century Company, 1894).

The author wishes to thank National Park Service historians Robert Krick (Richmond National Battlefield Park) and Jeff Driscoll (Cedar Creek & Belle Grove National Historical Site) for their assistance and advice.

Donald Smith is a retired Army military intelligence officer. For 8 years, he was the National Reconnaissance Office's field representative to Fort Huachuca, AZ. He holds a master's degree in strategic intelligence from the Joint Military Intelligence College. He currently teaches Distributed Common Ground System-Army operations at the U.S. Army Intelligence Center of Excellence. Mr. Smith is expanding this article into a book.

"The most important thing I learned is that soldiers watch what their leaders do. You can give them classes and lecture them forever, but it is your personal example they will follow."

– General Colin Powell



Introduction

Applying a best practice from the U.S. Army Intelligence Center of Excellence (USAICoE) Writing Program reduced the length of the USAICoE Lessons Learned report by 33 percent. When writing intelligence products, you too can obtain similar results by applying the writing best practices available on the CW2 Christopher G. Nason Military Intelligence (MI) Library webpage, accessed through the Intelligence Knowledge Network (IKN) public portal.

As much as I would like to think the preceding paragraph meets the requirement for a lessons learned article in the *Military Intelligence Professional Bulletin* (MIPB)—i.e., inform the reader—I will share additional information of potential benefit to MI professionals.

The best part of serving in a lessons learned position is receiving an email or telephone call describing how applying a lesson or best practice led to improved performance or mission success. Soldiers and leaders continually seek to improve their knowledge, skills, and abilities through independent self-development. The best leaders use their knowledge, skills, and abilities to increase the performance and readiness of their subordinate personnel and units. We share this attribute by seeking to improve the quality and effectiveness of our lessons learned support to MI leaders and Soldiers. In order to enhance our lessons learned processes, we use a variety of sources: academia, media, dissertations, studies, research, and analysis. Our most recent lessons learned effort realized quantifiable improvements in quality and effectiveness that may also yield similar results with others throughout the MI community.

The Lessons Learned Team collaborated with USAICoE's Directorate of Training, Learning Enhancement Branch (LEB), to help streamline our collection, reporting, and production process. We first enlisted the assistance of LEB's Dr. Macaela Cashman with whom we had previously partnered in a write for release project. She had become familiar with the processes, operations, and goals of the USAICoE

Lessons Learned mission during the write for release project collaboration. When members of the Lessons Learned Team were telling Dr. Cashman about the lessons learned process and associated tasks and challenges, they realized how the lessons learned functions of discovery, validation, integration, and assessment were similar to the components of the intelligence process. (If you are unfamiliar with the intelligence process, seek a copy of FM 2-0, *Intelligence*.)

Nonfiction Storytellers

Lessons Learned personnel share a feature with the MI professionals we support—we're storytellers. We are doing more than presenting just a series of facts: we are analyzing and interpreting the facts to develop the story, the "so what" of our observations. Some might be uncomfortable with using the word *story* to describe MI or lessons learned tasks, but it is what we do when we provide a report for commanders or our readers. I am not talking about fiction or fables. The stories we tell describe training or operations usually obtained from direct observation.

I made the connection between the concept of a story and MI tasks when an LEB tutor, Mrs. Floramae Kerr, lent me Stephen King's book *On Writing: A Memoir of the Craft*. In his book, King highlights effective techniques that clearly and concisely impart a description of events to his readers. Replace *readers* with *leaders* in the preceding sentence, and the link to MI writing is clear. We write to inform our *leaders* just as King writes to inform his *readers*. Clarity and brevity are features valued in both intelligence and lessons learned reports. A recent anecdote confirmed this when a commander told the intelligence officer, "Don't tell me everything that you know; just tell me what I need to know now." King's strategy for writing—telling readers only what they need to know—is the same strategy we use in Army Effective Writing. This is echoed in section IV, "Effective Writing and Correspondence," of AR 25-50, *Preparing and Managing Correspondence*, which emphasizes active voice and bottom line up front.

Stories of Past, Present, and Future Events

Three types of nonfiction stories relate to Army operations and contribute to the commander's situational understanding:

- ◆ What has happened?
- ◆ What is happening now?
- ◆ What is going to happen?

Every Army staff officer, element, or process tells the first two types of stories when appropriate. Information regarding what has happened and what is happening now is routinely contained in orders, reports, or staff running estimates. At every echelon, an intelligence staff officer, the J/G/S-2, tells the commander the story of past and present events when necessary.

The remaining staff and subordinate element commanders also tell their respective warfighting function stories to the commander. Although they differ, these stories provide insight and they support sharing situational understanding for better awareness. Using facts and facts-based assumptions during planning and operations to describe a future concept of operations (CONOPS) in part describes what the commander intends to happen. Describing the CONOPS in sequence involves stating a number of familiar tasks, conditions, techniques, and procedures. The CONOPS offers a predictive story to guide future events as the commander directs.

The responsibility we share in writing clearly and concisely brings us closer, but not quite, to fictional story telling. The estimated probability of occurrence inextricably links the J/G/S-2 story to what the enemy might do. Quantitative and/or qualitative assessments of the pertinent mission and operational variables ground the story of what may happen in the future. Facts of past and present events support expectation of future conditions.

What sets MI stories apart from those of the Army's other branches is the responsibility of the J/G/S-2 to describe what the enemy is going to do. Our story explains how the enemy force will operate; distinguishing what is probable from what is possible. Sometimes the story unfolds as we anticipated; sometimes the enemy changes the plot mid-chapter. Our ability to tell a story describing future events—whether it is an oral, written, or illustrated description of an estimated enemy course of action—depends on writing effectively. A written description should always accompany an enemy course of action sketch. A well-written story enables anyone to convey the situation accurately to the commander; all one has to do is read the narrative. A poorly written story requires a lot of knowledge and quick think-

ing for someone to be able to tell it effectively. With the higher operating tempo and anticipated casualty rates during large-scale combat operations, a story's author may be unavailable to tell the story directly. Thus, writing clearly does not just benefit the commander; it helps us all to support each other and increase mission success.

Writing Well Takes Effort

Writing well demands intention and careful selection of detail. I used to have a quote from Enrique Jardiel Poncela (Spanish playwright and novelist) posted near my desk. It said, "When something can be read without effort, great effort has gone into its writing." When I talked to the team about the importance of writing well, they would invoke the saying "Perfect is the enemy of good enough."¹ I would immediately point to the quote by my desk, because writing is not about being perfect; it is about effort. Jardiel Poncela's words about effort emphasize MI's inherent responsibility to support the commander in every way possible. We must not encumber the commander with having to decipher the important points in our writing. Our commanders will have much to do during large-scale combat operations. Our writing should not cause anyone to do mental Cheetah-flips trying to figure out the important parts of the story. Well-written products are easier for our leaders and colleagues to comprehend in all of the operational phases identified in FM 3-0, *Operations*. Our commanders require clear, concise, accurate, and timely intelligence products to best support rapid understanding and decision making.

Using accurate, commonly understood terms is, and will continue to be, highly important in exchanging information with our multinational partners. Words carry meaning. Furthermore, doctrinal terms convey precision and associated context. Using the correct word will help a multinational partner who is not a native English speaker to understand. Precise word use facilitates accurate translations of intelligence products from English into a variety of foreign languages. When discussing lessons learned products, we have found that using doctrinal terms in a specific manner eliminates avoidable questions. "Commonly understood" terms are often not commonly understood because MI and Army personnel have a variety of experiences and expertise; additional refinement may be needed when seeking to identify and resolve problems.

I Don't Write Good

I don't write *well*. Some may read the preceding sentence as my condescending correction. I wrote it as a shared declaration of a colleague's despair. The most time-consuming part of my job is writing, and then reviewing and revising what I already wrote. I used to joke with my fellow Soldiers

when struggling with facts, percentages, correlation of forces matrices, or any other problem involving numbers. I would tell them if I had been better at math in high school, I would not have had to join the Army. Determining declination or a back azimuth was easy due to the diagram provided in a map's legend and my ability to perform an about-face respectively. Converting odometer markings to kilometers for mounted land navigation often fell to a pocket calculator. Unfortunately, my English grades were only slightly better (less worse?) than my math scores.

Looking back at over 40 years of uniformed and civilian Army service, I now regret not having paid more attention in English classes because much of what I have done in MI has involved writing and compiling the writings of others. As in most endeavors, we improve when a challenge forces us out of our comfort zone. Writing is difficult. Writing well is even more difficult. Writing well in support of rapidly changing large-scale combat operations conditions may be the most difficult. Regardless of our different skill levels, we can accept the challenge to write more effectively.

Hope is not a Method

There is hope for those of us who do not know the difference between a dangling participle and a preposition. The USAICoE Writing Program is available to any Soldier or MI professional. To use this resource, access the CW2 Christopher G. Nason MI Library website on the IKN public portal (<https://www.ikn.army.mil/apps/MILibrary/>). Then scroll down to the USAICoE Writing Program icon "Writing & Citation Resources" and click on it. A number of tools are available for your use—writing aids, references, videos, and guides. The site also posts information about tutoring support services available both in person and online. We will continue to apply the benefits of the USAICoE Writing Program to increase our production quality and efficiency.

In closing, I will add a few more details about how we reduced the length of the lessons learned report by 33 percent. We took techniques learned from the Directorate of Training LEB personnel and from the CW2 Christopher G. Nason MI Library website and applied them to our most recent lessons learned collection report. We eliminated 7

pages of text by removing more than 2,000 words—which is about the length of this MIPB article. In addition to reducing the original report by 33 percent, we achieved another 25 percent reduction by consolidating 5 separate observations into the final 15 observations. If I were better at math, I'd be able to tell you the exact percentage of improvement. ✨

Endnote

1. " 'Perfect is the enemy of good'...is an aphorism which is commonly attributed to [French writer and philosopher] Voltaire, who quoted an Italian proverb in his *Dictionnaire philosophique* in 1770." "Perfect is the enemy of good," Wikipedia Foundation, last modified 14 December 2018, 01:46, https://en.wikipedia.org/wiki/Perfect_is_the_enemy_of_good. Many interpretations of this quote exist, one of which is "since you can never achieve perfection, if you wait to be perfect before you do anything, nothing will ever get done." John English, "What does 'perfect is the enemy of good' mean?" *Quora* (blog), February 21, 2017, <https://www.quora.com/What-does-perfect-is-the-enemy-of-good-mean>.



The poster is for the USAICoE Writing Program. At the top, it features the U.S. Army logo on the left and the USAICoE Writing Program logo on the right, which includes a fountain pen icon. The main text reads "NEED HELP with your WRITING?" in large, bold, yellow-outlined letters. Below this, it says "You don't have to do it alone." and "FREE TUTORING SUPPORT SERVICES". A box titled "Location and Times:" lists walk-in hours and appointment times. At the bottom, it provides the email address usaicoetutor@gmail.com and a small icon of an ink bottle.

USAICoE WRITING PROGRAM

NEED HELP
with your
WRITING?

You don't have to do it alone.

FREE TUTORING SUPPORT SERVICES

Location and Times:

MI LIBRARY Walk-In Hours:

- SUN - 1200-1800
- MON, WED, FRI 1100-1300
- TUE, THU - 1100-1300 and 1600-1730

Appointments: SUN 1100-1800
MON-FRI 0900-1730
SAT-Upon Request (48 Hr. notice)

Submit writing online or schedule an appointment via email
usaicoetutor@gmail.com

Awards

For Excellence in Military Intelligence

Captain Abdulla Mizead 2019 Recipient of the Lieutenant General Sidney T. Weinstein Award For Excellence in Military Intelligence

The Military Intelligence (MI) Corps created the Lieutenant General Sidney T. Weinstein Award in 2007 to honor the accomplishments of the "Father of Modern Military Intelligence." LTG Weinstein was not only a fine officer; he was a mentor, a role model, a friend to many, and a dedicated family man. This award is given annually to one MI captain who, through his or her actions, demonstrates the values and ideals for which LTG Weinstein stood: Duty, Honor, and Country.



CPT Abdulla Mizead was born in Baghdad, Iraq, and first worked as a linguist with United States forces in 2003. He enlisted in the United States Army as an infantryman in 2010 and deployed as a team leader to Kandahar, Afghanistan, in 2011. In 2012, he earned his commission as a military intelligence officer. His assignments include Assistant S-2, 1-187 Infantry, 3rd Brigade Combat Team, 101st Airborne Division (AASLT); Iraq Advisor to the Commanding General of 1st Infantry Division and Combined Joint Forces Land Component Command-Iraq during Operation Inherent Resolve (OIR); and Intelligence Analyst and Team Chief, U.S. Central Command (USCENTCOM).

In mid-2017, CPT Mizead served as the Cultural Advisor to the Commanding General (CG) of III Corps and Combined Joint Task Force (CJTF)-OIR in Iraq and Syria, filling an O-5 joint billet. He briefed Congressional, USCENTCOM, and CJTF-OIR leaders on critical developments in the area of operations and facilitated key leader engagements with senior regional political and military leaders. When Iraqi and Kurdish Security Forces clashed in October 2017, threatening to destabilize Iraq and disrupt the Defeat-ISIS mission, the CJTF-OIR CG sponsored an initiative to end hostilities. CPT Mizead convinced Iraq's Prime Minister and Chief of Defense and the Minister of Peshmerga to agree to a ceasefire. His critical role in the United States-sponsored negotiations was instrumental in preventing a potential civil war in Northern Iraq. CPT Mizead also assisted Department of State, Office of Security Cooperation-Iraq, and the Iraqi Prime Minister's Office in signing the \$1.1 billion United States loan to develop the Iraqi Security Forces. Due to his efforts, Iraq agreed to share detained foreign terrorist fighters' critical information and biometric data with the United States to enable exploitation of vital information on terrorist networks.

CPT Mizead currently serves as the Senior Intelligence Analyst for the Security Forces Team in USCENTCOM.

CPT Mizead's awards and decorations include the Defense Meritorious Service Medal, Joint Service Commendation Medal, Army Commendation Medal, Army Achievement Medal, and Air Assault Badge. He earned his bachelor's and master's in English from Baghdad University, a master's in journalism from Columbia University, and an associate's degree in intelligence studies from Cochise College. 🌟

Awards For Excellence in Military Intelligence

Chief Warrant Officer 2 Aaron A. Johnson 2019 Recipient of the Chief Warrant Officer 5 Rex Williams Award For Excellence in Military Intelligence

The Military Intelligence (MI) Corps established the Chief Warrant Officer 5 Rex Williams Award in 2016 to recognize the outstanding achievements of a company grade warrant officer (WO1-CW2) within the MI community. This award is named in honor of an icon in MI, who spent his 31-year military career improving training, mentoring countless Soldiers, and helping define the foundations of intelligence analysis. CW5 Williams also served as the first Chief Warrant Officer of the MI Corps.




CW2 Aaron Johnson was born in Dunedin, Florida, in 1987. He joined the U.S. Army as a 97E (now 35M) Human Intelligence (HUMINT) Collector in 2006. CW2 Johnson served in various enlisted and noncommissioned officer assignments as a HUMINT professional, including multiple deployments with conventional and special operations forces in Iraq and Afghanistan, before being commissioned a warrant officer in 2014. He served as the Operational Management Team (OMT) Officer-in-Charge (OIC), Delta Company, 8th Brigade Engineer Battalion (BEB), 1st Cavalry Division, Fort Hood, Texas, and OMT OIC, Korea rotational deployment, also with Delta Company, 8th BEB. While assigned to Schofield Barracks, Hawaii, he served as the OMT OIC and Information and Electronic Warfare OIC for Delta Company, 65th BEB, 2nd Infantry Brigade Combat Team, 25th Infantry Division and currently serves as the HUMINT Analysis Cell OIC for the 25th Infantry Division. CW2 Johnson is also a primary instructor cadre at the Digital Intelligence System Master Gunner Course on Fort Bragg, North Carolina.

During 2018, CW2 Johnson's myriad accomplishments impacted not only the 25th Infantry Division, but multiple organizations across Hawaii and throughout the U.S. Army. He assisted in the construction of the Division language lab; received the highest overall evaluation during the intelligence oversight inspection in the Division; established a Leaders Training Program for all company grade officers in the Division; and advised the 8th Military Police Brigade on detention operations best practices for use in their field exercises. He also sent more than 20 division

Soldiers to the Human Intelligence Training Joint Center of Excellence, maintaining a 100-percent graduation rate.

CW2 Johnson's competence in digital intelligence architecture was illustrated by his development of a robust lower tactical internet data transfer system that proved a viable solution to data transfer in an antiaccess/aerial denial environment. Additionally, to find unique solutions to increase intelligence readiness and operations, he worked with other 25th Infantry Division warrant officers to develop a structured data reporting method utilizing United States Message Traffic Format to transfer HUMINT information to the tactical edge in minutes. His efforts in the development of structured data reporting and object based production increased the tactical relevance of HUMINT and enabled time sensitive targeting during multiple exercises.

CW2 Johnson's awards include the Bronze Star, Army Commendation Medal, Army Achievement Medal, Afghanistan Campaign Medal, Iraq Campaign Medal, Korea Defense Service Medal, Military Outstanding Volunteer Service Medal, Military Unit Commendation, Knowlton Award, and German Armed Forces Proficiency Badge (Silver). He has an associate's degree in intelligence operations from Cochise College. 

Sergeant Oscar Ochoa III **2019 Recipient of the** **Command Sergeant Major Doug Russell Award** **For Excellence in Military Intelligence**

The Command Sergeant Major Doug Russell Award was created in 2001 in honor of an esteemed noncommissioned officer (NCO) who personified the integrity, moral courage, and loyalty espoused in the NCO Creed. CSM Russell served in uniform for 32 years, followed by 14 years as the Director of NCO and Enlisted Affairs, Director of Retiree Activities in the Association of the U.S. Army, and President of the American Military Society. The award is presented annually to an outstanding Soldier in the rank of sergeant or below, who has made a significant contribution to the Military Intelligence Corps.



SGT Oscar Ochoa III was born in El Paso, Texas, in 1989. He enlisted in the U.S. Army in September 2011 as a 35M, Human Intelligence Collector. After attending Advanced Individual Training at Fort Huachuca, SGT Ochoa was assigned to the Multifunction Platoon, Delta Company, 3rd Brigade Engineer Battalion, 3rd Brigade, 4th Infantry Division, Fort Carson, Colorado. From 2012 to 2016, SGT Ochoa participated in more than 20 field training exercises, two brigade-level gunnery events, the National Training Center, and a nine-month deployment to Camp Buerhing, Kuwait. In addition to being recognized as Delta Company Soldier of the Month for 12 consecutive months and top gunner at 3rd Brigade, he received an Army Commendation Medal for his performance as a Foreign Military Collections Activities strategic debriefer during his deployment to Kuwait.

In June 2016, SGT Ochoa received orders to Alpha Company, 303rd Military Intelligence Battalion, 504th Expeditionary Military Intelligence Brigade, Fort Hood, Texas. During a 12-month deployment to southeast Afghanistan in 2017-2018, as a Team Leader/Assistant Team Leader, he conducted military source operations in support of Operation Freedom's Sentinel. Working seamlessly with the S-2 of the 1st Security Forces Advisory Brigade at Advisory Platform Lightning in the Gardez District, SGT Ochoa provided ground force commanders with human intelligence integrated with signals intelligence, geospatial intelligence, targeting analysis, and electronic warfare information operations.

SGT Ochoa's intelligence reporting led to the prevention of a planned attack on a United States company based in Afghanistan, enabled a raid on a high-value individual's residence, neutralized two vehicle-borne improvised explosive devices targeting coalition forces, and facilitated the apprehension of two insider threats, saving the lives of United States personnel and partnered Afghan forces in the Task Force Southeast area of operations. SGT Ochoa also coordinated with the U.S. Federal Bureau of Investigation to counter a homeland security threat. His efforts were personally recognized by MG Gary Johnston, the Resolute Support J-2, and BG Richard Johnson, the Task Force Southeast Commander.

SGT Ochoa is currently serving in the 163rd Military Intelligence Battalion.

SGT Ochoa's awards and decorations include the Army Commendation Medal, Army Achievement Medal, Good Conduct Medal, National Defense Service Medal, Afghanistan Campaign Medal, Noncommissioned Officer Professional Development Ribbon, Army Service Ribbon, NATO Medal, Certificate of Appreciation, and Marksmanship Qualification Badge Expert-Pistol. 🌟

Awards For Excellence in Military Intelligence

Ms. Courtney L. Sustaire 2019 Recipient of the Ms. Dorothe K. Matlack Award For Excellence in Military Intelligence

In 2018, the Military Intelligence (MI) Corps established the Ms. Dorothe K. Matlack Award to honor a Department of the Army Civilian (GG-9—GG-12) who has made a significant contribution to MI within the previous three years. The Matlack Award is named for one of MI's early pioneers and champions of Army human intelligence efforts. Dorothe Matlack started her career in 1948 as a GS-2 File Clerk and retired in 1975 after serving 27 years in the Office of the Assistant Chief of Staff for Intelligence.



Ms. Courtney Sustaire enlisted in the U.S. Army in 2001 as a 35G, Imagery Intelligence Analyst. From June 2003 to November 2012, she deployed three times to Iraq and once to Afghanistan. In December 2015, she separated from service and served as a geospatial targeting analyst in support of U.S. Special Operations Command (USSOCOM) mission requirements.

In May 2016, Ms. Sustaire joined the Army Geospatial Intelligence (GEOINT) Battalion (AGB) as a Department of the Army Civilian. In November 2016, she volunteered to deploy in support of USSOCOM as the tactical operations center sole GEOINT analyst. While deployed she produced more than 700 imagery products and reports used for targeting action. Her efforts aided in vital intelligence collection, which led to the safety of multiple allied forces and up-to-date situational awareness reports for teams on the ground. In 2017, Ms. Sustaire forward deployed and served as the primary GEOINT analyst for the tactical operations center, creating thousands of GEOINT data points representing accurate battlefield representation for near-real-time use by commanders, mission partners, and partner nations.

Currently serving as a Supervisory Intelligence Specialist for the AGB, Ms. Sustaire is responsible for providing GEOINT expertise and predictive analysis in current and emerging Department of Defense intelligence requirements. Her 25-member military and civilian team manages requirements that span a variety of tactical and strategic mission sets from general imagery support to specialized cyber support with various customers spanning across six combatant commands. She is not only an expert in her tradecraft but she is dedicated to the personal and professional development of her team. Ms. Sustaire fosters an environment where critical thinking is encouraged to find creative solutions to GEOINT problems. She provides an environment where all analysts are expected to thoroughly research potential targets and problem sets, presenting a methodology on how to best conduct exploitation and analysis, and execute mission requirements. Her leadership allows analysts to take initiative and responsibility for production requirements in the absence of direction, resulting in decreased time spent waiting for guidance and increased time dedicated to analysis.

Ms. Sustaire has attended more than 1,600 hours of GEOINT and intelligence training courses throughout her career. She has also earned a bachelor of arts degree in humanities, with a focus in art history, from the University of Maryland—University College and is pursuing a master of science degree in geographic information systems with Johns Hopkins University. 🌟

Moments in MI History

Linguists Contribute to Success of Merrill's Marauders

by Lori S. Stewart, USAICoE Command Historian

In the early morning hours of March 4, 1944, the Intelligence and Reconnaissance Platoon of the Orange Combat Team, 3rd Battalion, 5307th Composite Unit (Provisional), found itself facing heavy Japanese fire. Led by 2LT Logan E. Weston, the platoon moved to higher ground overlooking a river, where they could see any enemy approaching from the east and southeast. Soon, however, Japanese forces were approaching the isolated platoon from the west and north.

SGT Henry Goshō, a Japanese-American Nisei¹ from Seattle, Washington, listened closely to the orders the Japanese officers were shouting. He was able to translate the information quickly, enabling the platoon to shift its automatic weapons to meet each of the attacks. After repelling the fifth attack, 2LT Weston radioed a supporting mortar section, whose timely response allowed the Intelligence and Reconnaissance Platoon to withdraw across the river. With the mortar section's assistance, the platoon had destroyed two thirds of the Japanese force and kept the enemy from attacking the rest of Orange Combat Team further downriver. Goshō's actions undeniably helped the platoon survive the five-prong attack by a larger force.

The objective of the 5307th Composite Unit, a temporary commando unit better known as Merrill's Marauders, was to harass the enemy and disrupt their supply and communications lines in advance of Allied efforts to reestablish a land supply route to China through Burma. The long-range penetration unit constituted the only American ground combat forces designated for the China-Burma-India Theater. Beginning in October 1943, BG (later MG) Frank Merrill quickly organized and trained the approximately 3,000 men for the "dangerous and hazardous mission" they would undertake between February and May 1944.

Goshō was one of 14 linguists who volunteered for assignment with the Marauders. The others were Thomas Tsubota, Roy Nakada, Robert Hondo, Edward Mitsukado, Herbert Miyasaki, Howard Furumoto, Russell Kono, Calvin Kobata, Akiji Yoshimura, Ben Sugata, Jimmie Yamaguchi, Roy Matsumoto, Grant Hirabayashi, and William Laffin. Seven of the linguists were from Hawaii and the others hailed from California or Washington.

Each linguist had a unique story. Miyasaki served as BG Merrill's personal interpreter, and Goshō, a member of the Ranger Hall of Fame, earned the nickname "Horizontal Hank" because his penchant for directing his platoon's machine gunners often exposed him to enemy fire. Hirabayashi was allergic to an ingredient in the Army's K-rations and often had to live

off the land. Despite being sick, he commonly crawled behind enemy lines to eavesdrop and bring back timely intelligence. CPT Laffin, of Japanese descent through his mother, had been in Japan at the time of the attack on Pearl Harbor



National Archives Photo

Men with the 5307th Composite Unit stop to rest on the Ledo Road in northern Burma, March 1944. The physical environment Merrill's Marauders contended with included massive mountain ranges and rugged hills coupled with a tropical rain forest climate.



Henry H. Goshō, a Washington native, volunteered for service in the U.S. Army in 1942. Fighting under the toughest conditions for 16 months, Goshō was seriously wounded, lost a kidney, and suffered innumerable attacks of malaria, typhus, and jungle rot. He was medically discharged from the Army in June 1945.

and returned to the United States as part of an exchange of civilians in 1942. After graduating from the Military Intelligence Service Language School in 1943, he served as the intelligence officer for Merrill's Marauders and provided oversight for the Nisei linguists. Tragically, Laffin was killed when enemy fighter planes shot down his L-1 observation aircraft near the Myitkyina airstrip in mid-May 1944.

Perhaps one of the most well-known Nisei linguists who served with Merrill's Marauders was MSG Roy Matsumoto (Military Intelligence and Ranger Halls of Fame). Matsumoto climbed trees to tap enemy telephone lines. On one occasion, he learned the location of a thinly defended enemy ammunition dump, subsequently destroyed by aerial bombing. In another, he overheard the enemy's plans for a late night assault. Passing the information on, he enabled a smaller U.S. force to withdraw before the attack. Matsumoto also translated a captured Japanese map that indicated a planned attack on the Chinese 22nd Division near Shaduzup. His greatest contribution, however, came when he infiltrated behind enemy lines and learned of plans for a dawn attack on his battalion. The Americans relocated their positions overnight and, in the morning, launched their own surprise attack. When Matsumoto stood up and yelled, in Japanese, an order to attack, the Japanese troops obeyed and charged directly into an American ambush. For his exceptionally meritorious conduct, Matsumoto received the Legion of Merit.

The 5307th disbanded in August 1944 after having achieved its objectives to disrupt the enemy and capture the all-weather airstrip and communications center at Myitkyina, key to the re-establishment of a major overland supply route to China. Approximately one third of the unit's personnel were killed in action. Another third were severely wounded.



Roy Matsumoto (right) volunteered for the Army from an internment center in 1942 and retired as a master sergeant in 1963.

Amazingly, only one of the Japanese-American linguists had been killed during the 4-month campaign. After the war, BG Merrill stated unequivocally, "I couldn't have gotten along without them. Probably few realized that these boys did everything that an infantryman normally does plus the extra work of translating [and] interrogating."² 🌸

Endnotes

1. The word *Nisei* is "a Japanese language term used in countries in North America and South America to specify the children born in the new country to Japanese-born immigrants." Wikipedia, s.v. "Nisei," last modified 1 November 2018, 23:49, <https://en.wikipedia.org/wiki/Nisei>.
2. Marauder Unit History (website), accessed 10 December 2018, <http://www.marauder.org/nisei01.htm>.

Fort Huachuca Museum








Check out the Fort Huachuca Museum website at:
<https://www.ikn.army.mil>
 Click on the **Fort Huachuca Museums** link



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 under 3,000 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 that 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 520-533-4662) 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 Cibique St.
Fort Huachuca, AZ 85613-7017

Headquarters, Department of the Army.
This publication is approved for public release.
Distribution unlimited.

PIN: 204533-0000