

# MI PROFESSIONAL BULLETIN



July-December 2024  
PB 34-24-2

A silhouette of a soldier operating a tank, set against a warm, orange-hued sunset background. The soldier is positioned on the left side of the tank, looking through a periscope. The tank's turret and various antennas are visible. The overall scene is bathed in the golden light of the setting sun, with a large tree visible in the background on the right.

**SEMIANNUAL  
ONLINE  
COLLECTION**

### **Commanding General**

MG Richard T. Appelhans

### **Command Sergeant Major, MI Corps**

CSM Jesse M. Townsend

### **Chief Warrant Officer, MI Corps**

CW5 Peter J. Davis

### **Chief of Staff**

COL Brendon K. Dever

### **Commandant, Intelligence School**

COL Sean P. Coakley

### **Director of Training and Doctrine**

Beth A. Leeder

### **Editor in Chief**

Christopher Amador

### **Managing Editor**

Tracey A. Remus

### **Associate Editor**

Lorilynn Iversen

### **Design and Layout**

Jonathan S. Dingler

### **Cover Design**

Jonathan S. Dingler

### **Military Staff**

SFC Andrew J. Gunn

### **Manuscripts**

Please send your manuscripts, including supporting documents, and any inquiries by email to—[usarmy.huachuca.icoe.mbx.mipb@army.mil](mailto:usarmy.huachuca.icoe.mbx.mipb@army.mil); visit our webpage for full article submission guidelines at <https://mipb.army.mil>.

### **Mailing Address**

MIPB, DOTD, USAICoE, 550 Cibique St., Fort Huachuca, AZ 85613-7017.

### **Reprints**

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

*The views expressed in the 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 supercede information in any other Army publications.*

The U.S. Army Intelligence Center of Excellence publishes the Military Intelligence Professional Bulletin (MIPB) under the provisions of AR 25-30. MIPB presents information designed to keep intelligence professionals informed of current and emerging developments within military intelligence. MIPB provides an open forum for the exchange and discussion of ideas; concepts; tactics, techniques, and procedures; historical perspectives; problems and solutions, and other topics for purposes of professional development.

By Order of the Secretary of the Army:

**RANDY A. GEORGE**

*General, United States Army  
Chief of Staff*

Official:



**MARK F. AVERILL**

*Administrative Assistant  
to the Secretary of the Army*

**2506209**

# MILITARY PROFESSIONAL BULLETIN

July–December 2024  
Volume 50, Number 2



## CONTENTS

- 02** **Bridging the Gap in Data Skills**  
by CW2 Jon Delima and CW2 Matt Olrogg
- 06** **Augmenting the Opposing Force with Military Intelligence Mission-Essential Task Training**  
by MSG Taylor Hadden and CSM John Rivera
- 10** **Intelligence Debriefing: From Terminology Development to Modern Tool**  
by MAJ Tomasz Golebiewski, Polish Armed Forces
- 20** **CHASE-ing Excellence in Collection Operations**  
by LTC John Wildt, SSG John Quinn, SSG Caleb Mazaika, and SSG Zachary Verrastro
- 23** **Innovating in the Gray Space**  
by LTC John Limauro, CPT Madison Hunter, and CPT Charlson Ro
- 29** **Closing the Gap Between Hobby and Professional Wargaming**  
by CPT Christopher Schwenck
- 35** **Overcoming Obstacles to Cyberspace Threat Intelligence**  
by CW2 Travis Whitesel, and Mr. Joseph Rudell
- 40** **Get Your Red Pen Ready**  
by LTC Matthew Fontaine
- 54** **The Moral Imperative of Our Time— by Wayne Michael “Mike” Hall (Book Review)**  
Reviewed by John W. Smith
- 61** **Intelligence Preparation of the Operational Environment in the Subarctic**  
by MAJ Michael Everett
- 66** **Integrating Space Domain Considerations into Intelligence Preparation of the Operational Environment**  
by LTC Matthew Fontaine

# BRIDGING THE GAP IN DATA SKILLS

by Chief Warrant Officer 2 Jon Delima  
and Chief Warrant Officer 2 Matt Olrogg



*The listing of products and services in this article does not imply any endorsement by the U.S. Army, the U.S. Army Intelligence Center of Excellence, or any U.S. government agency.*

## Introduction

Rapidly evolving information technology exacerbates commanders' uncertainty while they prepare for large-scale combat operations. Data overload is now pervasive as the Army has shifted its operating concept from unified land operations to multidomain operations. Intelligence professionals across all echelons must extrapolate a staggering amount of data from operational environments consisting of five domains (land, maritime, air, space, and cyberspace) and three dimensions (physical, information, and human). Despite this vast amount of data, the task for intelligence professionals remains unchanged: they must strive to understand and visualize the operational environment, regardless of the requisite data literacy skills.

The requirement to keep pace with ever-changing technology has resulted in a skills gap that degrades organizations' abilities to conduct analysis successfully.<sup>1</sup> Incorporating data literacy into organizational culture and operational training can minimize the gap for both Soldiers and analysts. Advancements in technology continue to bring new capabilities and materiel solutions for tackling data, but Soldiers require foundational knowledge to employ these tools appropriately and to their full potential.

In early 2022, the 1<sup>st</sup> Brigade Combat Team (BCT), 10<sup>th</sup> Mountain Division (Light Infantry) deployed to support Combined Joint Task Force—Operation Inherent Resolve. Although the brigade intelligence support element (BISE) was trained in the doctrine and concepts for near-peer threats and traditional counterinsurgency, the BISE analysts were not prepared to sift efficiently through the vast amounts of

data involving multiple state and non-state actors that comprised the adversaries operating in Central Command's area of responsibility.

Big data—"data that contains greater variety, arriving in increasing volumes and with more velocity"<sup>2</sup>—has continued to outpace analysts' ability to ingest information in a modern conflict. Further complicating matters, the BCT was dispersed across four countries, with units using various command and control systems and transport platforms. The BCT, therefore, needed a digital system common to all warfighting functions that was easy to learn and simple to deploy, while simultaneously allowing users to ingest and understand the vast amount of data that drives decision making. One specific area that captures the scope of the challenge is data visualization, which is critical for developing and managing a robust common intelligence picture and common operational picture.

In late 2021, anticipating the complex data environment, the BCT employed personnel and equipment to start a rapid training cycle focused on near-peer, large-scale combat operations. The BCT's intelligence structure and task organization led to strained command relationships and communications challenges between the BISE and the brigade's military intelligence (MI) company. Integrating the BISE's geospatial engineers and the MI company's geospatial intelligence (GEOINT) imagery analysts into one comprehensive GEOINT cell helped mitigate these challenges. The BCT's geospatial engineering technician managed the GEOINT cell's training and personnel development. The simultaneous training of engineers and analysts resulted in a successful Military Intelligence Training Strategy progression that prepared the Soldiers for deployment. This training structure also exposed the BISE to the National Geospatial-Intelligence Agency's Odyssey Program.<sup>3</sup>



## The Odyssey Program: Portal for ArcGIS

The Odyssey Program rapidly delivers GEOINT technology and capabilities to disadvantaged and disconnected users. One of the Odyssey Program's many software applications is Portal for ArcGIS (commonly known as Portal).<sup>4</sup> Although Portal is designed specifically for geospatial data, there were clear opportunities to use its data visualization suite across all the BCT's warfighting functions. This enabled the commander to make data-driven decisions. Portal for ArcGIS allowed users to—

- ◆ Manipulate and visualize geospatial data.
- ◆ Create and share maps and applications across the enterprise, providing subordinate staff with an added toolkit to understand, visualize, and describe the operational environment.
- ◆ Disseminate data and increase continuity during unit transitions and rotations (attributable to Portal's general user interface and cloud-based infrastructure).
- ◆ Access data stored on Portal's databases from any enclave.

**Supporting the Intelligence Warfighting Function.** Portal effectively supported the brigade's ability to create a common intelligence picture and provide a dissemination service. The BISE developed and maintained all-source intelligence and GEOINT dashboards. The following paragraphs detail how the BISE used Portal in support of each of the four intelligence warfighting function tasks, which are described in FM 2-0, *Intelligence*.

*Provide Intelligence Support to Force Generation.*<sup>5</sup> Portal was critical to establishing an intelligence architecture by enabling intelligence reach through rapid dissemination, establishing and maintaining access for users in assigned groups, and acting as the primary intelligence database for analytic production.

*Provide Support to Situational Understanding.*<sup>6</sup> Portal dashboards were essential to performing situation development by providing current intelligence through significant activity roll-ups, providing threat locations by geospatially depicting the ground order of battle, and developing indicators of threat intentions through data-driven trend analysis.

*Conduct Information Collection.*<sup>7</sup> Portal dashboards were vital to collection management, serving as the primary location to host all collection management tools. Internal and external organizations could easily access daily information collection synchronization matrices, information collection overlays, feature classes in named areas of interest, end-of-mission products, and imagery interpretation reports.

*Provide Intelligence Support to Targeting.*<sup>8</sup> Portal was crucial to providing intelligence support to targeting, directly supporting the fires, public affairs, and cyberspace electromagnetic activities (CEMA) sections. Portal provided a single repository

of structured intelligence data that allowed these sections to query and conduct further analysis to support targeting operations for lethal and nonlethal effects.

**Supporting Other Warfighting Functions.** Other warfighting functions within the BCT utilized Portal in a way comparable to that of the intelligence enterprise. Sections were tasked with maintaining running estimates on individual dashboards as an alternative to traditional, unstructured methods and products. Dynamic running estimates provided the brigade commander with transparency and continuous updates without necessarily relying on scheduled battle update briefs or synchronization meetings. Portal served as the primary means of command and control and provided a single system where all warfighting functions could effectively integrate across echelons.

*Movement and Maneuver.* The operations section maintained a dashboard that projected friendly forces and displayed future operations. Additionally, the operations dashboard hosted the concept of operations products, significant event storyboards, and operation orders, which adjacent, subordinate, and higher echelons could access.

*Fires.* The fires section maintained a dashboard that visualized the location, readiness status, and range of critical fires support systems throughout the area of operations. Pre-approved contingency target locations were also depicted on the dashboard, which assisted in deconflicting operations with internal and external organizations.

*Sustainment.* The sustainment section developed three distinct dashboards containing logistics, resource management, and medical operations estimates. The logistics dashboard detailed the locations of all sustainment nodes in the theater, the status of ground lines of communication, and the maintenance readiness statuses of critical assets. Resource management tracked each subordinate unit's expenditures and current operational needs statements funded or processed. Medical operations depicted all medical facilities categorized by roles, medical evacuation air asset locations, and disease and non-battle injury trend analysis based on geographic location.

*Protection.* The protection section established three dashboards, providing estimates of the brigade's engineer, CEMA section, and air and missile defense cell. The engineer dashboard displayed completed, ongoing, and future projects. The CEMA section used its dashboard to depict electromagnetic warfare equipment's readiness status and geographically display electromagnetic interference densities. The air and missile defense cell visualized the location, readiness status, and range of critical counter-unmanned aircraft systems throughout the area of operations. Additionally, the air and missile defense cell's dashboard hosted the brigade's counter-unmanned aircraft systems battle drills and tactics, techniques, and procedures, providing an accessible repository for all outstations and their base defense operations centers.

## Operational Impact

When asked how the single common digital system impacted operations, COL Brian Ducote, Commander, 1<sup>st</sup> Brigade Combat Team, 10<sup>th</sup> Mountain Division (Light Infantry) stated:

*By employing Portal's digital dashboards, our organization fundamentally transformed how we effectively visualized, described, and directed operations. Each warfighting function's digital running estimates were maintained on Portal, allowing primary staff officers to tailor a variety of data sources and display what was important in a manner that best resonated with end users. The level of ownership, accuracy, and relevancy of the information drastically increased through this methodology [and] greatly enabled my decisions. As opposed to outdated and redundant information on an antiquated slide, everyone had immediate, real-time access to updated and relevant information. Maintaining this information in one central location enhanced our ability to collect, create, and maintain information to improve our situational understanding of a complex area of operation. Insights gained from the staff's dashboards enabled quick, data-driven decisions, increased candid communication, and resulted in a more synchronized staff.*

## Data Literacy

Using a singular digital platform that can process data and comprehensively encompass all warfighting functions can enhance the Army's ability to generate and apply combat power within an ever-evolving operational environment. However, adopting a data processing platform or application must accompany the foundational knowledge of data skills. Implementing data skills training in the institutional domain will take time. In the operational domain, however, units can begin exposing and training their Soldiers to use data effectively by focusing on data literacy.

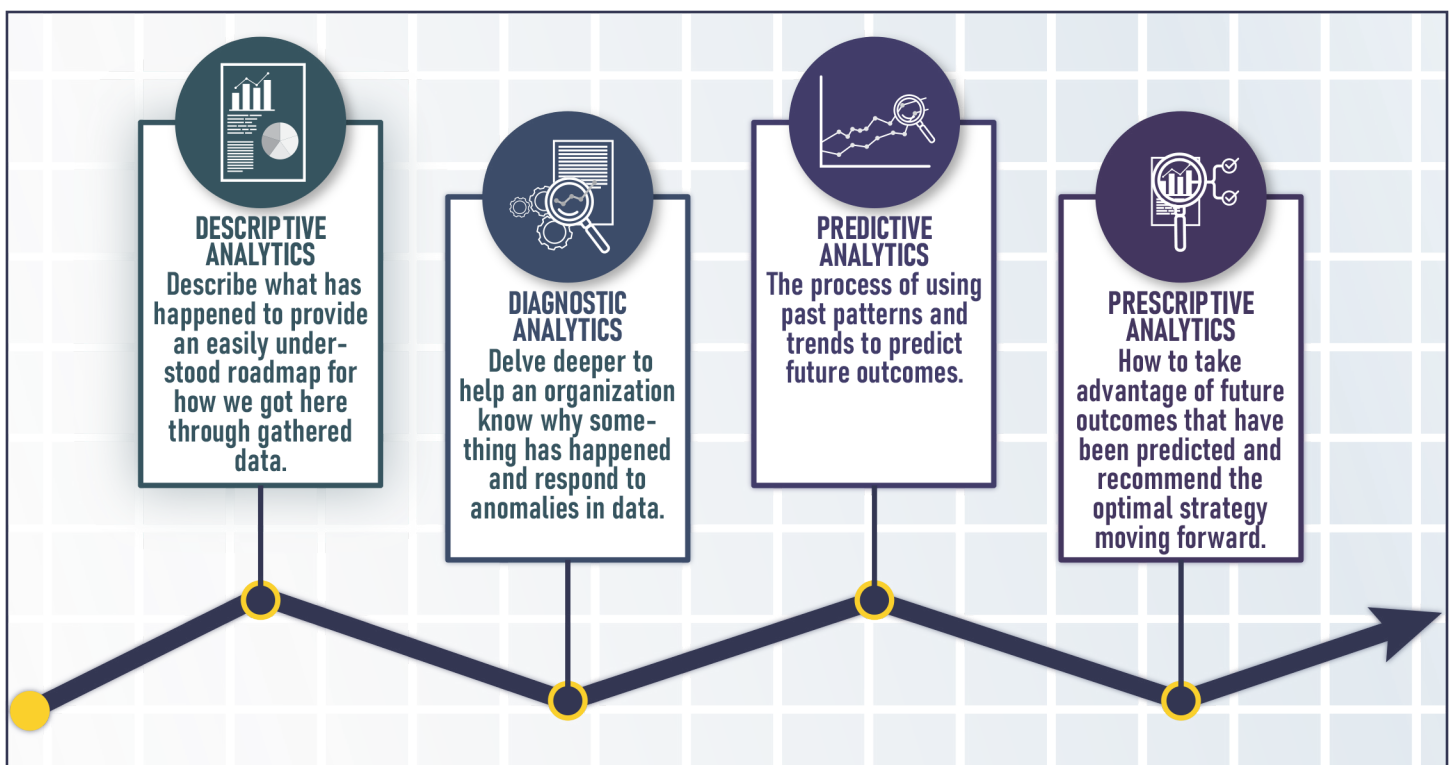
The most common definition of data literacy is “the ability to read, work with, analyze, and argue with data.”<sup>9</sup> In his book, *Be Data Literate*, Jordan Morrow proposes changing *argue* with data to *communicate* with data.<sup>10</sup> Intelligence professionals at all echelons can certainly argue analytic assessments using recognized terms of likelihood. Communicating with data, however, can be an effective method of showing your work when explaining why an assessment has changed from *likely* to *most likely*. Communicating with data can ultimately give analysts and their commanders more confidence in making data-driven decisions.

Jordan Morrow describes four levels of analytics (see figure below):

- ◆ Descriptive.
- ◆ Diagnostic.
- ◆ Predictive.
- ◆ Prescriptive.

Intelligence sections at all echelons perform these four analytic functions. FM 2-0, and ATP 2-33.4, *Intelligence Analysis*, describe similar principles to Morrow's ideas.<sup>11</sup>

**Descriptive.** “Descriptive analytics is the building of reports, dashboards, and observations that help an organization know what has happened...or what is currently happening.”<sup>12</sup> Much of an intelligence section's work falls within this level of analytics. Intelligence summaries, running estimates, and storyboards all contribute to intelligence warfighting task 2.2, Provide Support to Situational Understanding.<sup>13</sup>



Four Levels of Analytics.<sup>14</sup>

**Diagnostic.** “Diagnostic analytics is getting the insight in the data, learning the drivers, and why things happened.”<sup>15</sup> For military intelligence professionals, Morrow’s diagnostic analytics are similar to critical factors analysis, which ATP 2-33.4 describes as a framework to help analysts identify threat critical capabilities, threat critical requirements, and threat critical vulnerabilities along with aiding in identifying threat centers of gravity. This framework helps define why the threat operates a certain way and supports recognizing windows of opportunity and threat vulnerabilities.<sup>16</sup>

**Predictive.** Morrow’s idea of predictive analysis is synonymous with that found in Army military intelligence. Still, Morrow goes further and identifies one common trend within military intelligence organizations: analysts are often stuck at descriptive analysis and never get to a predictive level.<sup>17</sup> Analysts frequently spend a good amount of time creating a visually appealing product and only contribute one to two sentences of predictive analysis.

**Prescriptive.** “Prescriptive analytics is where the technology itself is telling the organization what to do.”<sup>18</sup> With the arrival of artificial intelligence and machine learning technologies, the Army is trending toward fielding programs that are prescriptive solutions. While algorithms can certainly aid the analytic effort, intelligence analysts will still need a solid foundation in all levels of analytics to assess our machine counterparts’ efforts critically.<sup>19</sup>

Becoming data literate without confusing one’s audience with technical jargon is difficult. The issue calls for a deep understanding of current doctrine and policy. Future revisions should embrace the common language used in the larger data community and the ever-evolving technology. Applying academic data literacy concepts to doctrine and training will decrease the data skills gap and help the intelligence community and the Army stay on top of modern problems such as big data. For the intelligence community, familiarizing analysts with these concepts can help build solid foundations for analytic production. Basic analytic techniques, such as sorting and building chronologies, are the cornerstones that drive prescriptive analysis. Advanced analytic techniques, such as high-impact, low-probability analysis and red hat/red team analysis, can help generate predictive analysis and develop more robust likely courses of action.

## Conclusion

FM 3-0, *Operations*, states, “Knowledge of the operational environment is the precursor to effective action.... Information collected from multiple sources and analyzed becomes intelligence that answers commanders’ intelligence requirements.”<sup>20</sup> With the advent of big data, the modern warfighter will need to expand their technical abilities to ingest and analyze data. The internet of things concept, described as “the collective network of connected devices and the technology that facilitates communication between devices and the cloud, as

well as between the devices themselves,”<sup>21</sup> will apply in modern conflicts fought with developing technologies. To maintain the tactical advantage, Soldiers must increase their data skills and leverage those skills in complex and dispersed battlespaces. ✨

## Endnotes

1. Jordan Morrow, *Be Data Literate: The Data Literacy Skills Everyone Needs to Succeed*, 1<sup>st</sup> ed. (London: Kogan Page, 2021), 9.
2. Sherry Tiao, “What is Big Data,” Oracle Cloud Infrastructure, Oracle, March 11, 2024, <https://www.oracle.com/big-data/what-is-big-data/>.
3. National Geospatial-Intelligence Agency, *Odyssey: Edge-Accessible GEOINT Data Tools*, 2022, [https://www.nga.mil/assets/files/Odyssey\\_Slicksheet.pdf](https://www.nga.mil/assets/files/Odyssey_Slicksheet.pdf).
4. Portal for ArcGIS is a software technology component that is the exclusive property of Environmental Systems Research Institute, Inc. (Esri).
5. Department of the Army, Field Manual (FM) 2-0, *Intelligence* (Washington, DC: U.S. Government Publishing Office [GPO], 1 October 2023), B-1–B-5.
6. *Ibid.*, B-5–B-15.
7. *Ibid.*, B-15–B-20.
8. *Ibid.*, B-21–B-24.
9. Rahul Bhargava et al., “Data Murals: Using the Arts to Build Data Literacy,” *The Journal of Community Informatics* 12, No.3 (2016): 197-216, <https://doi.org/10.15353/joci.v12i3.3285>.
10. Morrow, *Be Data Literate*, 36.
11. Department of the Army, FM 2-0, *Intelligence*, 1-4; Department of the Army, “Part Two: Task Techniques” in Army Techniques Publication (ATP) 2-33.4, *Intelligence Analysis* (Washington, DC: U.S. GPO, 10 January 2020), 4-1–6-12.
12. Morrow, *Be Data Literate*, 21.
13. Department of the Army, FM 2-0, *Intelligence*, B-5–B-15.
14. “Explain Descriptive, Diagnostic, Predictive, and Prescriptive Analytics,” April 27, 2023, Learning Innovations Branch, <https://lwntube.army.mil/webapps/imi/libicoe/data-literacy/explain-analytics/>.
15. Morrow, *Be Data Literate*, 24.
16. Department of the Army, ATP 2-33.4, *Intelligence Analysis*, 6-9–6-10.
17. Morrow, *Be Data Literate*, 22.
18. *Ibid.*, 33.
19. Department of the Army, FM 2-0, *Intelligence*, 1-13.
20. Department of the Army, FM 3-0, *Operations* (Washington, DC: U.S. GPO, 1 October 2022), 1-17.
21. “What is IoT (Internet of Things)?” Amazon Web Services, <https://aws.amazon.com/what-is/iot/>.

CW2 Jon Delima is an all-source intelligence observer, coach, and trainer at the Joint Readiness Training Center, Fort Johnson, LA. His previous assignments include brigade intelligence support element chief for 1<sup>st</sup> Brigade Combat Team, 10<sup>th</sup> Mountain Division (Light Infantry); doctrine writer and instructor for the Directorate of Doctrine and Intelligence Systems Training; and battalion S-2 noncommissioned officer in charge for 2<sup>nd</sup> Battalion, 12<sup>th</sup> Infantry Regiment, 2<sup>nd</sup> Stryker Brigade Combat Team, 4<sup>th</sup> Infantry Division. He holds a bachelor’s degree in data analytics and is currently working toward a master’s degree in analytics in computational data.

CW2 Matthew Ologg is an observer, coach, and trainer at the Joint Readiness Training Center, Fort Johnson, LA. His previous assignments include geospatial intelligence (GEOINT) officer in charge for 1<sup>st</sup> Brigade Combat Team, 10<sup>th</sup> Mountain Division (Light Infantry), instructor for the Army GEOINT Battalion and National Geospatial-Intelligence Agency under the GEOINT Career Advancement Program. He holds a bachelor’s degree in geography and is working toward a master’s degree in data science.



# AUGMENTING THE OPPOSING FORCE WITH MILITARY INTELLIGENCE MISSION-ESSENTIAL TASK TRAINING

BY MASTER SERGEANT TAYLOR HADDEN  
& COMMAND SERGEANT MAJOR JOHN RIVERA

## Introduction

Training U.S. Army military intelligence (MI) Soldiers is critical to national security. In our complex, unpredictable, and interconnected world, the role of intelligence Soldiers has never been more crucial. Amid the evolving landscape of military operations, however, and in an era where budgetary constraints, resource limitations, and limited realistic environments are a constant concern, challenges abound in pursuing excellence in MI training. Integrating MI mission-essential task training with the opposing force (OPFOR) during combat training center rotations is an innovative and holistic solution to these challenges.

Historically, intelligence training has often lacked sufficient resources to prepare Soldiers adequately for the complexities of the modern battlefield. Constraints on the level of realism that can be achieved and the physical size of the replicated operational environment limit the effectiveness of any purpose-built training setting.

Scripted scenarios are the primary method of executing MI training. However, accessing or developing realistic training scenarios is only sometimes possible within a unit's organic capability, and developing these scenarios across all collection and analysis disciplines is time-consuming. Organizations such as the Army Foundry Intelligence Training Program offer some relief from this burden via a catalog of off-the-shelf scenarios.

The effectiveness of any of these training scenarios depends on the script's realism. Ideally, scenario developers must have some expertise in the warfighting functions to create an environment that realistically immerses Soldiers in the complexities of military operations. However, it is not feasible for scenario developers to be experts in *all* warfighting functions and have the breadth of experience to generate scripts that effectively replicate these complexities. Additionally, once executed, a scenario's iterative training events become less effective because Soldiers gain knowledge of the environment, actors, and storyline progression. This necessitates the development of multiple scenarios.

As a supplement to scripted scenarios, combat training centers offer a unique opportunity for MI training. Combat training centers already have the resources, realistic environments, and immersive training experiences to replicate convincing scenarios. During combat training center rotations, rotational training units execute the operations process, create and disseminate orders, and provide personnel, weapons, and equipment to support their identified training objectives.

Through integration with the OPFOR, MI Soldiers capitalize on the subject matter expertise of a rotational training unit's planning and execution of operations as the scenario in which they will train, thus replicating the realism necessary for effective training. This reduces the time requirement for external scenario development to zero while leveraging existing training resources. An excellent illustration of this approach is the recent integration of a human intelligence (HUMINT) element with the OPFOR during exercise Saber Junction 2023 at the Joint Multinational Readiness Center (JMRC) in Hohenfels, Germany.

## A Case Study

To assess the effectiveness of integrating MI Soldiers with the OPFOR, we invited a HUMINT platoon to participate as the OPFOR HUMINT during the Saber Junction 2023 exercise. The OPFOR HUMINT comprised an operational management team, which included one human intelligence collection technician and one intelligence officer, plus a HUMINT collection team composed of one noncommissioned officer and two junior enlisted human intelligence collectors. The primary training objective of the OPFOR HUMINT was to complete the MI Training Strategy (MITS) for the brigade combat team tier 3 crew certification. The training tasks focused on interrogation operations and friendly force debriefings.<sup>1</sup> The JMRC exercise procedures allow for the capture of rotational training unit personnel as enemy prisoners of war (EPWs) along with their associated equipment. When captured, the OPFOR holds EPWs at a replicated prisoner-of-war camp for 24 hours. Captured equipment may be retained until the end of the exercise if it is determined to have exploitation value.<sup>2</sup>



### ARTEP to Replace MITS

The Army is re-establishing the Army Training and Evaluation Program (ARTEP) for the operational domain and developing Mission Training Plans (MTPs). ARTEP MTPs focus training units, at echelon, on their mission essential tasks. MTPs are descriptive training products that provide battalions, companies, and platoons a hierarchy of collective training tasks showing leaders what training is needed to achieve mission essential task proficiency. The products will also provide guidance on how to plan, prioritize, and conduct unit training.

Throughout the exercise, the OPFOR HUMINT conducted a range of EPW tasks using the captured rotational training unit personnel, their documents, and their equipment. These tasks included screening, interrogation, intelligence report writing, technical report writing, and basic document and media exploitation. The OPFOR HUMINT also conducted friendly force debriefings with the organic OPFOR personnel.

During the exercise, the OPFOR captured 28 rotational training unit Soldiers ranging in rank from private first class to first lieutenant, incorporating at least 10 military occupational specialties (MOSs), as EPWs. The OPFOR seized various vehicles, communications systems, and paper documents associated with the multiple capturing events. Due to time and personnel constraints, the OPFOR HUMINT conducted 10 interrogations of the possible 28. The OPFOR HUMINT also conducted 5 friendly force debriefings of OPFOR personnel and wrote 6 spot reports (SPOTREPs), 7 intelligence information reports (IIRs), and 10 summary interrogation reports.

### Realism for the Opposing Force

The most valuable insight gathered from this training event was heightened realism. This realism took many forms, including integration with a higher headquarters operational structure, critical thinking for interrogation approach strategies, non-role player EPWs, and the quality and availability of exploitable documents and equipment.

The OPFOR personnel integrated the HUMINT team into all aspects of their operational infrastructure and operations. The OPFOR commander intentionally incorporated the OPFOR HUMINT into all battle rhythm events, including all staff briefings and rehearsals. This exposed the OPFOR HUMINT personnel to the operations process, a training feature usually ignored in scripted scenarios. This was particularly educational for the younger members of the OPFOR HUMINT as, traditionally, scripted scenarios do not consider the organizational structure of a unit's forces.

Immediately following EPW screening after capture events, the OPFOR HUMINT and the OPFOR operations staff conducted ad hoc meetings. These

meetings allowed the OPFOR HUMINT to immediately identify the OPFOR commander's most current information needs, which influenced the development of the interrogation strategy. Participation in rehearsals allowed the OPFOR HUMINT to develop tailored questioning plans for future friendly force debriefings.

There is an unavoidable element of gaming when conducting this type of training in conjunction with OPFOR integration. The JMRC exercise procedures impose some restrictions on operational methodology that would not otherwise be present during combat operations. Exercise procedures are briefed to rotational training units and are available for reference throughout the exercise. The most acute constraint is the 24-hour time limit imposed on EPW capture.<sup>3</sup> Because this time limit is known to the rotational training unit, the OPFOR HUMINT was limited in the number of iterative interrogations and their execution of interrogation approach strategies available to gain EPW cooperation. To overcome this, the OPFOR HUMINT had to think more critically about approach strategies to reduce gaming of the exercise.

The OPFOR HUMINT Soldiers described diverting from the traditional "easy button" approach strategies usually attempted during scripted training events. This process, which was primarily abandoned, combined the love of family and the futility approaches—a common strategy wherein an interrogator implies that the EPW's cooperation with the interrogator will facilitate a quicker resolution of conflict and hasten their return home.<sup>4</sup> As the exercise progressed, the OPFOR HUMINT was forced to devise approach strategies that focused more on the EPWs. One method included a combination of a hate of comrades approach, which focused on perceived low morale traceable to leadership, and a pride and ego-up approach centered on actions the EPW would

Soldiers from the Human Intelligence Platoon, Delta Company, 54<sup>th</sup> Brigade Engineer Battalion, 173<sup>rd</sup> Infantry Brigade Combat Team (Airborne), wearing the black uniforms and augmenting the opposing forces, interrogate a captured 2<sup>nd</sup> Cavalry Regiment Soldier during Exercise Saber Junction 2023 at the Joint Multinational Readiness Center, Hohenfels, Germany, September 2023. (U.S. Army photo by SGT Maria Tsukino)



A convoy of U.S. Army Soldiers, playing the role of opposition forces, roll through a training village with various armored vehicles during Saber Junction 23 at the Joint Multinational Readiness Center near Hohenfels, Germany, Sept. 13, 2023. (U.S. Army photo)

have undertaken to prevent capture and successfully execute their mission.<sup>5</sup>

Unlike scripted HUMINT training, the EPWs were not role-players during this training event. The knowledge of any individual EPW was directly associated with their rank, MOS, experience level, and duty position. The EPWs understanding of the rotational training unit's operations and the quality of information they received from respective headquarters or commanders also affected their knowledge level. The OPFOR HUMINT noted that the type of information these EPWs possessed was different from that experienced training with scripted role players. This reflects a need for scripted EPWs to have increased knowledge of future operational activities, technical equipment specifications, operational tactics, and operations intentions.

Because the EPWs were subject matter experts in their fields, the availability of detailed follow-up information far exceeded any scripted role. This was both an advantage and a disadvantage. Data collected through follow-up questions provided nuanced and specific information required by the OPFOR. It also allowed the interrogator to lose time pursuing immaterial information. However, the OPFOR HUMINT indicated the utility of the follow-up questioning for rapport building.

In scripted scenarios, captured documents and equipment are rare additions to HUMINT roles. The quantity and availability of captured documents and equipment in this unscripted environment, however, provided an added layer of realism for the OPFOR HUMINT, who used these seized items as control measures to identify truthfulness and accuracy, validate analytical assessments, and provide additional actionable intelligence. In at least one instance, the OPFOR HUMINT conducted part of an interrogation inside a captured vehicle using the Joint Battle Command-Platform's blue force tracking capability as the centerpiece of the collection effort.

### Utility to the Opposing Force

At JMRC, the OPFOR is a battalion-sized element replicating a brigade-sized enemy. The JMRC OPFOR has a minimal number of personnel composing their intelligence warfighting function, consisting of reconnaissance Soldiers, electronic warfare, virtual-only unmanned aircraft systems, and intelligence analysts. The OPFOR has no permanently assigned Soldiers with MI *collection* MOSs.



The integration of the OPFOR HUMINT significantly increased the OPFOR's warfighting capability, which enhanced the OPFOR Soldiers' training objectives. Typically, the five permanently assigned all-source intelligence analysts process and exploit the OPFOR-captured personnel and equipment. These analysts conduct tactical questioning of EPWs and screen captured documents and equipment on a time-available basis, which has limited success. Incorporating the OPFOR HUMINT alleviated these requirements, allowing the all-source intelligence analysts to focus on analytical assessments. The OPFOR HUMINT's SPOTREPs and IIRs led the OPFOR all-source intelligence analysts to practice fusing single-source HUMINT streams into their analytical assessments. Additionally, the OPFOR HUMINT provided an extra workforce to screen and process captured enemy documents and equipment, which led to more analytically robust evaluations.

The OPFOR used information gleaned from SPOTREPs, IIRs, and exploitation of captured documents and equipment in several ways. Future intentions confirmed analytical assessments, allowing modification of maneuver operations. Disposition information tipped and cued follow-on operations, including reconnaissance and fires. Interestingly, discussions between the OPFOR staff and the OPFOR HUMINT compelled the OPFOR leadership to reevaluate intelligence priorities and reexamine their targeting strategy.

### Logistics and Finance

The OPFOR integration proved to be a highly cost-effective method of training. The only training costs for the HUMINT Soldiers were the temporary duty expenses covering transportation to JMRC and meals and incidentals. The total cost to the government for the entire team was approximately \$6000. The HUMINT platoon integrated with the OPFOR and provided their own specialized equipment, which only included government computers with the essential operational



document templates needed for intelligence reporting. The OPFOR provided a workspace for report writing, an area for conducting interrogations, maps, radios, and the OPFOR uniforms. The JMRC provided billeting for the duration of the exercise.

## Opposing Force Augmentation as a Vehicle for MI Training Strategy Certification


The integration of OPFOR elements to achieve MITS certification posed several challenges that highlight the need for a more creative approach to the evaluation process. While the OPFOR HUMINT did achieve tier 3 MITS certification through this training event, this strategy has significant drawbacks. Although well-defined, the conventional performance step-based standards model used for MITS evaluation may align differently with the spontaneous and ever-changing scenarios encountered at a combat training center. For example, assessing the “Conduct Map Tracking” performance step depended on specific conditions, such as the EPW’s cooperation and knowledge of unit dispositions, which may not occur during an exercise.<sup>6</sup> Furthermore, procedural lapses by the OPFOR personnel—for example, not creating adequate capture tags or not documenting the chain of custody for enemy materials beyond the JMRC exercise requirements—hindered the evaluation process, particularly regarding the “Initial Examination of Records and Materials” step.<sup>7</sup>

The presence of MITS evaluators had unintended consequences during interrogations. Instead of focusing solely on extracting intelligence based on the EPW’s cooperation, knowledge, and attitude, the interrogators were preoccupied with adhering to the MITS performance step criteria. One OPFOR HUMINT Soldier likened this disruption to “trying to qualify on your weapon in the middle of a firefight.”

Moreover, the presence of MITS evaluators led to confusion among the EPWs, with some mistaking them for the JMRC observer, coach, and trainers responsible for assessing adherence to the code of conduct within the rotational training unit. This misunderstanding likely influenced the EPWs’ behavior during interrogations, which diverged from their expected participation had the MITS evaluators been absent.

Given the limited time available for exercises at a combat training center, it is improbable that an OPFOR HUMINT element could certify on all MITS tables without disrupting the flow of intelligence collection and the realism of the training environment. The sheer number of performance steps and OPFOR HUMINT personnel requiring evaluation would monopolize the available time, especially considering the dynamic and unpredictable nature of OPFOR operations and the availability of intelligence sources. Therefore, there is a pressing need to explore alternative evaluation approaches that balance certification requirements with practical training and realistic scenarios.

## Conclusion

Conducting MI training through OPFOR augmentation during Saber Junction 2023 was a significant success. The simplicity and cost-effective nature of this training strategy is transferable to all MI occupational specialties. This method is scalable to incorporate individual, crew, or platoon-sized assets. It is infinitely modifiable to fit the training needs of MI Soldiers and the intelligence augmentation requirements of the OPFOR. The strategy is easily transferable to other combat training centers and any training event using a dedicated OPFOR element. The JMRC intends to continue MI augmentation of with the OPFOR, including electronic warfare, signals intelligence, unmanned aircraft systems, geospatial intelligence, all-source intelligence analysis, and subsequent HUMINT teams. 

## Endnotes

1. Department of the Army, Training Circular 2-19.403, *Military Intelligence Training Strategy for the Brigade Combat Team Tier 3* (Washington, DC: Government Publishing Office [GPO], 25 February 2020).
2. Seventh Army Training Command, *2023 Exercise Procedures*, ver.23.0 (Hohenfels, Germany: Joint Multinational Readiness Center, 2023).
3. Ibid.
4. Department of the Army, Field Manual 2-22.3, *Human Intelligence Collector Operations* (Washington, DC: GPO, 6 September 2006) 8-9, 8-13.
5. Ibid., 8-10, 8-12.
6. Ibid., 9-4.
7. Ibid., 6-5, D-2.

## References

- 173<sup>rd</sup> Infantry Brigade Combat Team (Airborne). *Exercise Summary HUMINT Support to JMRC OPFOR for Saber Junction 2023 Friendly Forces Debriefing and Interrogation Operations* [EXSUM]. 2023.
- Hadden, Taylor. “LTC Huff (Warrior 6) and CSM Lothspeich (Warrior 7) Interview.” In *Exercise Summary HUMINT Support to JMRC OPFOR*.
- Hadden, Taylor. “OPFOR HUMINT Soldier Interviews.” In *Exercise Summary HUMINT Support to JMRC OPFOR*.
- Hadden, Taylor. “SFC Shin interview, MITS Evaluator.” In *Exercise Summary HUMINT Support to JMRC OPFOR*.

MSG Taylor Hadden is a senior intelligence sergeant who serves as an operations observer, coach, and trainer at the Joint Multinational Readiness Center, Hohenfels, Germany. He previously served as an instructor for the Human Intelligence (HUMINT) Advanced Leader Course and the HUMINT Advanced Individual Training Course at the U.S. Army Intelligence Center of Excellence in Fort Huachuca, AZ.

CSM John Rivera is the Command Sergeant Major for the 743<sup>rd</sup> Military Intelligence (MI) Battalion, 704<sup>th</sup> MI Brigade, Buckley Airforce Base, CO. He previously served as the senior intelligence sergeant major at the Joint Multinational Readiness Center, Hohenfels, Germany and as the Deputy Commandant at the Noncommissioned Officer Academy, U.S. Army Intelligence Center of Excellence in Fort Huachuca, AZ.

# Intelligence Debriefing: From Terminology Development to Modern Tool

by Major Tomasz Golebiewski, Polish Armed Forces

## Introduction

Debriefing is a structured review process commonly used in the military, healthcare, academic, and even business domains to extract or reveal specific information from individuals based on past events. The debriefing techniques and the source's intentions may influence the information collected by intelligence personnel. Thus, the structure and format of any debriefing depends on its intended objective.

In considering the military applications of the debriefing process, we must acknowledge its historical background. In the early days of World War II, U.S. Army Brigadier General and historian Samuel Lynn Atwood Marshall was tasked with documenting combat events. Reconstructing events solely from historical data was difficult, so the designated collector interviewed Soldiers who took part in the battles. This offered an excellent opportunity to gather critical information and assess mission results. After action debriefing became a standard course of action when the intelligence gathered from these interviews proved beneficial to future warfighting strategy.<sup>1</sup>

## Terminology Development

An introduction to debriefing terminology is necessary to understand its meaning in context with its implementation goals. This overview offers a broad perspective of the terminology's development and influence on our understanding of debriefing techniques. The definitions presented here provide a general understanding of debriefing terminology and the recognition of debriefing as an adapted human intelligence (HUMINT) technique.

Intelligence-related military literature from the last century defined debriefing as "questioning of individuals who are sources of information in a strategic or operational environment. This is done to obtain usable information in response to command and national level intelligence needs."<sup>2</sup> While this definition presented the general aim and subject of debriefing, it simultaneously raised other considerations for military intelligence personnel and compelled a more detailed description. The definition was supplemented by identifying debriefing subjects: "The primary categories of sources for debriefing are military personnel (such as patrols), personnel who have been in contact with HN [host nation] personnel, business people who may have worked in the areas of interest (AOIs), and foreign personnel such as refugees and local inhabitants."<sup>3</sup>

In a 2005 Directive, the Department of Defense expanded the debriefing discussion to define debriefing as "the process of questioning cooperating human sources to satisfy intelligence requirements, consistent with applicable law. A source may or may not be in custody. His or her willingness to cooperate need not be immediate or constant. The debriefer may continue to ask questions until it is clear to the debriefer that the person is not willing to volunteer information or respond to questioning."<sup>4</sup> For the first time, a definition introduced debriefing sources as willing subjects. This was a breakthrough in the perception of debriefing as an effective tool for gathering intelligence, as practitioners realized the importance of cooperation and consent. Subsequently, socio-psychological considerations began to play a vital role in the conduct of debriefing, which contributed to developing



specific techniques that strengthened the effectiveness of debriefing methods. This added a new dimension to the evolving definition of debriefing, to include the “systematic questioning of individuals to procure information to answer specific collection requirements by direct and indirect questioning techniques.”<sup>5</sup> Supporting explanations such as “systematically covering topics and areas with a voluntary source who consents to a formal interview”<sup>6</sup> and “the process of using direct questions to elicit intelligence information from a cooperative detainee to satisfy intelligence requirements”<sup>7</sup> amplified the evolving definition. The military intelligence community further identified primary source categories such as friendly forces and civilians, “including refugees, displaced persons (DPs), third-country nationals, and local inhabitants.”<sup>8</sup>

Collaboration between the source and the collector is a fundamental element of debriefing. It allows decision-makers to decide whether the source’s personal situation may influence their willingness to cooperate. “Typically, refugee sources do not require immediate extraction of intelligence. Later on, these sources may be willing to contribute information. This may be due to the personal situation which may include being in custody or detained.”<sup>9</sup> The search for suitable and cooperative sources drove the development of human source operations activities. From this point, practitioners started recognizing debriefing as a sophisticated process organized in a formal, planned manner.

While this approach to information sources improved the chances of obtaining accurate and required information regarding the adversary’s attitude and intentions, it necessitated employing only trained, educated, and certified personnel.<sup>10</sup> Moreover, the responsibility for developing a positive relationship with the source and creating a friendly atmosphere became the collector’s primary responsibility. Collectors had greater flexibility in scheduling meetings with the source, considering the time and place of arranged meetings from the source’s perspective<sup>11</sup> to “maximize the quality and quantity of information obtained.”<sup>12</sup>

Because debriefing often gathered information from Soldiers after missions, it provided opportunities to develop future courses of action and reduce mistakes. It also allowed practitioners to employ the more positive aspects of their missions, which became recommendations and standards. This approach and its benefits carried over into the civilian sphere, with applications in education, business, and healthcare. From this perspective, debriefing was perceived as “a discrete moment in the qualitative data collection process where a research manager sits with a data collector (or data collection team) to discuss the tenor, flow, and resulting findings from a recently undertaken data collection activity”<sup>13</sup> and “focused conversations usually led by a facilitator (‘debriefers’) with learners (‘debriefees’) that typically occur directly following

a simulation experience to reflect on aspects of the simulation, exploring and addressing learner’s needs.”<sup>14</sup>

These definitions appear compatible with military goals and highlight the importance of the data collection process. Moreover, immediate action is fundamental to preventing data collection delays and degraded data quality. Similar to the military approach, Roxanne Gardner noted in her 2013 paper that “debriefing provides opportunities for exploring and making sense of what happened during an event or experience, discussing what went well and identifying what could be done to change, improve and do differently or better next time.”<sup>15</sup> This approach includes the collection process and data analysis, similar to an after action review. Many civilian domains are trying to build their debriefing models by adapting military lessons learned collection techniques; meanwhile, the military intelligence branch is investigating tactics and techniques to strengthen the effectiveness of intelligence collection. From this perspective, the collector seeks knowledge of specific value from the debriefing.

In his 2016 study “The Value of Debriefing,” William M. Duke proposed two aspects of knowledge: explicit and tacit. He noted that explicit knowledge includes data that can be written or stored, while tacit knowledge consists of data kept in the back of peoples’ minds.<sup>16</sup> The availability of tacit knowledge requires added measures and precautions for its exploration. Intelligence use involves employing measures such as an analysis of the approach to the source, cultural considerations, the mental condition of the source, and the availability of trained personnel.

NATO influenced the development of the current, more modern definition of debriefing. As the definition evolved, the historical record in *the Official NATO Terminology Database* introduced debriefing as “the systematic questioning of a willing individual to obtain information of operational or intelligence significance.”<sup>17</sup> During the NATO terminology approval process, however, the intelligence community promoted a more modern definition: “In intelligence usage, the formal and systematic questioning of consenting individuals by personnel trained in human intelligence in order to gather information of intelligence value.”<sup>18</sup> This rewording emphasizes the relevance of the intelligence descriptor and expands the previous description of debriefing into a *formal* and systematic process. In April 2023, this more modern definition obtained NATO Agreed status.

## The Cognitive Debriefing Model

In his 2020 study *Human Sources, Managing Confidential Informants*, John Buckley presents a common approach to debriefing. He proposes a modern debriefing style, presented in the following tables. The process is broken into 5 stages, further divided into 22 steps. Each table introduces one of the five stages; the first column reflects the steps included in

the stage, and the second column lists a description of activities and advice to consider for each step. The third column provides supportive advice adapted to HUMINT from civilian domains such as education and healthcare.

**Stage 1.** This stage includes all preparatory activity before the planned meeting with the source. This stage should focus on training HUMINT personnel in social competencies that emphasize adapting to the situation. Collectors' personality traits determine their ability to acquire these necessary social competencies. For example, HUMINT personnel should be

able to correctly interpret the source's statements and behaviors and react with empathy. The ability of collectors to project an appropriate emotional response significantly impacts the scope of their ongoing relationship with the source.

When it comes to physical barriers, collectors should consider the physical arrangement of the meeting place, such as their choice of seats, seating arrangements, and adequate room lighting, as well as other equipment (e.g., furnishings and décor) conducive to a suitable debriefing climate.

Table 1. Stage 1: Prepare and Plan<sup>19</sup>

STEP	DESCRIPTION OF ACTIVITY	ACTIONS AND ADVICE FOR HUMINT COLLECTORS
RELATIONSHIP MANAGEMENT	<ul style="list-style-type: none"> <li>○ Identify the state of the collector/source relationship, including the welfare and productivity perspective.</li> <li>○ Assess the source's current behavior.</li> <li>○ Identify unresolved matters from previous meetings.</li> <li>○ Determine options for dealing with identified problems.</li> <li>○ Decide a future course of action.</li> </ul>	<ul style="list-style-type: none"> <li>○ Assess the collector's expertise and familiarity with conducting experience-based debriefing activities.<sup>20</sup></li> <li>○ Consider factors that can influence engagement in the activity.<sup>21</sup></li> <li>○ Study the source by analyzing and learning about their behavior patterns, level of access, any previous contacts, interests, occupations, etc.<sup>22</sup></li> <li>○ Address preliminary considerations adequately so they do not hinder or prevent the source's full participation in the debrief, regardless of how well planned.<sup>23</sup></li> <li>○ Consider a source's developmental needs and characteristics. In keeping with the tenets of developmentally appropriate practice, collectors must be aware of and responsive to their sources' cognitive development, emotional maturity, and life experiences.<sup>24</sup></li> <li>○ Assess your adaptability to the given source.<sup>25</sup></li> </ul>
INTELLIGENCE REQUIREMENT	<ul style="list-style-type: none"> <li>○ Identify the expected information.</li> <li>○ Develop specific questions for the source.</li> </ul>	<ul style="list-style-type: none"> <li>○ Assess the source's knowledge and skills relative to the topic.<sup>26</sup></li> <li>○ Begin with identifying the intended objectives.<sup>27</sup></li> <li>○ Think, "What do I need to know to accomplish the mission?"<sup>28</sup></li> </ul>
EQUIPMENT	<ul style="list-style-type: none"> <li>○ Decide what supportive equipment to take for the meeting.</li> <li>○ Determine meeting expenditures.</li> <li>○ Determine source expenditures.</li> </ul>	<ul style="list-style-type: none"> <li>○ Provide access to the instructions and materials needed.<sup>29</sup></li> <li>○ Consider the physical characteristics and accessibility of the meeting space.<sup>30</sup></li> <li>○ Devise a coherent, achievable plan with the data available.<sup>31</sup></li> </ul>
OPERATIONAL PLAN	<ul style="list-style-type: none"> <li>○ Determine how the source will come into physical contact with the handler.</li> <li>○ Determine where and how the activity will take place.</li> <li>○ Identify defensive surveillance involvement.</li> <li>○ Give the source instructions regarding the time and place of the meeting.</li> <li>○ Confirm the source clearly understands details related to the meeting.</li> </ul>	<ul style="list-style-type: none"> <li>○ Select the specific participatory strategy and plan the activity upon which the debrief will be based.<sup>32</sup></li> <li>○ Create a safe debriefing space. When the source perceives the debriefing place as physically and emotionally secure, they can feel free to participate despite facing difficult and unfamiliar challenges.<sup>33</sup></li> <li>○ Cultivate a positive climate. A positive environment fosters source engagement, encourages cooperation and collaboration, and improves outcomes.<sup>34</sup></li> <li>○ Focus on describing models and attributes of exemplary performance, identifying and elucidating incremental steps that lead to success, and formulating plans for revising one's actions during future activity.<sup>35</sup></li> <li>○ Assess the amount of available time.<sup>36</sup></li> <li>○ Write a draft of reflection and discussion that will guide the source through each debrief phase.<sup>37</sup></li> <li>○ Plan the operation in a detailed, organized manner.<sup>38</sup></li> <li>○ Break plans down into smaller, shorter-range plans.<sup>39</sup></li> </ul>

**Stage 2.** This stage provides substantial guidance for the collector and concentrates on the first minutes of interaction with the source. It includes advice for building rapport with the source, guidance the collector should provide to the source, and an explanation of what collectors should expect from the delivered information.

The ability to interact effectively with another person is critical to productive debriefing. It influences the effectiveness of initiating and maintaining contact, the success of bilateral negotiations, and the final decision to terminate the relationship. Making sources aware that they are completely understood and demonstrating empathy increases the likelihood of building deep trust with the collector.

Table 2. Stage 2: Engagement<sup>40</sup>

STEP	DESCRIPTION OF ACTIVITY	ACTIONS AND ADVICE FOR HUMINT COLLECTORS
ENTRANCE	<ul style="list-style-type: none"> <li>○ Initiate initial physical contact between source and collector.</li> <li>○ Use effective non-verbal communication.</li> <li>○ Think about the manner of greeting.</li> <li>○ Determine who will do what and say what.</li> <li>○ Determine who will sit where and the impact space/proximity will have.</li> <li>○ Plan provisioning of refreshments and ambiance.</li> </ul>	<ul style="list-style-type: none"> <li>○ Personal appearance and demeanor are relevant aspects. The source will also evaluate and judge the collector.<sup>41</sup></li> <li>○ Introduce themselves.<sup>42</sup></li> <li>○ Be polite.<sup>43</sup></li> <li>○ Dress appropriately to the source and the location.<sup>44</sup></li> <li>○ Investing a few minutes to review the qualities of effective cooperation and the expectations for participation in the debriefing will help ensure a positive experience for everyone.<sup>45</sup></li> </ul>
SECURITY	<ul style="list-style-type: none"> <li>○ Be alert from the initial entrance. The primary concern is when contact begins.</li> <li>○ Think about the source's immediate security concerns.</li> <li>○ Focus on factors to regain the source's safety in the event of a detrimental occurrence.</li> <li>○ Maintain awareness of available time for the meeting.</li> <li>○ Plan a valid reason for attending the meeting and provide a rationale for this event.</li> <li>○ Ensure the source has a locked phone.</li> </ul>	<ul style="list-style-type: none"> <li>○ Adapt to different personalities and all types of locations, operational rhythms, and environments.<sup>46</sup></li> <li>○ Tell a credible cover story.<sup>47</sup></li> <li>○ Be alert at all times. Constantly assess the value and veracity of information, the source's behavior, and its influence on the security of the environment where the encounter occurs.<sup>48</sup></li> <li>○ Assure the source that the discussion is confidential.<sup>49</sup></li> </ul>
RELATIONSHIP AND WELFARE	<ul style="list-style-type: none"> <li>○ Build rapport.</li> <li>○ Build source-centric relations.</li> <li>○ Concentrate on the forthcoming tasks and review the conversation, if needed.</li> <li>○ Think about the mood of the source judgment.</li> </ul>	<ul style="list-style-type: none"> <li>○ Tailor the discussion to match the unique parameters or demands of the activity, objectives, and the developmental needs and attributes of the source.<sup>50</sup></li> </ul>
AGENDA	<ul style="list-style-type: none"> <li>○ Determine what information must, should, and could be obtained.</li> <li>○ Execute the intended course of the debrief, including different things planned to debate.</li> <li>○ Avoid topics that cause stress to the source, and postpone if necessary.</li> </ul>	<ul style="list-style-type: none"> <li>○ Meet the goals set for the encounter.<sup>51</sup></li> <li>○ Keep the initiative during the encounter, and avoid irritation or anger if the meeting does not go as expected.<sup>52</sup></li> </ul>
EXPLANATION	<ul style="list-style-type: none"> <li>○ Present a detailed explanation of the interview process.</li> <li>○ Present an explanation of the Reporting Everything technique and its meaning.</li> <li>○ Encourage the source to provide details that lie within their knowledge.</li> <li>○ Use encouraging phrases.</li> <li>○ Illustrate the depth of expected descriptions (i.e., people, events, things).</li> <li>○ Note non-verbal communication exhibited by the source.</li> <li>○ Do not pressure the source. If the source feels pressured to give more complete information, it could damage their self-esteem. (They may be tempted to omit the topic or introduce limited information).</li> </ul>	<ul style="list-style-type: none"> <li>○ Providing the source with basic rules for the debriefing can improve psychological safety and prevent potential problems.<sup>53</sup></li> <li>○ Help the source to develop a rich and detailed, collective understanding of what happened during the event<sup>54</sup>—establish a shared mental model.<sup>55</sup></li> <li>○ Interrogatives such as who, what, when, where, why, and how, also known as the Five Ws and an H, or as journalists' questions, provide a simple framework for generating open-ended discussion prompts.<sup>56</sup></li> <li>○ Introduce the debrief by explaining the overall purpose, how it relates to the objectives and goals of each phase, and how they will be conducted.<sup>57</sup></li> </ul>

During this stage, making a positive first impression on the source is crucial, so the collector should make every effort to appear trustworthy. This requires a wide range of body language skills and the ability to control posture and facial expressions to reflect the source's expectations. The collector must adapt to the source by credibly mirroring the source's body language and manner of speaking; it is also essential to recognize how much feedback the source is willing to accept. Thus, the collector must recognize and interpret the source's habit patterns, behaviors, vocabulary, and even their manner of dress.

In his 2014 *Journal of Neuroscience* article, psychologist J. B. Freeman noted that trust in unknown people is determined subconsciously and instantly based on facial expressions.<sup>58</sup> His research highlights the significance of a collector having a predisposition to perform tasks related to conversations with another human. A high level of interpersonal skills gives the collector a distinct advantage and is based on an awareness and desire to obtain information from the source.

Self-presentation significantly impacts the effectiveness and course of a conversation. First impressions determine the source's initial attitude toward the collector, and maintaining the source's trust guarantees the success of the chosen debriefing strategy. Distrust, however, may cause the source to withdraw and resort to confabulation out of fear for their safety.

It is also important for the collector to ensure that the source tells them everything. The collector should explain the *reporting everything* technique to the source, who should understand that sometimes even trivial information makes sense and is valuable. Even small pieces of information the source provides can affect the operational environment.

**Stage 3.** This stage, which implements socio-psychological aspects and skills, forms the bulk of the debriefing process. Here, collectors use specialized techniques and methods to gather information. The collector should demonstrate conscious action to build trust with the source. They should strive for a situation where the source will enjoy the dialogue and believe they have made the right choice in speaking with the collector. The collector should show interest not only in the content of the conversation but also in the source as a person.

Elicitation, a widely used marketing technique, is a primary aspect of conducting effective debriefing. It consists of extracting criteria about the source's value system and then redirecting the conversation through skillful guidance and stimulation to a specific area of the collector's interest. Selection of the motivational criteria allows the collector to build an information-gathering strategy based on positive knowledge gained during the debriefing and negative values the source manifests. This technique lets the collector keep control of the situation while paving the way for future conversations.

Verbal communication barriers between the collector and the source carry a risk of failure to achieve the desired result. Barriers such as incomprehensible linguistic content, problematic speaking pace, or ambiguous language can present challenges and may distort events described by the source. By using the paraphrasing technique—repeating what the source has just related using different words and phrasing—the collector can confirm that the source's intentions are consistent with their feelings and the way of understanding what they heard. This technique clarifies ambiguous language and confirms whether the information obtained is consistent with the source's original meaning. Paraphrasing also reassures the source that the collector is actively listening, encouraging the source to engage on a deeper level and actively participate in the conversation.

The collector should speak at a pace that allows the source to understand what they are saying. Speaking too slowly or too quickly could disturb the flow of the conversation, negatively affecting not just the conversation itself but the quality of the relationship between the collector and the source. The collector should tailor their mode of speech to the source. Using sophisticated vocabulary may negatively affect the source's self-esteem and could result in a hostile attitude and a desire to break off the relationship. At the same time, the collector must take care to avoid oversimplification—the source may perceive this as condescension, with the same negative outcome.

Depending on the situation, collectors may use different types of listening, such as cognitive, critical, and empathic:

- ◆ Cognitive listening uses systematic, targeted questioning to gain deeper information, explanations, and organization of the content.
- ◆ Critical listening analyzes content, opinions, facts, arguments, and their meaning. In this case, the collector must assess the source's credibility through the criteria of the consistency and logic of the presented facts.
- ◆ Empathic listening views the perceived environment from the source's perspective through understanding and use of shared emotions.

Another important technique is active listening, which includes remembering, understanding, engaging, reacting, exchanging ideas (which also establishes cooperation), effort, time, and the ability to overcome perceived barriers. Barriers to active listening include hearing problems, information overload, running away from the topic, personal biases, intense emotions, noise, and physical, physiological, and psychological conditions. Active listening is the collector's responsibility, and they should demonstrate that by having a positive attitude toward the source, maintaining an open posture, and evincing self-control and patience. Maintaining eye contact,



Table 3. Stage 3: Accounting<sup>59</sup>

STEP	DESCRIPTION OF ACTIVITY	ACTIONS AND ADVICE FOR HUMINT COLLECTORS
<b>CONTEXT REINSTATEMENT</b>	<ul style="list-style-type: none"> <li>Memory recall—debrief the source where the event occurred and under similar circumstances when possible.               <ul style="list-style-type: none"> <li>The source should picture the place of the event as clearly as possible.</li> <li>The source should envision everything that happened at the time of the event.</li> </ul> </li> <li>Allow the source to feel they have control over the topic and manner of discussion.</li> <li>Determine the amount of time sufficient to discuss each event.</li> </ul>	<ul style="list-style-type: none"> <li>Prompt the source to provide an objective account of what happened, their unique point of view, descriptions, and observations regarding other involved parties.<sup>60</sup></li> </ul>
<b>FREE RECALL</b>	<ul style="list-style-type: none"> <li>Allow the source to recount information without interruption.               <ul style="list-style-type: none"> <li>Encourage the source to start where they want.</li> <li>Make no effort to separate the events.</li> </ul> </li> <li>Do not interrupt or interject during the conversation. Inappropriate collector behavior can break the source's concentration and reinforce the undesirable perception of domination.               <ul style="list-style-type: none"> <li>Once a collector interrupts, the source cannot retrieve the same information.</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>Be empathic.<sup>61</sup></li> <li>Be a good listener.<sup>62</sup></li> <li>Read the source's body language and pay attention to the above requirements.<sup>63</sup></li> <li>Give the source time to deal with reactions and emotions.<sup>64</sup></li> </ul>
<b>QUESTIONING</b>	<ul style="list-style-type: none"> <li>Employ non-confrontational methods.</li> <li>Ask subtle rather than blunt questions (poorly structured questions confuse the source and damage their trust).</li> <li>Avoid closed and leading questions.</li> <li>Use open questions that guarantee more accurate and complete answers, encouraging further recall and leading to more specific questions.</li> <li>Ascertain the provenance of information. Clarify how the source obtained the information and how it might influence source perception.</li> <li>Ask all questions relevant to one event at a time. Do not jump from event to event.</li> <li>Collect the known information along with the unknown.</li> </ul>	<ul style="list-style-type: none"> <li>Examine the similarities between the information provided and that which is already known.<sup>65</sup></li> <li>Avoid outbursts or displays of impatience, as these may cause a source to lose respect for the collector and become less willing to convey the information.<sup>66</sup></li> <li>Objectivity may cause unconsciously distorted information analysis and prevent the collector from using questioning techniques effectively.<sup>67</sup></li> <li>Use questions to stimulate reflection and expose the source's thinking processes.<sup>68</sup></li> <li>Incorporate clear objectives into each event.<sup>69</sup></li> <li>Ask open-ended questions to facilitate discussion and foster reflection and self-assessment.<sup>70</sup></li> <li>Be patient after posing questions and use silence effectively as a tool, allowing it to take place as needed. Silence during the debriefing is precious for the participants.<sup>71</sup></li> </ul>
<b>VARIED RETRIEVAL AND CLARIFICATION</b>	<ul style="list-style-type: none"> <li>Use different techniques depending on the context of the debriefing:               <ul style="list-style-type: none"> <li>Perspective change: Let the source retell the event from a different perspective (i.e., view from a different place or another set of eyes).</li> <li>Temporal order change: Let the source tell the story backward from the end, starting from the most salient point.</li> <li>Retrieval prompts: Let the source act out what happened or draw out the location, then collect additional information using the source's sketches as an aid.</li> </ul> </li> <li>Ask the source to consider the five senses (hearing, seeing, smell, taste, and touch). This will help refresh the event details.</li> <li>Let the source imagine what involved persons looked like or how their names sounded. This can draw out more details.</li> <li>Assess gathered details and clarify any anomalies. The collector should take ownership of the lack of clarity to avoid threatening the source.</li> <li>Do not spend too much time on any one specific topic. Doing so allows the source to assess the importance of this knowledge to the collector.</li> <li>A second collector should interject when a piece of missed information is spotted.</li> </ul>	<ul style="list-style-type: none"> <li>Act as a conversational guide and ensure that the relevant issues (e.g., objectives) that occurred during the simulation event or were identified a priori are discussed and that the debriefing conversation flows smoothly and does not go off track.<sup>72</sup></li> <li>Analyze the relationship between the information and skills used during the debriefing content.<sup>73</sup></li> <li>Use higher-order cognitive and critical thinking skills to clarify the lessons learned.<sup>74</sup></li> <li>Draft a timeline describing the events in the order in which they occurred.<sup>75</sup></li> <li>Create a diagram depicting the individuals involved and what each of them did or said.<sup>76</sup></li> <li>Use the circular questions technique to track behavior patterns, generate new information, and foster perspective-taking (relation and description from third person perspective).<sup>77</sup></li> </ul>

Table 3. Stage 3: Accounting (continued)

STEP	DESCRIPTION OF ACTIVITY	ACTIONS AND ADVICE FOR HUMINT COLLECTORS
<b>CONFIRMATION AND COMMENT</b>	<ul style="list-style-type: none"> <li>○ Confirm that the collected facts are understood correctly.</li> <li>○ Inform the source that your narration can be interrupted with any new information or if there are any errors.</li> <li>○ Systematically summarize the details and try to follow each event in order.</li> <li>○ Stop speaking and actively listen if the source interrupts the narration.</li> <li>○ Add commentary to ensure the source understands the facts and feels involved.</li> <li>○ Invite the source to add their opinion. The source has expert knowledge that can be useful from an intelligence perspective.</li> <li>○ Discuss with the source any intelligence requirements not answered by the gathered information, as well as previous tasks or requests.</li> </ul>	<ul style="list-style-type: none"> <li>○ Identify the information provided and compare it to the objectives.<sup>78</sup></li> <li>○ Close the session by summarizing the main points discussed.<sup>79</sup></li> <li>○ Recap the topics addressed in the encounter.<sup>80</sup></li> <li>○ Allow the source to analyze and self-correct the information provided.<sup>81</sup></li> <li>○ Provide the source with feedback to improve future performance.<sup>82</sup></li> </ul>

mirroring the source's non-verbal communication, and discernment in seeking clarification are effective supplements to active listening.

Collectors can use active listening techniques interchangeably to create favorable conditions for obtaining information. These techniques include—

- ◆ Adjusting to the source: maintaining eye contact and offering physical cues such as nodding the head and brief positive vocalizations in response to the source's statements.
- ◆ Comprehension check: confirming with the source that the collector correctly understood the information.
- ◆ Interview: asking the source specific questions to clarify meaning and eliminate confusion.
- ◆ Emotional acceptance: displaying empathy to reassure the source that their feelings are valid.
- ◆ Involvement level of the parties: determining the source's level of investment in the conversation and the likelihood that they will maintain interest.
- ◆ Source testing: using several types of questions (e.g., topical, follow-up, nonpertinent, repeat, and control) to verify the integrity of the source's information.
- ◆ Approbation: offering approval and encouragement of the source's behavior and views.
- ◆ Juxtaposition: asking questions to compare information the source provides against information the collector already knows.
- ◆ Point of the matter: following the key facts of the conversation and returning to them if the conversation strays.

- ◆ Paraphrasing: summarizing what the source has said and repeating it back to them in the collector's own words.
- ◆ Editorial changes to presented facts: making statements containing facts that the source has not provided to reveal inconsistencies and untruths.
- ◆ Alternative: the collector's impartial response to the presented facts and descriptions without consideration for the source's narrative.
- ◆ Counterproposal: presentation of the opposite perspective to force the source to reveal the real reason for their actions.
- ◆ Source impeachment: calling the source's integrity into question in the hope that this will push the source into a defensive posture, thus offering more details to prove their reliability.

Only some of these techniques are desirable from a debriefing perspective; however, depending on the source's behavior they can nevertheless be useful to the collector.

**Stage 4.** Known as the "progression stage," this stage is primarily concerned with source development and focuses on the source's ongoing ability to gather information. Collectors must consider the source's situation as a fundamental influence on their attitude toward information expectations. At this point, the collector and source should address the context of the information the source provides, the collector's feedback on the importance of the information, and the source's efforts to transfer the information. This stage is a suitable time for the collector to advise the source on how they should conduct themselves in the future to maintain safety and create the opportunity to provide information of intelligence value.

Table 4. Stage 4: Progression<sup>83</sup>

STEP	DESCRIPTION OF ACTIVITY	ACTIONS AND ADVICE FOR HUMINT COLLECTORS
CONSULTATION	<ul style="list-style-type: none"> <li>○ Determine what the source could and should do next.</li> <li>○ Maximize information to assess source safety.</li> <li>○ Listen carefully to what the source can or cannot achieve.</li> </ul>	<ul style="list-style-type: none"> <li>○ <i>Co-debriefing</i><sup>84</sup> includes the potential for collectors to complement each other's styles, provide a larger pool of expertise and viewpoints, and cross-monitor and manage source expectations and needs.<sup>85</sup></li> </ul>
TASKING	<ul style="list-style-type: none"> <li>○ Tasking is fundamental to a productive source relationship.</li> <li>○ Ensure the source agrees to the task/request.</li> <li>○ Be clear regarding task priorities.</li> </ul>	
EQUIPMENT	<ul style="list-style-type: none"> <li>○ Equip the source with the necessary skills.</li> <li>○ Train the source in the operational aspects of their role.</li> <li>○ Record training in the contact note.</li> </ul>	
RECOGNITION AND REWARD	<ul style="list-style-type: none"> <li>○ Recognize the value of the source's information and the effort made to obtain it.</li> <li>○ Address the source's motives concerning self-esteem and sense of belonging to a team.</li> <li>○ Discuss rewards or reimbursements.</li> <li>○ Give the source clear information regarding the impact of the information they provided. The source should see the positive aspects of their efforts.</li> </ul>	<ul style="list-style-type: none"> <li>○ Emphasize that all contributions to the discussion, no matter how small or from whom, are beneficial and contribute to the collective understanding of what happened and what it might mean.<sup>86</sup></li> <li>○ Articulate complex situations and concepts, behave believably and consistently, follow through on any promises, and refrain from making promises that cannot be kept.<sup>87</sup></li> </ul>

Table 5. Stage 5: Closure<sup>88</sup>

STEP	DESCRIPTION OF ACTIVITY	ACTIONS AND ADVICE FOR HUMINT COLLECTORS
RAPPORT	<ul style="list-style-type: none"> <li>○ Concentrate on personal and social issues relating to the source.</li> <li>○ Lightening the source mood.</li> <li>○ Show genuine concern for the source's well-being.</li> </ul>	
FUTURE CONTACT	<ul style="list-style-type: none"> <li>○ Offer the source a tentative agreement on when the next meeting will occur.</li> <li>○ Gain agreement from all parties on the next contact.</li> <li>○ Remind the source to get in touch immediately if they encounter sensitive information.</li> </ul>	<ul style="list-style-type: none"> <li>○ Set up a future meeting with the source.<sup>89</sup></li> </ul>
SECURITY	<ul style="list-style-type: none"> <li>○ Comment on any matters related to the source's safety.</li> <li>○ Make sure that the source has no security concerns.</li> </ul>	
EXIT	<ul style="list-style-type: none"> <li>○ Activities should not draw the eyes of a third party.</li> <li>○ Allow the source to leave the location first if the location is a public place.</li> <li>○ Return to the place of work securely.</li> </ul>	

**Stage 5.** In this final stage, which concentrates on report-building details and security measures, the collector ensures that the source is secure following the meeting and that there are no concerns about their pattern of life before the next intelligence activity. Third-party suspicions aimed at the source may also target the collector, which can have a detrimental effect on intelligence operations.

## Conclusion

A hybrid approach to debriefing could positively affect the research and development of modern debriefing tools. The new debriefing model appears more generic in its approach to the source and allows the collector to adapt the most effective tactics and techniques during debriefing. The proposed model should encourage researchers in this direction, especially regarding intelligence applications.

The cognitive debriefing model demonstrates the importance of structured consistency in ongoing HUMINT activity. Moreover, it highlights the complexity of debriefing, which includes organizational and execution aspects. This approach is compatible with the latest terminology and fulfills its core demands.

The model presented here employs soft socio-psychological skills, which are the main pillars of this type of intelligence activity. The intelligence community should implement these skills into the training domain and consider them when recruiting HUMINT personnel. ✨

## Endnotes

1. Roxane Gardner, "Introduction to Debriefing," *Seminars in Perinatology* 37, no. 3 (June 2013): 166-167, <https://doi.org/10.1053/j.semperi.2013.02.008>.
2. Department of the Army, Field Manual (FM) 34-52, *Intelligence Interrogation* (Washington DC: U.S. Government Publishing Office [GPO], 28 September 1992 [obsolete]), 3-31.
3. Department of the Army, Student Text 2-22.7, *Tactical Human Intelligence and Counterintelligence Operations* (Fort Huachuca, AZ: U.S. Army Intelligence Center and Fort Huachuca, April 2002 [obsolete]).
4. Department of Defense (DoD), Directive 3115.09, *DoD Intelligence Interrogations, Detainee Debriefings, and Tactical Questioning* (Washington, DC: GPO, 03 November 2005 [obsolete]), 10.
5. Department of the Army, FM 2-22.3, *Human Intelligence Collector Operations* (Washington DC: GPO, 06 September 2006), Glossary-4.
6. Robert A. Fein, "Introduction," in *Educating Information—Interrogation: Science and Art Foundations for the Future*, Intelligence Science Board Phase 1 Report, ed. Russell Swenson (Washington, DC: National Defense Intelligence College, December 2006), 2.
7. DoD, Directive 3115.09, *DoD Intelligence Interrogations, Detainee Debriefings, and Tactical Questioning* (Washington, DC: GPO, 09 October 2008 [obsolete]), 20.
8. Department of the Army, FM 2-22.3, *Human Intelligence Collector Operations*, 1-4.
9. Keshav Mazumadar, *Actionable Intelligence—Humint-Centric Operations ES2* (Athens, Greece: The Research Institute for European and American Studies, September 2013), 22, ebook, <https://rieas.gr/publications/2026-keshav-mazumadar-actionable-intelligence-humint-centric-operations-es2-rieas-e-book-no5-september-2013>.
10. Ibid.
11. Jordan Nunan et al., "Source Handler Perceptions of the Interviewing Processes Employed with Informants," *Journal of Policing, Intelligence and Counter Terrorism* 15, no. 3 (2020): 244-262, <https://www.tandfonline.com/doi/full/10.1080/18335330.2020.1820069>.
12. John Buckley, *Human Sources: Managing Confidential Informants* (United Kingdom, HSM Publishing, 2020), 183.
13. Shannon A. McMahon and Peter J. Winch, "Systematic Debriefing after Qualitative Encounters: An Essential Analysis Step in Applied Qualitative Research," *BMJ Global Health* 3, no. 5 (2018): 3, <https://gh.bmj.com/content/3/5/e000837>.
14. Janice C. Palaganas et al., "Cultural Considerations in Debriefing: A Systemic Review of the Literature," *BMJ Simulation & Technology Enhanced Learning* 7, no. 6 (2021): 605. <https://doi.org/10.1136/bmjstel-2020-000857>.
15. Gardner, "Introduction to Debriefing," 166.
16. William M. Duke, *The Value of Debriefing* (Atlanta, GA: Afterburner, 2016), 1, [afterburner.com/wp-content/uploads/2017/01/WP-The-Value-of-Debriefing.pdf](https://afterburner.com/wp-content/uploads/2017/01/WP-The-Value-of-Debriefing.pdf).
17. *Official NATO Terminology Database*, <https://nso.nato.int/natoterm/content/nato/pages/home.html?lg=en>.
18. *Official NATO Terminology Database*, s.v. "debriefing," Record 27703, approval date April 17, 2023, <https://nso.nato.int/natoterm/content/nato/pages/home.html?lg=en>.
19. Table based on Buckley, *Human Sources*, 203-206.
20. Judith A. Johns, Matthew T. Moyer, and Lisa M. Gasque, "Planning and Facilitating Debriefs of Experiential Learning Activities in Skills-Based Health Education," *Journal of Health Education Teaching* 8, no. 1: 67, <https://files.eric.ed.gov/fulltext/EJ1163872.pdf>.
21. Ibid., 64.
22. Carlos Miguel Coelho Rosa Marques da Silva, "HUMINT—Conceptualization and Use in Military Operations," *Revista de Ciências Militares* VII, no. 1 (May 2019): 63.
23. Johns, Moyer, and Gasque, "Planning and Facilitating Debriefs," 64.
24. Ibid.
25. Silva, "HUMINT—Conceptualization and Use," 61.
26. Johns, Moyer, and Gasque, "Planning and Facilitating Debriefs," 65.
27. Ibid.
28. Silva, "HUMINT—Conceptualization and Use," 63.
29. Johns, Moyer, and Gasque, "Planning and Facilitating Debriefs," 67.
30. Ibid.
31. Silva, "HUMINT—Conceptualization and Use," 63.
32. Johns, Moyer, and Gasque, "Planning and Facilitating Debriefs," 65.
33. Ibid., 64.
34. Ibid.
35. Ibid., 65.



36. Ibid., 66.
37. Ibid., 67.
38. Silva, "HUMINT–Conceptualization and Use," 63.
39. Duke, "The Value of Debriefing," 5.
40. Table based on Buckley, *Human Sources*, 206-215.
41. Silva, "HUMINT–Conceptualization and Use," 61.
42. Ibid., 64.
43. Ibid.
44. Ibid.
45. Johns, Moyer, and Gasque, "Planning and Facilitating Debriefs," 69.
46. Silva, "HUMINT–Conceptualization and Use," 61.
47. Ibid., 64.
48. Ibid., 60.
49. Sawyer Taylor et al., "More Than One Way to Debrief: A Critical Review of Healthcare Simulation Debriefing Methods," *Simulation in Healthcare: The Journal of the Society for Simulation in Healthcare* 11, no. 3 (June 2016): 213.
50. Johns, Moyer, and Gasque, "Planning and Facilitating Debriefs," 67.
51. Silva, "HUMINT–Conceptualization and Use," 64.
52. Ibid., 61.
53. Sawyer et al., "More Than One Way," 213.
54. Johns, Moyer, and Gasque, "Planning and Facilitating Debriefs," 69.
55. Sawyer et al., "More Than One Way," 213.
56. Johns, Moyer, and Gasque, "Planning and Facilitating Debriefs," 67.
57. Ibid., 69.
58. Jonathan B. Freeman, Ryan M. Stoller, Zachary A. Ingebretsen, and Eric A. Hehman, "Amygdala Responsivity to High-Level Social Information from Unseen Faces," *Journal of Neuroscience* 34, no. 32 (6 August 2014): 10573-10581.
59. Table based on Buckley, *Human Sources*, 215-226.
60. Johns, Moyer, and Gasque, "Planning and Facilitating Debriefs," 67.
61. Silva, "HUMINT–Conceptualization and Use," 64.
62. Ibid.
63. Ibid.
64. Sawyer et al., "More Than One Way," 212.
65. Johns, Moyer, and Gasque, "Planning and Facilitating Debriefs," 70.
66. Ibid.
67. Silva, "HUMINT–Conceptualization and Use," 61.
68. Sawyer et al., "More Than One Way," 212.
69. Ibid., 213.
70. Ibid., 214.
71. Ibid.
72. Ibid., 215.
73. Johns, Moyer, and Gasque, "Planning and Facilitating Debriefs," 67.
74. Ibid., 68.
75. Ibid., 70.
76. Ibid.
77. Sawyer et al., "More Than One Way," 214.
78. Johns, Moyer, and Gasque, "Planning and Facilitating Debriefs," 70.
79. Ibid.
80. Silva, "HUMINT–Conceptualization and Use," 64.
81. Sawyer et al., "More Than One Way," 214.
82. Ibid.
83. Table based on Buckley, *Human Sources*, 226-228.
84. *Co-debriefing* means that more than one collector is involved in a debriefing process. Usually, the debriefing is conducted by a collector and co-collector.
85. Sawyer et al., "More Than One Way," 214.
86. Johns, Moyer, and Gasque, "Planning and Facilitating Debriefs," 69.
87. Silva, "HUMINT–Conceptualization and Use," 60.
88. Table based on Buckley, *Human Sources*, 229-230.
89. Silva, "HUMINT–Conceptualization and Use," 59.

Major Tomasz Golebiewski, PhD, is a staff officer in the Doctrine and Standards Section of the North Atlantic Treaty Organization Human Intelligence (HUMINT) Center of Excellence. He is the former Commandant of the Polish HUMINT Training Centre and a graduate of the War Studies University in Warsaw, Faculty of National Security.

# CHASE-ing Excellence in Collection Operations

by Lieutenant Colonel John Wildt,  
Staff Sergeant John Quinn,  
Staff Sergeant Caleb Mazaika,  
and Staff Sergeant Zachary Verrastro

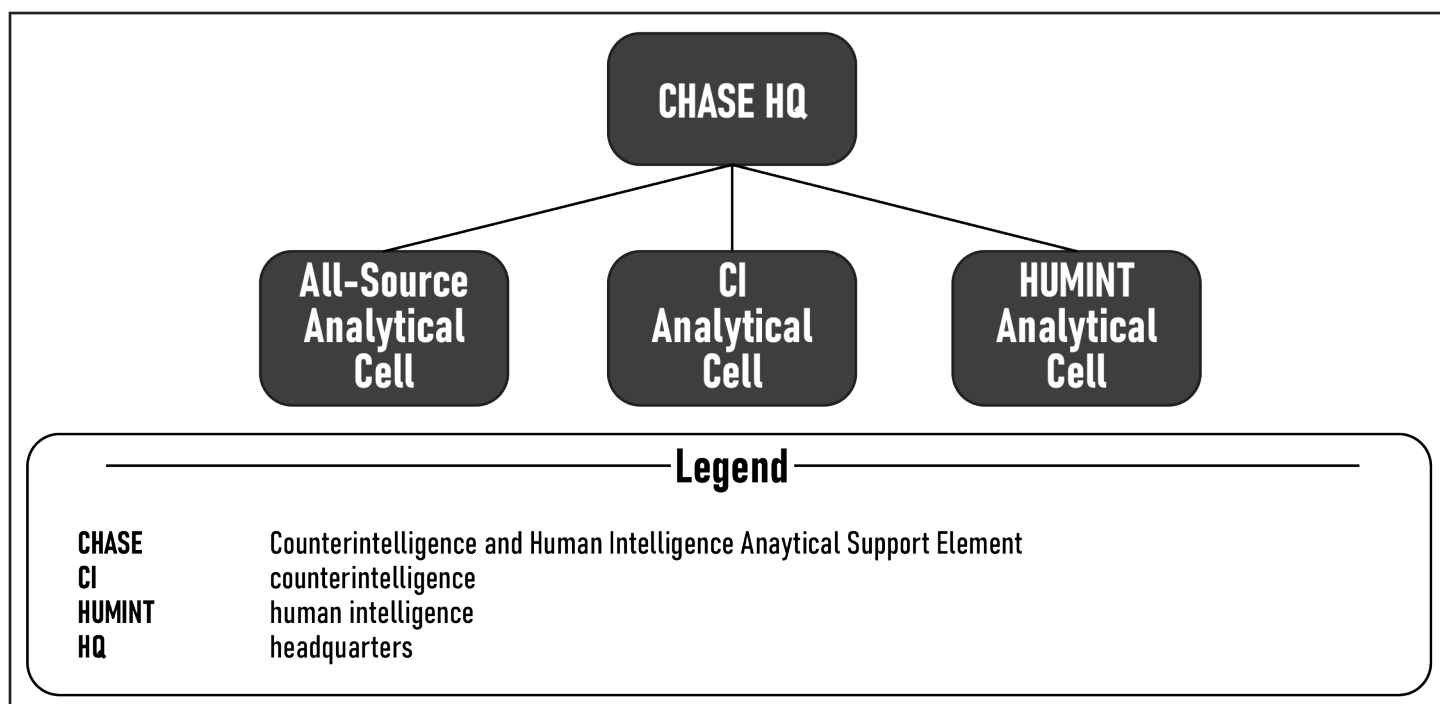
## Introduction

In January 2023, the 207<sup>th</sup> Military Intelligence (MI) Brigade—Theater (MIB—T) task-organized the Counterintelligence (CI) and Human Intelligence (HUMINT) Analysis Cell from the 522<sup>nd</sup> MI Battalion (Operations) to the 307<sup>th</sup> MI Battalion (Forward Collection) to form the CI and HUMINT Analytical Support Element (CHASE). This element provided direct intelligence analysis support to the brigade intelligence collection teams. One year later, this experiment is a success. Individual collectors are better prepared for missions and can answer more priority intelligence requirements for commanders at all levels. The keys to its success are all-source intelligence analysis augmentation and talent management focused on getting the right people into the CHASE. Though the formation of the CHASE created some administrative friction, it also increased the quality of our collector's reporting. We encourage "CHASE-ing excellence" as a best practice for all MIB—Ts.

## Staffing the CHASE

The 207<sup>th</sup> MIB—T's table of organization and equipment places the CI and HUMINT Analysis Cell in the theater Analysis and Control Element (ACE). The cell provides CI and HUMINT support to the U.S. Army Southern European Task Force, Africa. While the theater ACE appreciated the cell's expertise, the brigade leadership believed that the CI and HUMINT Analysis Cell could make a more significant impact by directly supporting collectors. As a small, often undermanned element of collectors not engaged in operations and assigned to the ACE, it was hard for the CI and HUMINT perspectives to gain traction. After moving to the 307<sup>th</sup> MI Battalion (Forward Collection), the CI and HUMINT single-source analytical cells were rechristened as the CHASE. The CHASE is divided into three sections: All-Source Analytic Cell, CI Analytic Cell, and HUMINT Analytic Cell. A noncommissioned officer (NCO) who provides technical expertise and mission guidance leads each section.





CHASE Organizational Structure (figure adapted from authors' original)

The CHASE resides in the Forward Collection Battalion, where it can streamline communication and coordination efforts between intelligence collectors and analysts. The team coalesced and developed an all-hands-on-deck mentality to support collection requirements. The Intelligence Analysts helped the CI Agents and HUMINT Collectors learn how to navigate intelligence community web portals; collectors helped analysts understand the nuances of their operational cycle. Gathering this group of motivated intelligence professionals together in the same space to work on the same mission resulted in outcomes more significant than the sum of the individual inputs. The team could not have achieved these results if the CHASE had not been integrated and collocated.

The 207<sup>th</sup> MIB-T's CI and HUMINT Analysis Cell consisted of CI Agents and HUMINT Collectors who provided CI and HUMINT perspectives to the theater ACE. When these elements transferred as the CHASE to the Forward Collection Battalion, the battalion also task-organized its limited organic Intelligence Analysts to the CHASE. While this removed personnel from the battalion staff, the increased analytic support and all-source intelligence perspective were crucial to the CHASE's ability to provide in-depth analysis. The personnel transfer from the Operations Battalion also included an additional Intelligence Analyst to increase the all-source intelligence support to the CHASE. The inclusion of Intelligence Analysts provides rounded all-source intelligence analysis capabilities to the CHASE that complements the tactical understanding of the CI Agents and HUMINT Collectors. The Intelligence Analysts provide operational coordination between the CHASE and the ACE, ensuring synchronization.

## Managing Talent in the CHASE

Talent management and member selection are essential factors in the CHASE's success, but selecting the right Soldiers for the CHASE is only part of the process. Potential team members must also be at the right juncture in their assignments with the 207<sup>th</sup> MIB-T to maximize their skills and understanding. Junior Soldiers generally serve 6 to 12 months in the CHASE, while NCOs in leadership positions typically serve 12 to 18 months.

An Intelligence Analyst candidate for the CHASE should already be working in the 207<sup>th</sup> MIB-T ACE as a regional analyst or in the deployable intelligence support element. This placement gives analysts a basic understanding of all-source intelligence production, theater requirements, and operational and tactical intelligence. Following their time in the CHASE, these analysts may return to the ACE to refine and develop operational- and strategic-level intelligence production. Alternatively, they can move on a permanent change of station to follow-on assignments, bringing their new skillsets to further improve the intelligence community.

CI Agents and HUMINT Collectors coming to the CHASE have more flexibility because they generally serve their entire tour in the Forward Collection Battalion. We usually assign junior CI Agents and HUMINT Collectors to home station platforms before templating them for deployment. After a deployment, these CI Agents and HUMINT Collectors move to the CHASE to reset their dwell period, support currently deployed collectors, and develop their analytic skills to improve future collection efforts. After their CHASE assignment, they return to the collection companies to serve as team leaders, sharing their experiences with their teams and improving future collection efforts.



## Overcoming CHASE Challenges


Though moving the CHASE to the Forward Collection Battalion has been successful, there are challenges to overcome. Our primary operational challenge is maintaining continuous ties with the ACE to ensure that the ACE receives CI and HUMINT support and that the CHASE's work is fully integrated into the analytical process. We mitigated this challenge by working closely with the CI and HUMINT staff element (G-2X) to ensure the CHASE fully supports the G-2's collection priorities. We also embedded G-2X personnel inside the CHASE and are working toward increased integration of CHASE leadership into the ACE and G-2X battle rhythms.

The main administrative challenge has been managing CHASE personnel assigned to the Operations Battalion while working in the Forward Collection Battalion. We have not yet found a systemic solution, but commanders at the company, detachment, and battalion levels constantly communicate to mitigate administrative issues.

## Conclusion

The CHASE was originally realigned to increase support to intelligence collectors; as we pass the one-year mark, it has succeeded in that mission. The CHASE has successfully provided tailored and timely intelligence support to the current collection platforms both forward and at home station. After establishing steady-state support for current operations, the CHASE uses the successful practices developed over the last year to shift its priority focus toward future operations. Task-organizing Intelligence Analysts and carefully managing

the assignment of personnel to the CHASE ensured that we had the right Soldiers to test this concept. As we move into the second year with the CHASE in the Forward Collection Battalion, our priorities are maintaining strong ties with the theater ACE and preserving the CHASE's standard operating procedures.

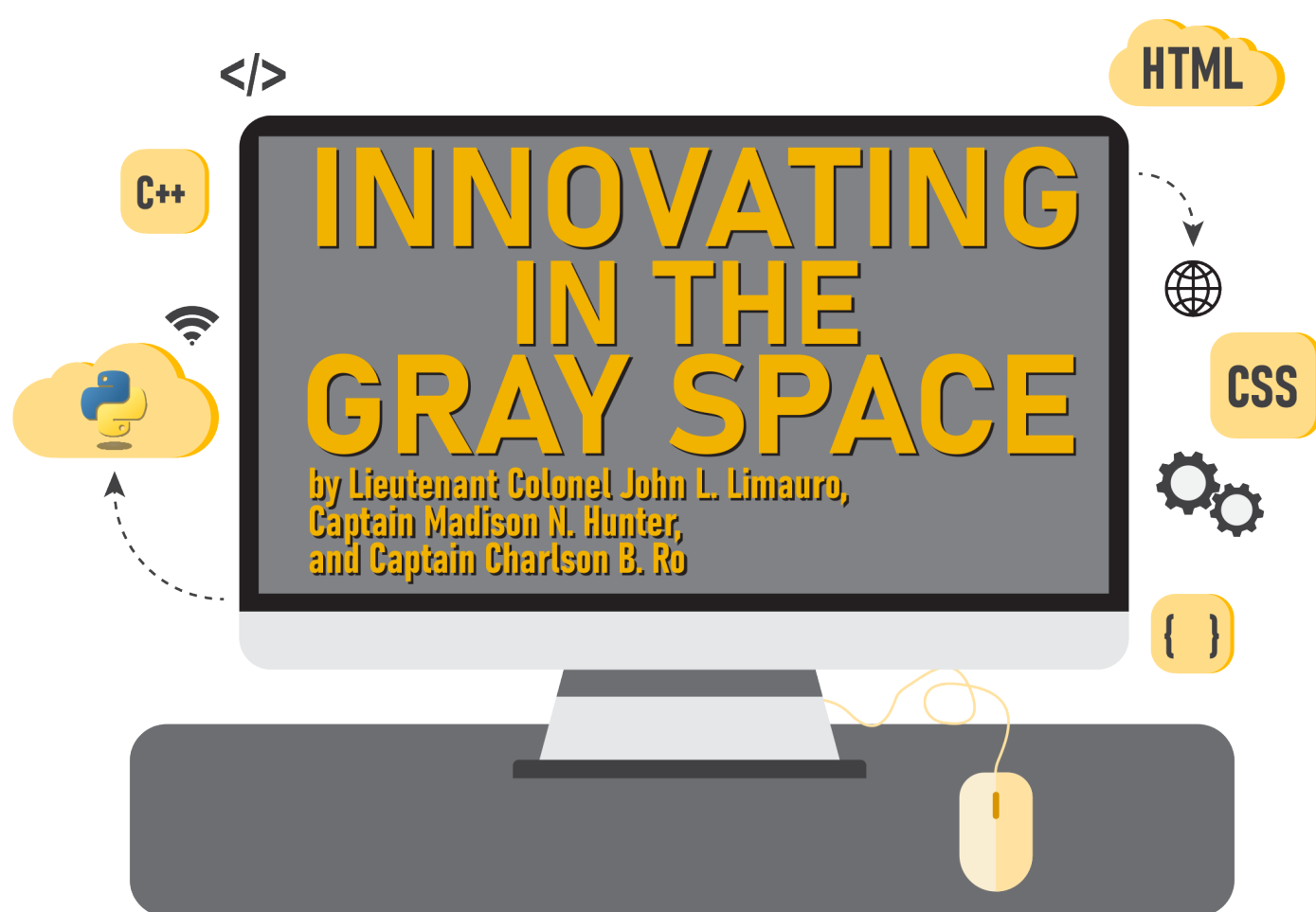
The 307<sup>th</sup> MI Battalion's CHASE has been successful because of experienced, empowered, and motivated NCOs. Any forward collection battalion with strong NCOs who want to take ownership of their mission and increase the quantity and quality of the collection they support can replicate this framework. 

*LTC John G. Wildt commands the 307<sup>th</sup> Military Intelligence (MI) Battalion in Vicenza, Italy. He deployed six times to Iraq and twice to Afghanistan, serving in positions with U.S. Army Forces Command (FORSCOM), U.S. Army Special Operations Command, Headquarters, Department of the Army, the interagency, and the Office of the Secretary of Defense. He holds a bachelor of economics from the University of Alabama and a master of policy management from Georgetown University.*

*Ssg John A. Quinn serves as the 307<sup>th</sup> MI Battalion Counterintelligence (CI) and Human Intelligence (HUMINT) Analytical Support Element (CHASE) All-Source Analytic Cell noncommissioned officer in charge (NCOIC). He deployed to Iraq once, serving in support of a joint task force as a targeting analyst. He holds a bachelor of science in liberal arts from Excelsior University and is pursuing a master of arts in global security studies from Johns Hopkins University.*

*Ssg Caleb M. Mazaika serves as the 307<sup>th</sup> MI Battalion CHASE HUMINT Analytic Cell NCOIC. He deployed once to Afghanistan and once to Africa, serving in positions with FORSCOM and the U.S. Army Intelligence and Security Command as a HUMINT collector, sergeant, and team leader. He holds an associate of applied science in computer graphic design from Carroll Community College in Westminster, MD.*

*Ssg Zachary A Verrastro serves as the 307<sup>th</sup> MI Battalion CHASE CI Analytic Cell NCOIC. He previously served overseas in Korea, Kuwait, and Djibouti, holding NCOIC and Special Agent in Charge positions for CI sections. He holds an associate of general studies from the American Military University and is pursuing a bachelor of arts in psychology with a minor in family development from the same institution.*



*Listing the products and services in this article does not imply any endorsement by the U.S. Army, the U.S. Army Intelligence Center of Excellence, or any U.S. government agency.*

## Framework for Innovation

The October 2023 edition of FM 2-0, *Intelligence*, was a major step forward in how Intelligence professionals adapt and fight along with the other warfighting functions in the Army's multidomain operations warfighting concept. It acknowledges advancements in technology and references data literacy skills as imperative in addressing the volume of data in the future fight.<sup>1</sup> The release of this significant field manual, concurrent with the brutal escalation of the decades-long Israel-Hamas conflict, elevated demands on the 513<sup>th</sup> Military Intelligence (MI) Brigade-Theater (MIB-T) to adapt to the evolving needs of the Army Service component command and the operational theater. The brigade supported multidomain operations alongside U.S. forces and multinational partners while brigade leadership leveraged the workforce on hand and purposefully task organized. The result was an approach to MI problem sets focused on the data-centric capabilities and requirements of the MIB-T, such as a common operational picture, common intelligence picture, and knowledge management.<sup>2</sup>

Data training, including such skills as data comprehension, data manipulation, and data-driven decision making, are mission critical to the functions of a MIB-T.<sup>3</sup> FM 2-0 gives units the responsibility of incorporating data training into their annual training plans and encourages individuals to

build their skillsets through self-development.<sup>4</sup> At the 513<sup>th</sup> MIB-T, innovation focuses on closing the skill gaps between these data requirements and Soldiers' existing skillsets. The innovation team emerged under the guidance of the brigade commander and assigned to the operations section (S-3), ensuring innovation directly supports operations. Fashioning a section in this manner requires the officers and Soldiers assigned to these projects to work outside of their modified table of organization and equipment (MTOE) billets—this is where we find the gray space.

Retired COL Joe Buccino describes this reality in his article "Innovation Overload: Army Units Are Drowning in Ideas." He offers "double-[hatting] to serve this intense focus on innovation"<sup>5</sup> as an argument for the dissolution of Soldier-led innovation elements throughout the Army. Indeed, units must make trade-offs when Soldiers assigned to one section are performing duties in another; however, the value these Soldiers provide when empowered through upskilling in data and software domains necessitates the existence of "innovation show [ponies]."<sup>6</sup>

After the Hamas-led attack on Israel on October 7, 2023, Soldiers of the 513<sup>th</sup> MIB-T tackled challenging problems as they arose. The team developed automation and solutions from the ground up that would otherwise take years of research, development, testing, and authorization to produce across the enterprise. Thus, we created a scalable and mission-focused framework for innovation centered on the MIB-T's data demands.

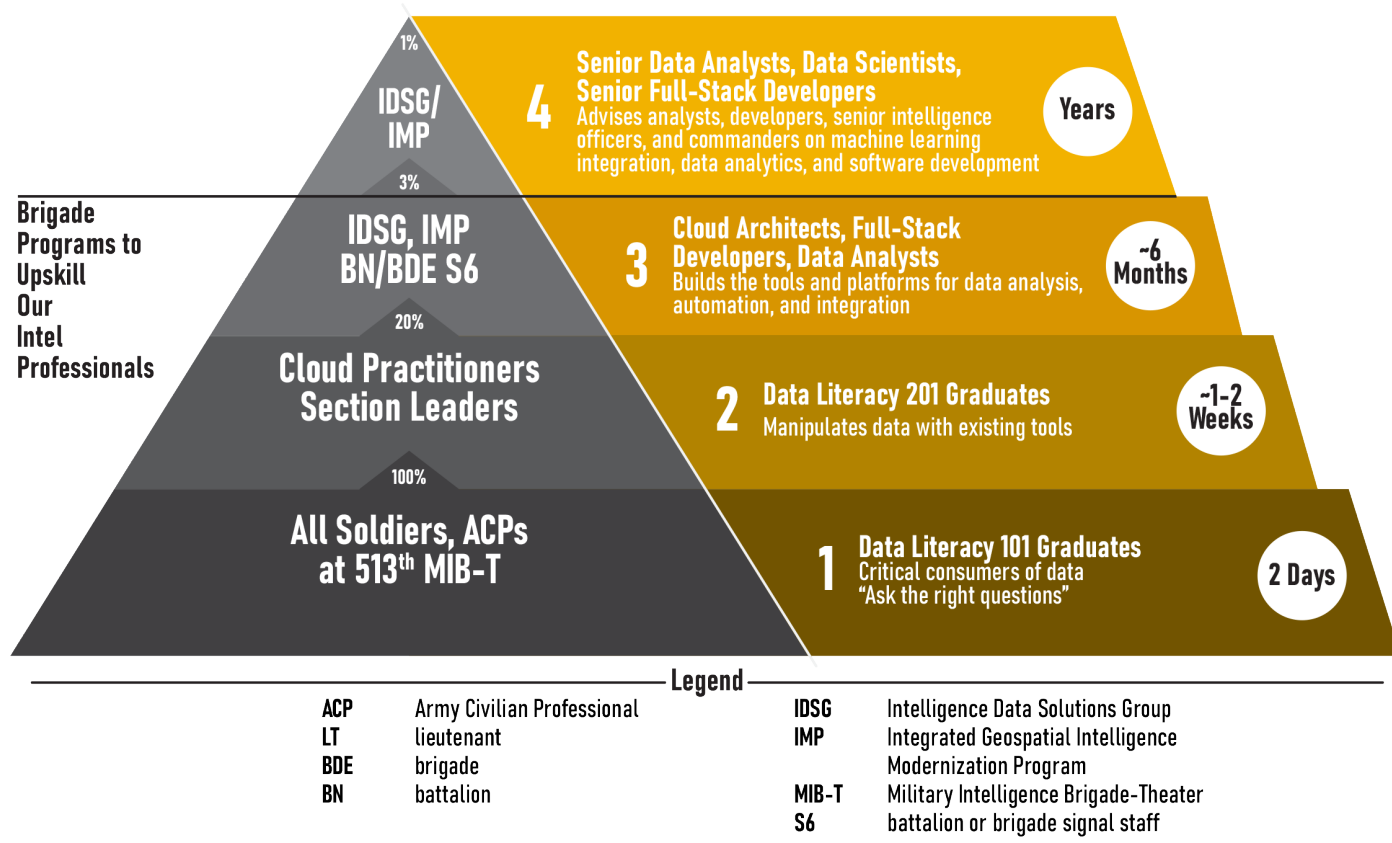


Figure 1. 513<sup>th</sup> Upskilling Pathway (figure adapted from original by CPT Madison Hunter)

## Views on Innovation and Data Expertise Progression

Organizations need users and collectors who understand how to read, work, analyze, and communicate with data to incorporate artificial intelligence and enable advanced analysis. The 513<sup>th</sup> MIB-T views data expertise as foundational to innovating our problem sets. Data Literacy (DL101) is a course that lays the groundwork for increasing this data expertise. It serves as the basis of a pathway to upskilling in the brigade and drives a cultural change in how intelligence professionals use data (see figure 1).

The 513<sup>th</sup> MIB-T began hosting iterations of the two-day DL101 course in May 2022 to equip Soldiers and Civilians with this foundational data knowledge. The course aims to provide Soldiers and analysts with data literacy fundamentals they can apply when returning to their sections. For example, when analysts receive a priority intelligence requirement (PIR), they should know what data is the most valuable to answer the requirement quickly and accurately. They should also recognize what other data may be needed.

In response to the growing demand for DL101, the 513<sup>th</sup> MIB-T established a data literacy task force to teach and certify instructors. Instructors are typically section noncommissioned officers who understand the data their teams encounter daily. They use relevant examples like specific intelligence discipline data to bridge the theoretical to practical knowledge gap. The brigade strives for 100 percent of all Soldiers and Army Civilians to take this foundational course.

Our colleagues address data literacy training and education in their August 2023 article "Take Ownership of Your Formation's Data Literacy."<sup>7</sup>

The next level of data expertise is empowering users who understand the capabilities of existing tools to maximize their use when responding to commanders' PIRs and friendly force information requirements (FFIRs). The 513<sup>th</sup> MIB-T covers these skills in Data Literacy 201 (DL201), which provides Soldiers with knowledge of the available tools to manipulate and work with data effectively. Many Soldiers have access to discipline-specific tools that effectively organize and analyze data, such as the Army Intelligence Data Platform for intelligence analysts and the Microsoft 365 Power Business Intelligence tool for human resource personnel. However, Soldiers often learn to use these tools on the job and understand just enough to meet their section's immediate daily requirements. This somewhat limited understanding can lead to inefficient processes and habits. DL201 consists of several courses driven by section requirements that teaches Soldiers how to make the most of these existing tools. Course offerings include—

- ◆ Database orientations.
- ◆ Microsoft Excel beginner to advanced.
- ◆ Amazon Web Services Cloud Practitioner Essentials.<sup>8</sup>
- ◆ Microsoft Power Business Intelligence and Power Applications.<sup>9</sup>
- ◆ Beginner Python.<sup>10</sup>



DL201 has several modalities, including online offerings, Foundry, and in-person courses taught by section noncommissioned officers. The 513<sup>th</sup> MIB–T aims for about 20 percent of the brigade to be DL201 certified.

Practitioners at the next tier (DL301) develop tools to answer PIRs and FFIRs. These individuals fully integrate software, data, artificial intelligence, and machine learning knowledge. Automating processes enables the units to adapt to a shrinking MTOE while increasing intelligence production quality. These users complete a much more intensive upskilling option that provides Soldiers in project teams the skills to build tools and platforms for data analysis and automation. Courses include—

- ◆ Amazon Web Services Certified Solutions Architect.<sup>11</sup>
- ◆ Galvanize Software Development Immersive.<sup>12</sup>
- ◆ Galvanize Data Analytics Immersive.<sup>13</sup>

The 513<sup>th</sup> MIB–T strives for about three percent of the brigade to be DL301 certified because of the length and cost of these courses.

Finally, the senior data analysts, data scientists, and full-stack developers are at the top of the pyramid. These individuals deeply understand industry knowledge and work within more restrictive environments such as classified networks. They advise commanders, Soldiers, and developers on pathways ahead and help overcome roadblocks. This background requires a level of knowledge and expertise beyond what the 513<sup>th</sup> MIB–T can teach in-house. Thus, the brigade strives to hire or recruit individuals who already possess this advanced training. These individuals deeply understand industry knowledge and how to apply these skills in restrictive environments such as classified networks. They advise commanders, Soldiers, and developers on pathways ahead and help overcome technical roadblocks.

## Innovation Task Organization

Most innovation elements operate and are resourced at the division or higher level. The 513<sup>th</sup> MIB–T’s innovation element operates at the brigade level, focusing the scope of our problem sets on teams of 5 to 20 users. Operating at the brigade level enables closer coordination between Soldier requirements and developers. It also allows developers to focus on workflows and to generate solutions for problems that do not affect a large enough percentage of the Army population to warrant high-cost, industry-level solutions. The brigade does not intend its solutions to be enterprise solutions. Additionally, funding limitations necessitate efficient resource management; therefore, innovation falls under the S-3, brigade operations staff, to maximize allocated resources.

As the commander’s arm for planning and execution, the S-3 operationalizes the commander’s vision and intent to innovate. The S-3 does this through the innovation officer, who works closely with project team leads. The 513<sup>th</sup> MIB–T project teams align skillsets to the focus of each project. There are six project teams organized into enabling and action groups.

These teams house developers who create tools based on the needs of Soldiers conducting intelligence operations. These teams meet foundational requirements for innovation in data and software domains such as training and education, platforms, data storage, and computational resourcing. The action group includes the Staff Modernization Strategy (STAMOS), IDSG, and the Integrated Geospatial Intelligence Modernization Program (IMP). These teams house developers that create tools using algorithms and software based on Soldier and analyst needs, such as the IDSG and the IMP. The full-time team leads ensure adequate resourcing and management of innovation efforts by collaborating closely with the brigade’s Chief Innovation Officer, who works within the brigade S-3 and aligns project teams with unit organic skillsets (see figure 2). While each section has unique capabilities, we will focus on the IDSG for a detailed discussion.

## Intelligence Data Solutions Group

The IDSG comprises a team of software developers and a team of data analysts. In figure 1, the IDSG personnel occupy the third and fourth tiers of the pyramid alongside their counterparts in the IMP. Soldiers who are a part of the IDSG attend Galvanize coding bootcamps that are 12 weeks long. The IDSG program manager oversees project management and ensures that the team’s efforts align with unit priorities and mission. In addition, the 513<sup>th</sup> MIB–T appointed the brigade’s FA26B, Data Systems Engineer, as the platform lead responsible for building and maintaining the cloud environment and ensuring developers have access to coding environments. This position is organic to every MIB–T and does not require recoding a billet or moving a Soldier from one set of duties to another (see figure 3).

The IDSG has three focus areas, each with a designated section lead: advanced analytics supporting the intelligence process, intelligence workflow automation, and application development. These section leads work closely with the program manager to identify, understand, and determine the scope of problem sets. They also assign team members to problems based on background knowledge, individual expertise, and talent. The IDSG represents numerous intelligence military occupational specialties. For example, 35G geospatial imagery intelligence analysts work closely with the IGD team members on projects involving coordinate, terrain, and imagery data. The 352N signals intelligence (SIGINT) analysis technician, works closely with the SIGINT section to identify analytical needs and scope problems for projects (see figure 4).

Projects generally fall within the three focus areas and must support mission requirements or provide benefit to the organization. Among these foci, intelligence workflow automation has been the most fruitful in generating solutions of immediate value to our analysts. Many processes within the intelligence enterprise have small userbases, and thus do not

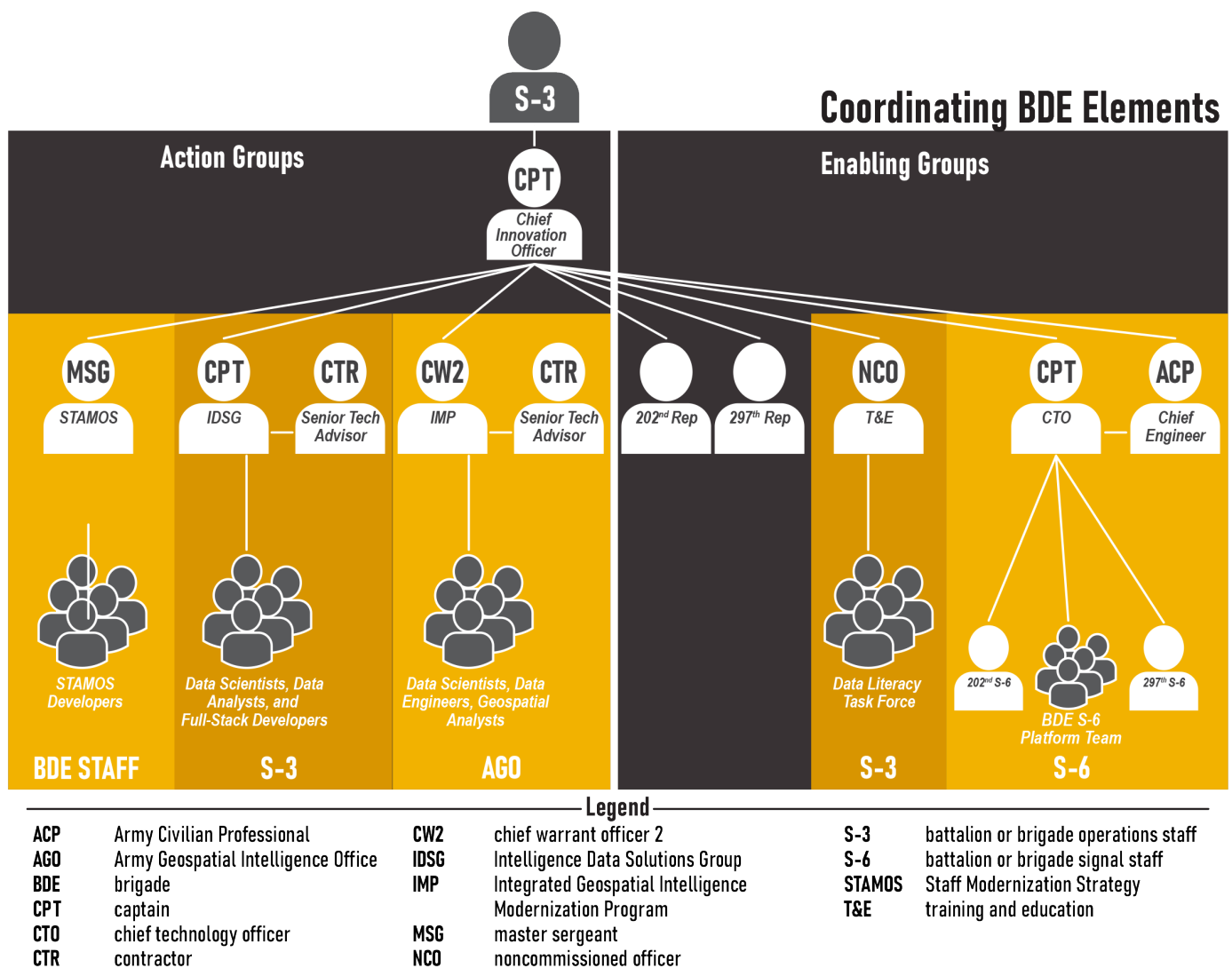


Figure 2. Brigade Innovation Task Organization (figure adapted from original by CPT Madison Hunter)

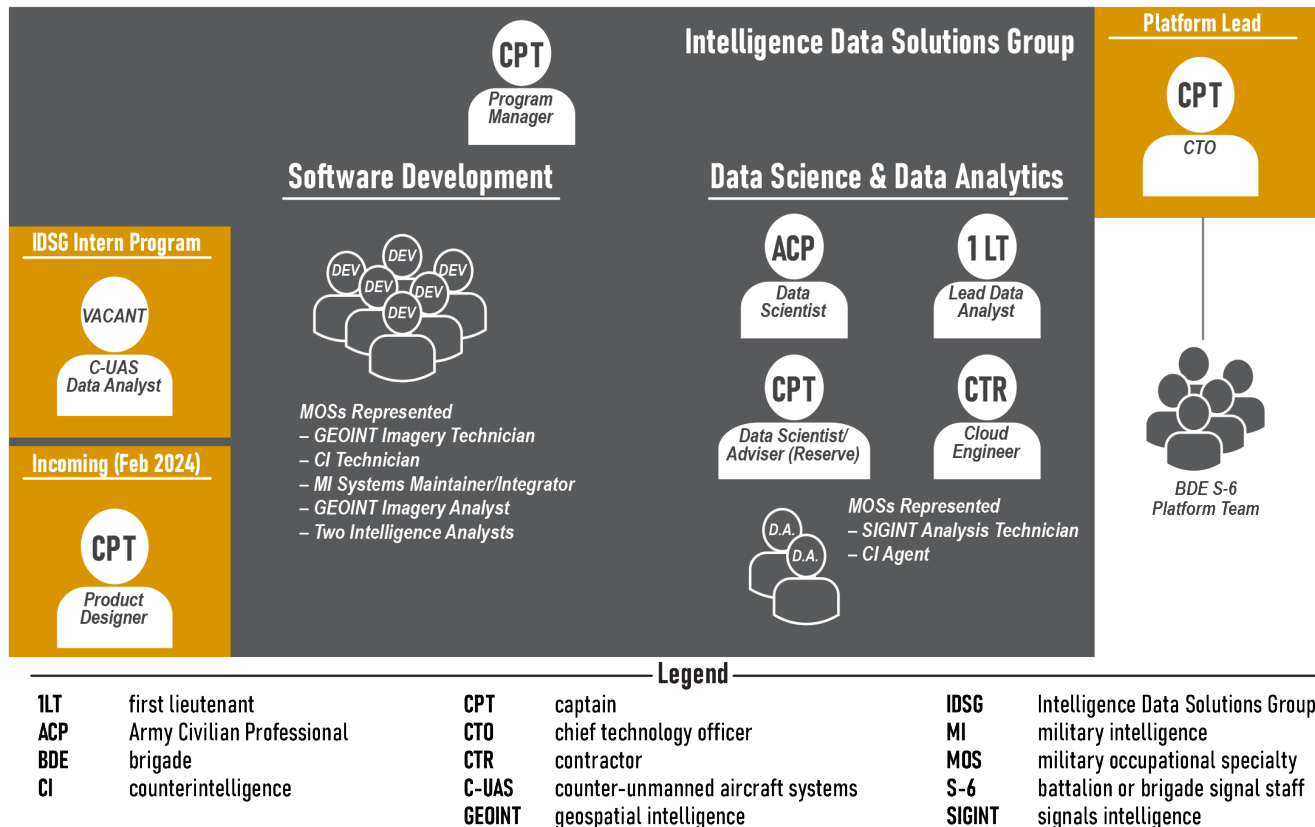


Figure 3. Intelligence Data Solutions Group Task Organization (figure adapted from original by CPT Charles Ro)

receive enterprise-level software solutions. The intelligence workflow automation section's userbase may have Soldiers dedicated to tasks as simple as copying information from one platform or interface to another.

One example of this is the automation of monitoring equipment statuses. The status of critical mission-oriented equipment is typically a commander's critical information requirement because it provides intelligence value. Consequently, an analyst must monitor the equipment throughout the day and report promptly through other channels when equipment fails. The IDSG automated this process by creating a dashboard indicating equipment status in real time. This effort frees bandwidth for analysts who no longer must devote entire daily shifts to monitoring and reporting.

In web application development, IDSG recently created a tool to automate the drafting of open-source intelligence reports. This effort coincided with intelligence workflow automation and allowed analysts to create more timely reports. The software, designed like a bibliography generator, is run locally by an analyst. It takes the necessary input fields from the user and creates a pre-formatted output that is ready to copy and paste. The tool saves about 30 to 60 seconds per report, which quickly adds up to hours saved as the volume of reporting increases. Currently, the tool saves approximately 20 hours each week for the open-source intelligence cell. The tool also expedites onboarding new personnel, enabling them to integrate into the team sooner.

For advanced analytics supporting the intelligence process, the IDSG took unlabeled data from the SIGINT section and developed an algorithm to identify the collection platform associated with each data point rapidly. The algorithm reduces by 15 minutes the time needed for an analyst to identify a collection platform, which translates to approximately 800 hours of labor saved each year. More importantly, it reduces the time for indications and warnings to flow from sensor to shooter, providing early warning and force protection capabilities. With algorithm deployment planning underway, this

idea won the U.S. Army Central Command Ideas for Innovation challenge in October 2023.<sup>14</sup>

Initiatives like the IDSG enable Soldiers with unique skills to apply their talents to the problems facing them, becoming force multipliers. These Soldiers solve immediate problems at the lowest level. These solutions better enable the MIB-T to provide pivotal data and ingest services while avoiding expensive acquisition processes. Although they are performing duties in the gray space outside their military occupational specialties, their efforts directly contribute to the success of their teams' mission—moreover, programs like the IDSG open doors in the MI Corps for data-savvy Soldiers.

The MI Corps will undoubtedly be in a war for talent with other branches to recruit and retain technical talent. Both recruitment and retention require creative solutions such as additional skill

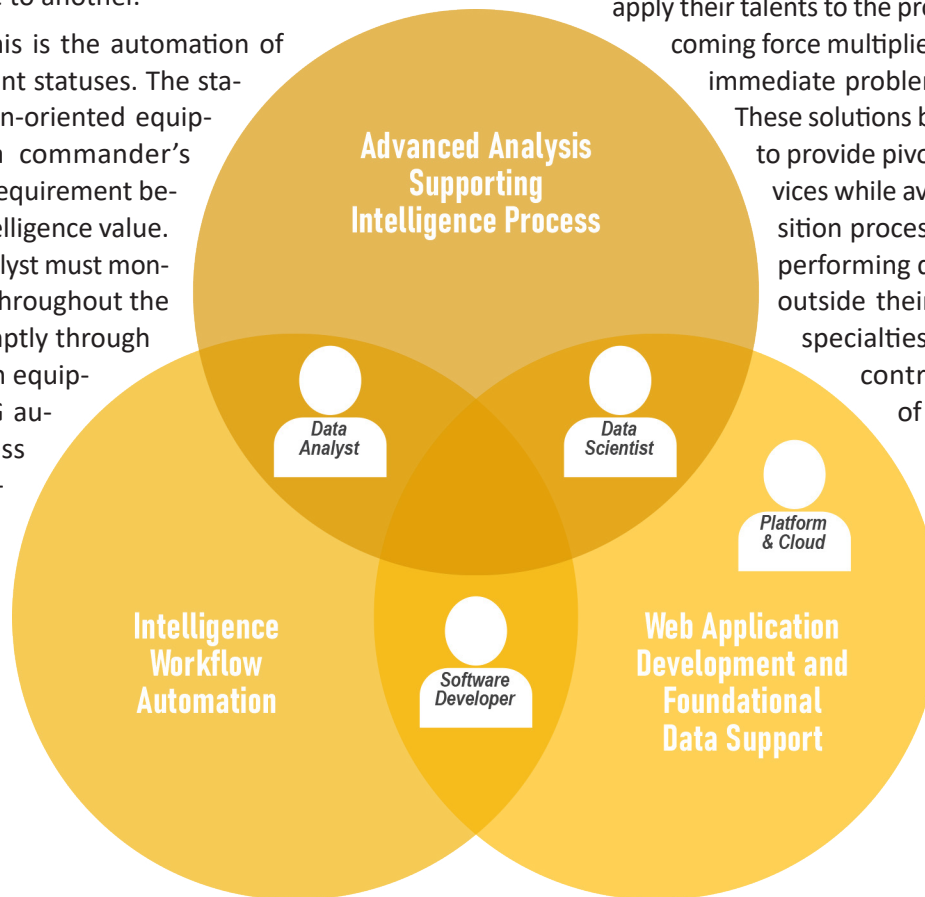



Figure 4. Intelligence Data Solutions Group Focus Areas (figure adapted from original by CPT Charles Ro)

identifiers and personnel development skill identifiers, especially for Soldiers with extensive schooling and experience. Establishing career pathway maps and progression is another option for retaining talented Soldiers. For example, the FA35B (Strategic Intelligence) career map allows all majors' assignments to count as key developmental assignments per branch guidance and DA Pam 600-3, *Officer Talent Management*.<sup>15</sup>

## Conclusion

Commanders must make decisions regarding risks, specifically to the force and to the mission. Innovating in the gray space is no different. To ensure efficient and effective mission accomplishment, leaders must apply resources, talent, and time to each unit's innovation effort appropriately. This is where commanders at each echelon can task organize their formation for purpose as MTOEs and requirements change. Since October 7, 2023, the operational tempo for 513<sup>th</sup> MIB-T Soldiers has increased while the quantity of Soldiers in upcoming MTOEs has decreased. Innovation, particularly in the automation of routine workflows, enables a shrinking workforce to keep pace with the speed of operations. It is, therefore, critical to winning the next conflict. Deputy Secretary of Defense Kathleen Hicks stated in May 2023 that



innovating isn't about research and development dollars but about bringing a warfighting culture of operators, analysts, and technologists together.<sup>16</sup> 

#### Endnotes

1. Department of the Army, Field Manual 2-0, *Intelligence* (Washington, DC: U.S. Government Publishing Office [GPO], 1 October 2023), 1-13.
2. Ibid., 7-10.
3. Ibid., 1-13.
4. Ibid.
5. Joe Buccino, "Innovation Overload: Army Units Are Drowning in Ideas," *Opinions*, Military.com, September 19, 2023, <https://www.military.com/daily-news/opinions/2023/09/19/innovation-overload-army-units-are-drowning-ideas.html>.
6. Buccino, "Innovation Overload."
7. Orlando Nieves, John Boyer, and Feihrrren Calhoun, "Take Ownership of Your Formation's Data Literacy," *Military Review Online Exclusive*, 25 August 2023, <https://www.armyupress.army.mil/journals/military-review/online-exclusive/2023-ole/data-literacy/>.
8. "Cloud Practitioner," *Learn About, Training*, Amazon Web Services, 2024, <https://aws.amazon.com/training/learn-about/cloud-practitioner/>.
9. "Learn Power BI," *Products*, Power Platform, Microsoft Corporation, 2024, <https://www.microsoft.com/en-us/power-platform/products/power-bi/learning?country=us>; and "Power Apps," *Products*, Power Platform, Microsoft Corporation, 2024, [https://www.microsoft.com/en-us/power-platform/products/power-apps#tabs-pill-bar-resources\\_tab1](https://www.microsoft.com/en-us/power-platform/products/power-apps#tabs-pill-bar-resources_tab1).
10. "About Python," *Python Software Foundation*, 2024, <https://www.python.org/about/>.
11. "AWS Certified Solutions Architect – Associate," *Certification*, Amazon Web Services, 2024, <https://aws.amazon.com/certification/certified-solutions-architect-associate/>.
12. "Active Duty Coding Training in Software Development," *Galvanize*, 2024, <https://www.galvanize.com/software-development-immersive/>.

13. "Data Analytics Immersive Bootcamp for Active Duty Service Members," *Galvanize*, 2024, <https://www.galvanize.com/data-analytics-immersive-program/>.

14. Richard Moore, "USARCENT Hosts Ideas for Innovation Challenge," *U.S. Army Worldwide News*, October 3, 2023, [https://www.army.mil/article/270464/usarcent\\_hosts\\_ideas\\_for\\_innovation\\_challenge/](https://www.army.mil/article/270464/usarcent_hosts_ideas_for_innovation_challenge/).

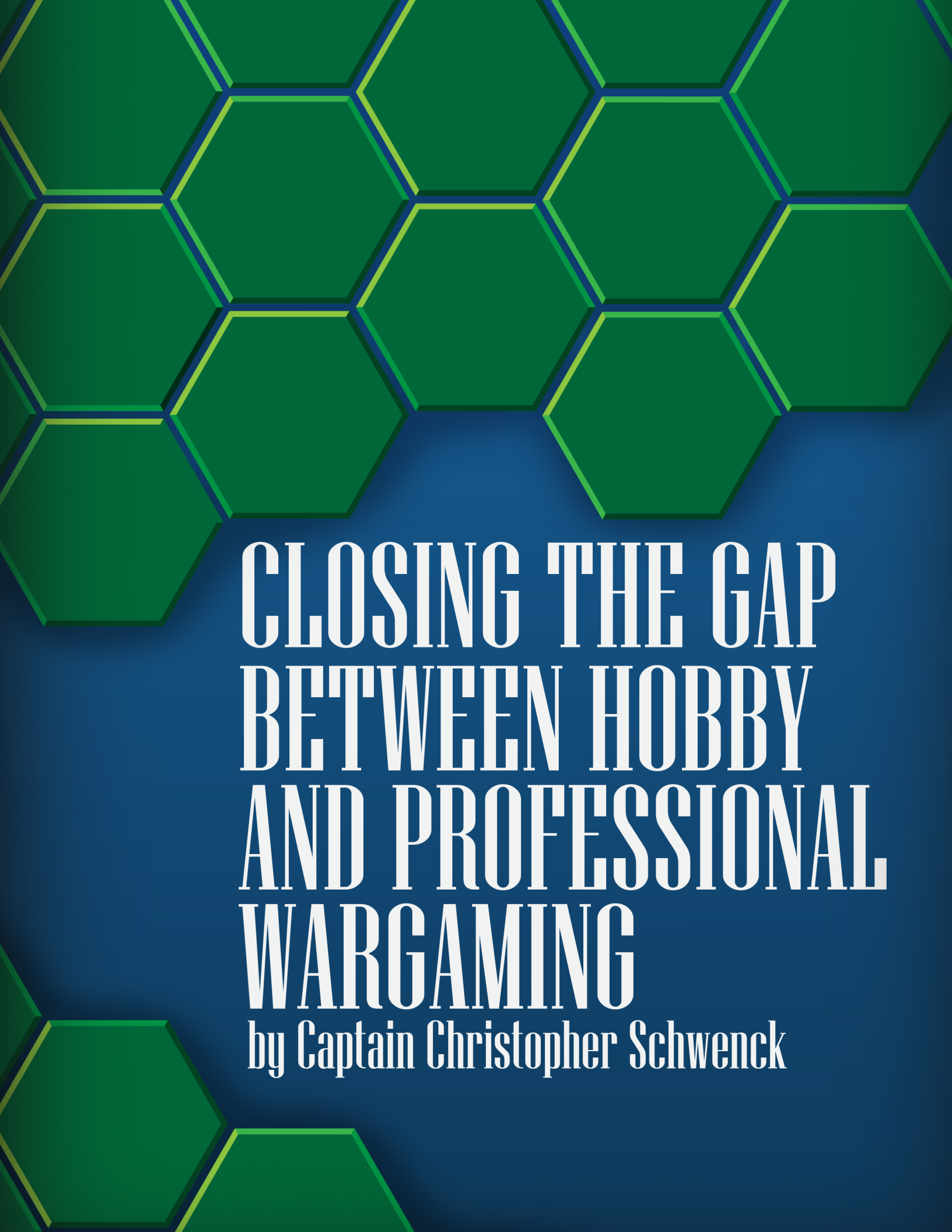
15. Department of the Army, "Operations Support: Military Intelligence Branch," May 2024, in *Smartbook* online supplement to Department of the Army Pamphlet 600-3, *Officer Talent Management* (Washington, DC: U.S. GPO, 14 April, 2023), 4.

16. Joseph Clark, "Innovation Critical to Success as DOD Faces Competition with China," *DoD News*, May 9, 2023, <https://www.defense.gov/News/News-Stories/Article/Article/3390241/innovation-critical-to-success-as-dod-faces-competition-with-china/>.

*LTC John Limauro is currently the assistant chief of staff, G-2 for 11<sup>th</sup> Airborne Division and was formerly the operations officer for the 513<sup>th</sup> Military Intelligence (MI) Brigade-Theater (MIB-T). As the brigade's operations officer he planned and executed the brigade's innovation, modernization, and continuous transformation strategy, focusing on data literacy and Soldiers' upskilling to solve intelligence problems in support of U.S. Army Central and U.S. Central Command missions. He previously served in numerous units and positions across the Army Intelligence and Security Enterprise to include as the senior intelligence officer, 75<sup>th</sup> Ranger Regiment and G-2 operation chief, 25th Infantry Division.*

*CPT Madison Hunter is the innovation officer for the 513<sup>th</sup> MIB-T. She commissioned from Duke University in 2019 as a MI officer. Following the MI Basic Officer Leaders Course, CPT Hunter served in the 2<sup>nd</sup> Brigade Combat Team, 101<sup>st</sup> Airborne Division (Air Assault) as the assistant S-2 for 1<sup>st</sup> Squadron, 75<sup>th</sup> Cavalry Regiment and as the military intelligence company multifunction platoon leader, 39<sup>th</sup> Brigade Engineer Battalion, 75<sup>th</sup> Cavalry Regiment.*

*CPT Charlson Ro is currently attending the signal captains career course and formerly served as the lead data analyst for the 513<sup>th</sup> MIB-T, Intelligence Data Solutions Group. He commissioned from the U.S. Military Academy at West Point in 2020 as a MI officer. He earned his master's in business analytics from the Massachusetts Institute of Technology through the Lincoln Laboratory Military Fellowship following commissioning. After the MI Basic Officer Leaders Course, CPT Ro served at Camp Humphreys, Republic of Korea as the theater architecture and all-source fusion officer in charge for the 532<sup>nd</sup> MI Battalion, 501<sup>st</sup> MIB-T.*



# CLOSING THE GAP BETWEEN HOBBY AND PROFESSIONAL WARGAMING

by Captain Christopher Schwenck

Discussion of the commercial products and services in this article does not imply any endorsement by the U.S. Army, the U.S. Army Intelligence Center of Excellence, or any U.S. government agency.

## Introduction

Wargaming represents the core of the military decision-making process's vital fourth step: course of action analysis. It helps decision makers simulate contact with the enemy, exercise decision making, and analyze and refine a course of action. However, professional wargaming still suffers from a series of shortfalls. A misapplication of the wargame concept, a lack of professional gamers and game designers, and stovepiped accessibility prevent professional wargaming from reaching its full potential. Despite increased emphasis and standardization across the Department of Defense in the past decade, professional military wargaming could still learn much from its smaller hobby-focused cousin, as hobby gaming could provide a commercial-off-the-shelf solution to military wargaming's pitfalls.

## Historical Background

For centuries, military strategists sought methods of simulating war to introduce general tactical concepts to officers and general staff that would allow them an opportunity to exercise their decision-making prowess. Early examples took their inspiration from chess and fall under a broad category of games called "war chess." Like classic chess, the pieces on the board symbolized different abstract types of military units, each with its own movement rules around a gridded board. As war chess evolved, pieces began to denote actual military units more closely, and the square spaces on the board came to signify real terrain like hills and lakes.<sup>1</sup> These early wargames did little to simulate actual conflict and served merely as intellectual exercises and introductions to terminology. As they evolved, they also became an incredibly unwieldy and expensive privilege, consisting of ornate pieces played on a large sand table modeling terrain, only accessible to military elite.

Modern hobby and professional wargaming trace their lineage back to 1824 when Prussian Lieutenant Georg Heinrich Rudolph Johann von Reisswitz published a set of wargaming rules and instructions called *Anleitung zur Darstellung militairischer manöver mit dem Apparat des Kriegsspiels (Representation of Tactical Maneuvers under the Guise of a Wargame)*. Reisswitz opted to scrap the system developed by his father, which used a large sand table and hand-carved pieces. Instead, he employed modern paper maps, used since the 1730s, that utilized contour lines to accurately indicate real-world

terrain and elevation on the potential future battlefield. Following a demonstration

to Prussian Chief of Staff General von Muffling, Reisswitz's *Kriegsspiel* (wargame) became a mainstay among Prussian military officers. Even General Helmuth von Moltke, forefather of the U.S. Army's mission


command principles, became an avid player.<sup>2</sup> Since then, wargaming has evolved into numerous hobby and professional adaptations and has driven military planners to experiment with courses of action, exercise decision making, and to simulate hypothetical scenarios.

## Misapplication of Wargames

Defining wargaming and its intended purpose is the first major hurdle both professional wargamers and military staff must overcome. In defining a wargame, professional naval game designer Peter Perla wrote, "Wargames revolve around the interplay of human decisions and game events....A wargame's maps, rules, pieces, or computers are only the media through which competing decisions are implemented and judged. Wargames are tools for gaining insights into the dynamics of warfare."<sup>3</sup> For Perla, human decisions are the central focus of a wargame, and the wargame is only one side of a triangle of tools needed for the study of defense matters. Decision makers should use wargaming in addition to exercises and historical analysis, with all three offering unique insights: wargames emphasize human decisions; exercises test human or technological capability; history enables informed analysis of possible outcomes.<sup>4</sup> Decision makers must choose the best tools to answer the applicable question.

Decision makers often confuse and misuse wargames and exercises. Millennium Challenge 2002 (MC '02) is the most infamous example of this in recent professional wargaming history. The U.S. Joint Forces Command (JFCOM) executed MC '02 in the summer of 2002 to simulate conflict between the United States and a potential Middle Eastern adversary. JFCOM intended to evaluate new military concepts such as effects-based operations, rapid decisive operations, and a standing Joint Force headquarters.<sup>5</sup> MC '02 proved to be one of the most expensive concept developments in U.S. military history. The exercise cost \$250 million and grew to include 13,500 Service members over a 2-year development period.<sup>6</sup> Despite its massive scale, MC '02 failed in its application of wargaming.





JFCOM conducted its wargame in conjunction with a massive live-fire, forcible-entry exercise that pulled the entire 82<sup>nd</sup> Airborne Division and 1<sup>st</sup> Marine Regiment out of their training cycles. However, the game jeopardized the viability of the exercise when the red (opposition) force, led by Marine Corps Lt. Gen. Paul Van Riper, managed to destroy 19 ships of the blue (friendly) force Carrier Strike Group. The notional casualties included several cruisers, five amphibious assault ships, and the carrier itself.<sup>7</sup> In a real-world scenario, these losses would make the forcible entry operation impossible. The simulation's white cell, or game administrators, quickly called the JFCOM commander to inform him that the red force's actions had jeopardized the joint force, live-fire component of MC '02.

Consequently, the commander decided to notionally refloat the blue force fleet and continue as if nothing had happened. As JFCOM attempted to prove its concept, institutional bias inevitably compromised the game's integrity. Without an independent or unbiased arbitrator, the white cell manipulated the results and followed a script that maximized the blue force's capabilities and tied the red force's hands. JFCOM falsely confirmed the integrity of the game and in the immediate aftermath declared all concepts validated. However, 10 years after the exercise, the final 752-page JFCOM report detailed the limitations of the exercise and how artificialities had aided the blue force victory.<sup>8</sup>

Commercial solutions from the hobby realm or a contract producer could have benefitted MC '02. JFCOM attempted to assess too many variables in one joint wargame and exercise. Following the scientific method requires individually isolating the variables under investigation and evaluating them repetitively to confirm results. Without isolation, the experimenters cannot determine which variables affected which aspects of the simulation. The three variables JFCOM intended to validate suggest a required minimum of four iterations of the wargame: one for each variable plus one control without any variables. However, conducting the game in conjunction with an expensive, large-scale exercise eliminated this possibility. JFCOM had only one attempt.

A traditional hex-and-counter style wargame on a paper map could have provided the command with a cheaper, repeatable alternative to validate their concepts before moving to a large-scale exercise. While physical exercises have merit for testing technological or physical capabilities, their steep cost makes them unsuitable for proving concepts. Even on a smaller scale, it can cost the U.S. Army between \$20 and \$30 million to send a brigade combat team to one of the nation's

three combat training centers, not including routine logistical needs like food and ammunition.<sup>9</sup> These time-consuming, expensive exercises rarely allow the repetition required for good analysis. By contrast, commercially produced hobby wargames are much less costly. For example, leading hobby wargame publisher GMT Games produces off-the-shelf products that provide limitless opportunity and adaptability for real-world decision-making exercises, with topics ranging from small tactical skirmishes to theater-level large-scale combat operations—and the average cost of their products is \$70 to \$90.<sup>10</sup>


Additionally, many hobby wargames run one to eight hours of playtime, offering plenty of opportunity for repeated playthroughs to compare variables, compile after action reviews, and document lessons learned. Since independent third parties develop them, these games also benefit from freedom from bias. In MC '02, JFCOM attempted to prove that the concepts they developed justified the command's existence. Consequently, when the results of the wargame decision making jeopardized the integrity and continuation of the exercise, the white cell allowed institutional bias to affect the game's play, skewing the results.

### **The Next Generation of Professional Wargamers**

The heyday of hobby wargaming in the 1970s contributed to the revival of professional wargaming in the 1980s and 1990s. Since then, demand for professional wargames continues to rise, with the Department of Defense continuously seeking new ways to simulate experimental concepts like multidomain operations in the modern era. Yet, the rising demand for professional wargames has not cultivated a sufficient increase in the number of professional wargamers.

To stay at the forefront of modern conflict simulation, professional wargaming requires experienced gamers capable of identifying complex problems and developing scenarios that showcase them. These gamers must implement both time-tested and innovative mechanisms and technologies to provide decision makers a vehicle to simulate these scenarios.<sup>11</sup> While organic wargamers spearheaded the field's resurgence in the 1990s, modern professional military wargaming relies on defense contractors and civilian experts. Aside from not being cost-effective, this inverted wargamer pyramid does not foster the development of institutional knowledge management. The lack of a designated wargaming military occupational specialty or a pipeline to recruit, train, and develop future wargamers compounds this issue.<sup>12</sup> While suggestions for these concepts merit consideration, hobby wargaming provides a short-term stopgap.

Senior game designer Sebastian Bae, a defense wargaming research analyst at the Center for Naval Analyses, details his introduction to professional wargaming: "My career in wargaming began by chance, not by design....I learned to be a



wargamer on the job. With no prior wargaming experience, I was taught to combine my storytelling ability, my knowledge of the military, and my personal experience with commercial board games to develop analytical wargames.”<sup>13</sup> Bae proposes that continued wargaming competition provides the best method to train future wargamers to analyze human decision making. He argues that competition will teach principles of chance, strategy, and reward while encouraging players to continuously tackle the intellectual challenge provided by a good game. The repetition will eventually enable players to “devise new tactics and strategies, recognize patterns, and employ new concepts.”<sup>14</sup>

Bae suggests forums like Tabletopia and Tabletop Simulator on Steam, an online gaming service. However, these forums still require existing games to be manually ported onto the platform. Existing hobby wargames provide the most expedient method for fostering these decision-making competitions across the force to identify, recruit, and train the next generation of professional wargaming talent. Board Game Geek, a popular hobby gaming forum with a database and reviews for over 120,000 games, illustrates the wide availability of commercial wargaming. A search for wargames on the platform returns 23,263 results with subcategories for tactical, operational, and strategic scenarios spanning ancient and medieval, Napoleonic, World War I and II, Vietnam, and modern eras of conflict.<sup>15</sup> Each of these 23,263 games represents unique insights and interpretations of a historical or hypothetical conflict, mechanisms to simulate that conflict, and limitless decision opportunities for players to navigate.

### **Making Wargames Accessible to the Warfighter**

Made a believer by Lieutenant von Reisswitz, General von Muffling saw *Kriegsspiel*’s value to the entire Prussian army. *Kriegsspiel* appealed to Muffling so much that he offered to supplement the number of available copies, claiming anyone with any military experience could and should play the game. In the Prussian *Militär Wochenblatt* no. 402, Muffling recommended the game to the entire army, declaring that “the further distribution and knowledge of the game will earn [von Reisswitz] the thanks of the whole army.”<sup>16</sup> Military commanders from Muffling to Admiral Nimitz have seen the value in wargaming’s ability to shape the military understanding and intellectual development of leaders across operational levels of warfare.

Contemporary professional wargamers worry that only a limited leadership population has access to this intellectual development by virtue of their position or seniority. Like

MC ‘02, most training exercises provide only commanders and staff with the experiential development offered by wargaming. Training provided to other participants is primarily skills-based. Despite this, professional gamers believe wargaming delivers the most value when it is widely accessible, and gamers benefit from iterative play. Sebastian Bae argues, “In a wargame, failure is not final, but merely an opportunity to learn a new method of success. The first time a tactical leader exercises their independent decision-making under stress should not be on the battlefield.”<sup>17</sup> Leaders at all echelons require the opportunity to think creatively under stress and flex their intellectual muscles in a risk-free, limited-cost environment. The hobby wargaming market gives this opportunity to leaders across the operational spectrum.

The variety of commercially available wargames provides limitless scenarios and scales of past, present, future, and fictional conflicts for gamers. Popular titles like *Memoir ‘44*, *Tide of Iron*, or *Bolt Action* use miniatures (miniature figures) on a notional tactical battlefield, using familiar tactical concepts of cover, concealment, and line of sight.<sup>18</sup> This type of game aims to simulate the immediate decisions frontline leaders make in the face of an active enemy or opponent. They scale perfectly to the issues junior officers and noncommissioned officers may face, such as the placement of specific weapon systems or suppressive effects.

Scaling upwards, games such as the *Standard Combat Series* or *World at War ‘85* bring the conflict to the battalion level.<sup>19</sup> These games’ playing pieces act as platoons or companies instead of individual soldiers and teams. This scale allows commanders and staff the opportunity to conduct key steps of the military decision-making process. Notably, these games offer staff officers a chance to gain valuable repetition in mission analysis, intelligence preparation of the operational environment, and course of action development and analysis. These games tend to use realistic orders of battle garnered from historical or modern military units to achieve a historical or potential future military objective. Similarly, division and corps staff members could find GMT’s *The Next War* series of value.<sup>20</sup> Using well-researched potential global flashpoints, each installment in this series utilizes battalion- and brigade-sized units to maneuver over vast swaths of territory such as eastern Poland, the Baltics, Korea, or Taiwan.

Even at the level of strategic simulation, there are commercially available wargames that simulate the possible decisions faced by policymakers and strategic planners. GMT’s *COIN* series of games includes scenarios from the British in Malaysia and Palestine to the United States in Afghanistan.<sup>21</sup> Each of these installments uses two insurgent and two counterinsurgent factions working cooperatively against one another. For example, in *A Distant Plain*, two players control the counterinsurgent factions of coalition forces and the Afghan

government, while another two control insurgent forces acting for local warlords and the Taliban. All players must navigate a realistic labyrinth of conflicting loyalties and shifting alliances. At an even higher level, GMT's *Mr. President* allows players to navigate daily crises in the White House Situation Room as the President of the United States and the White House staff.<sup>22</sup> Here, players prioritize time and resources across a variety of conflicts around the world.

Commercially available hobby wargames offer the luxury of iterative play in prepackaged scenarios that allow repetition, enabling players to learn from their mistakes. They also provide scenarios across various tactical, operational, and strategic levels of conflict. This enables players to execute scenarios pertinent to their circumstances regardless of the echelon where their decision-making occurs. Noncommissioned officers and junior officers can move individual Soldiers, squads, and vehicles in a tactical skirmish. Battalion and brigade staff can simulate courses of action with pieces symbolizing platoons, companies, or battalions. Corps staff and higher can simulate the strategic decision making needed for an entire theater of war or national policy development. This addresses the most significant criticism leveraged against modern professional wargaming—it does not provide pertinent scenarios for the relevant unit of action to exercise their decision making. Hobby wargames do exist that can enable units of action at every echelon across all levels of warfare.

### Hobby Wargaming in the Professional Realm

Hobby wargaming's utility to professional intellectual development is not a novel concept. While hobby gaming has not yet seen widespread implementation, the idea has gained traction throughout the Department of Defense. For example, in 2019, the Marine Corps War College organized a war-game to simulate the United States' ability to fight a modern conflict across multiple fronts. It used three installments of GMT's *Next War* series: *Next War: Korea*, *Next War: Taiwan*, and *Next War: Poland*. The game pitted three red teams (North Korea, China, and Russia) against three blue teams representing Taiwan, Indo-Pacific Command, and European Command. The blue teams faced the additional challenge of balancing U.S. and coalition forces across three theaters and even appointed a Joint Chief of Staff to prioritize force allocation.<sup>23</sup> The exercise resulted in multiple lessons learned, including the logistical challenges posed by a multi-theater conflict, the fleeting advantages of cyber warfare, and the superiority of enemy fires complexes.

Further down the scale of professional military education, a wargaming club in the Military Intelligence Captains Career Course introduces students to hobby wargaming. The tabletop exercises simulate everything from platoon-level World War II skirmishes to corps-level maneuvers in the American Civil War. They force students to think logistically and prioritize

strategically through a wide array of scenarios. The club's faculty sponsor used a playtest copy of GMT's *Decisive Action* to provide students with repetitions on intelligence preparation of the operational environment. *Decisive Action*, set on potential battlefields in Syria and Poland, requires players to conduct terrain analysis and phased allocation of combat enablers via a battalion-scaled conflict between Russian and NATO forces.<sup>24</sup> Functionally forcing players to conduct mission analysis, students drafted and wargamed their red and blue courses of action and intelligence collection plans.<sup>25</sup> The game was a valuable tool for the club's sponsor to provide students with a pragmatic, hands-on application of the fundamentals and processes taught in the classroom. Utilizing a wargame in lieu of a pre-built scenario from the schoolhouse enabled students to assess their plans against real, thinking opponents and required them to adapt to changing battlefield circumstances.

### Conclusion

Hobby and professional wargaming share a common history in the *Kriegsspiel* of the 19th-century Prussian Army. While the two domains have diverged, a significant overlap still exists, and hobby gaming has much to offer its professional counterpart. Hobby gaming provides a cheaper, isolated alternative for staff members and commanders to exercise their intellectual decision-making capabilities. The sheer volume of available hobby wargames allows units to exercise their staff processes and decision making. It also supports professional gaming as it curates the next generation of professional wargamers. Hobby games can be played repeatedly outside the traditional training cycles at a combat training center. Finally, the variety of wargames available provides realistic scenarios for any decision maker regardless of their position or echelon. Hobby wargaming already exists along the fringes of military education. Its embrace by decision makers would help professional military wargaming fill gaps in understanding, training, and accessibility. ✨



## Endnotes

1. Peter P. Perla, *The Art of Wargaming: A Guide for Professionals and Hobbyists* (Annapolis MD: Naval Institute Press, 1990), 17–18.
2. Ibid., 25–30.
3. Ibid., 8–9.
4. Ibid., 11.
5. Gary Anderson and Dave Dilegge, “Six Rules for Wargaming: The Lessons of Millennium Challenge ‘02,” War on the Rocks, November 11, 2015, <https://warontherocks.com/2015/11/six-rules-for-wargaming-the-lessons-of-millennium-challenge-02/>.
6. Micah Zenko, “Millennium Challenge: The Real Story of a Corrupted Military Exercise and Its Legacy,” War on the Rocks, November 5, 2015, <https://warontherocks.com/2015/11/millennium-challenge-the-real-story-of-a-corrupted-military-exercise-and-its-legacy/>.
7. Ibid.
8. Ibid.
9. Michelle Tan, “Combat Training Rotation Will Increase to 18 Days,” Your Army, *Army Times*, February 6, 2015, <https://www.armytimes.com/news/your-army/2015/02/06/combat-training-rotations-will-increase-to-18-days/>.
10. In Stock Games, GMT Games, updated June 25, 2024, <https://www.gmtgames.com/s-3-in-stock-games.aspx>.
11. Sebastian Bae, “Just Let Them Compete: Raising the Next Generation of Wargamers,” War on the Rocks, October 9, 2018, <https://warontherocks.com/2018/10/just-let-them-compete-raising-the-next-generation-of-wargamers/>.
12. Ibid.
13. Ibid.
14. Ibid.
15. “Wargame,” Board Game Geek, <https://boardgamegeek.com/boardgamecategory/1019/wargame/>.
16. Perla, *The Art of Wargaming*, 27.
17. Sebastian Bae, “Put Educational Wargaming in the Hands of the Warfighter,” War on the Rocks, July 13, 2023, <https://warontherocks.com/2023/07/put-educational-wargaming-in-the-hands-of-the-warfighter/>.
18. Richard Borg, *Memoir ‘44* (Days of Wonder, 2004), board game, <https://www.daysofwonder.com/memoir-44/>. *Memoir ‘44* is a war-themed strategy board game based on the D-Day landing and liberation of France; Christian T. Petersen, Corey Konieczka, and John Goodenough, *Tide of Iron* (Fantasy Flight Games, 2007), board game, [http://www.fantasyflightgames.com/edge\\_minisite.asp?eidm=8&enmi=Tide%20of%20Iron](http://www.fantasyflightgames.com/edge_minisite.asp?eidm=8&enmi=Tide%20of%20Iron). *Tide of Iron* is a World War II based tactical conflict wargame focused on the struggle between American and German forces in Northern Europe during 1944 and 1945; and Alessio Cavatore and Rick Priestley, *Bolt Action* (Warlord Games, 2014), tabletop wargame, <https://www.boltaction.com>. *Bolt Action* is a tabletop, miniatures wargame set during famous battles of World War II.
19. *Standard Combat Series* (Multi-Man Publishing, 1993–2023) simulation wargame, <https://mmpgamers.com/standard-combat-series-c-11>. *The Standard Combat Series* includes 26 individual map-based simulation wargames focused on World War I and II battles; and *World at War ‘85* (Lock ‘N Load Publishing, 2019–2024), board game, <https://store.lnlpublishing.com/world-at-war-85-series>. *World at War ‘85* includes two main board games with several expansions and companion products. It is a series of platoon-level combat games set in an alternate history of World War III across Europe in the mid-1980s.
20. *Next War* (GMT Games, 2012–2024) board game, <https://www.gmtgames.com/c-47-next-war-series.aspx>. *The Next War* series of games includes six main board games with several supplements that add new rules, scenarios, and expansions to these games.
21. *COIN* (GMT Games, 2012–2023) board game, <https://www.gmtgames.com/c-36-coin-series.aspx>. The *COIN* or counterinsurgency series includes 12 games and focuses on asymmetric conflict, covering both historical and contemporary scenarios.
22. *Mr. President: The American Presidency, 2001–2020* (GMT Games, 2022) board game, <https://www.gmtgames.com/p-1056-mr-president-the-american-presidency-2001-2020-2nd-edition.aspx>. *Mr. President* is a solo board game that spans four 1-year turns. It covers various aspects of presidential duties including domestic policy, international relations, and crisis management.
23. James Lacey, “How Does the Next Great Power Conflict Play Out? Lessons from a Wargame,” War on the Rocks, April 22, 2019, <https://warontherocks.com/2019/04/how-does-the-next-great-power-conflict-play-out-lessons-from-a-wargame/>.
24. Evan Yoak and Joe Chacon, *Decisive Action* (GMT Games, 2023) tabletop wargame, <https://www.gmtgames.com/p-1007-decisive-action.aspx>. *Decisive Action* is a tactical-level game focused on deep planning, tactical maneuver, and combat multipliers like artillery and electronic warfare.
25. Leo Barron, “Unveiling the Future of Gaming: *Decisive Action* Promises a Thrilling GMT Experience,” Inside GMT Games, February 7, 2024, <https://insidgmt.com/unveiling-the-future-of-gaming-decisive-action-promises-a-thrilling-gmt-experience/>.

CPT Christopher Schwenck is the S-2 for 3<sup>rd</sup> Battalion, 6<sup>th</sup> Field Artillery Regiment, 1<sup>st</sup> Infantry Brigade Combat Team, 10<sup>th</sup> Mountain Division (Light Infantry). He previously served as the executive officer for B Company, 24<sup>th</sup> Military Intelligence Battalion and as the platoon leader for the 66<sup>th</sup> Military Intelligence Brigade-Theater signals intelligence collection team in Wiesbaden, Germany. He holds a bachelor of arts in political science from Norwich University and a master of arts in government with a specialization in diplomacy and conflict studies through a graduate fellowship at the Interdisciplinary Center in Herzliya, Israel.

# Overcoming Obstacles to Cyberspace Threat Intelligence

by Chief Warrant Officer 2 Travis M. Whitesel  
and Mr. Joseph Rudell



*Discussion of the commercial products and services in this article does not imply any endorsement by the U.S. Army, the U.S. Army Intelligence Center of Excellence, or any U.S. government agency.*

*This article is primarily relevant to intelligence professionals supporting cyberspace operations at the U.S. Army Cyber Command and the U.S. Army Network Enterprise Technology Command. However, with the intelligence profession's continuing expansion and overlap into the cyberspace domain, the article will serve as a primer for discussion about obstacles facing those in the digital fight.*

## Introduction

The U.S. Army Network Enterprise Technology Command (NETCOM) G-2 is developing and implementing cyberspace threat intelligence (CTI) techniques to protect the Department of Defense Information Network-Army (DoDIN-A). However, current challenges with the incident management and reporting processes hinder the intelligence community's ability to provide relevant and predictive intelligence to drive operations. This article captures the lessons learned and obstacles identified by NETCOM G-2 while implementing new tactics, techniques, and procedures. The article also conveys recommendations assisting the signal community with enabling CTI for improved threat visibility within the cyberspace domain.

## Issues of the Cyberspace Domain

Current challenges with the cyberspace domain's incident management process include:

- ◆ Lack of investment in a unified toolset for incident management.
- ◆ Lack of standardization in the reporting process.
- ◆ Misunderstanding of the role of intelligence within the process.

These obstacles significantly hinder predictive analysis and an in-depth examination of the domain's problem sets. Resolving these problems will enable better protection and sustainment of the DoDIN-A.

**Lack of Investment in a Unified Toolset.** This failure to invest in a unified toolset for incident management significantly affects reporting procedures because the incident management instrument is different for each network provider. Government Accountability Office reporting highlights the problem, indicating that in spite of investing \$100 billion annually into information technology and cyberspace-related infrastructure, the federal government has yet to achieve effective results.<sup>1</sup> This failure to produce practical outcomes is partially a product of not learning from past mistakes. Each incident on the DoDIN is an opportunity to understand our visibility gaps, process failures, and configuration requirements. The approximate 12,000 cyberspace attacks against the Department of Defense (DoD) and defense industrial base since 2015 compound the issue, emphasizing the adversary's intent and capability.<sup>2</sup> (NETCOM G-2 assesses this number to be significantly higher.) A unified incident management toolset would provide insight into the process failures and the threat's intent and capability, which would further improve the Army's response through subsequent analysis. The incident management toolset is the primary entry point to capture information about cyberspace attacks. Both industry and the various service components have proposed unified toolsets; however, to date they have not captured requirements to collect the relevant information to enable future analysis and data sharing.

**Lack of Standardization in the Reporting Process.** This failure to standardize incident management reporting requires analysts to apply more strenuous analytic rigor to identify factors for creating relevant and timely intelligence. Additionally, employing multiple toolsets coupled with the required fields and descriptions of incidents varies across the DoDIN-A enterprise. These problems degrade the ability to diagnose an incident with structured analytic techniques.

The 12,000 documented cyberspace attacks since 2015 should serve as a foundation for understanding cyberspace threat capabilities, common targets, and trends in threat avenues of approach. However, the information available in official repositories about these attacks is principally limited to incident response actions and status without addressing the attack's techniques, targets, and key indicators. When an attack occurs in the physical domain, the operational report includes all available information, including the number of enemy personnel, potential descriptions, their capabilities, when and how the attack occurred, and descriptions of any related artifacts. To be effective in the cyberspace domain, operatives must capture the same level of detail about cyberspace attacks. Through standardization of the incident management reporting process, CTI will improve the defense of the DoDIN-A.

**Misunderstanding of the Role of Intelligence.** Integrating intelligence into incident management processes is essential, and the Army must actively implement procedures to include it. One critical obstacle to implementation is the inability of intelligence professionals to access and complete incident records in a timely manner. This is attributable to a misunderstanding of the role of intelligence in the incident management process. The incident management and intelligence processes overlap and have similar activities intended for different purposes. (See figure on the next page.) The main difference is that, while incident management in cyberspace operations aims to respond to and eradicate the current threat, intelligence personnel want to exploit and analyze the information to answer intelligence requirements and reduce *future* threats. Concerns about impacting ongoing cyberspace operations or intelligence oversight lead to hesitation in allowing intelligence analysts to view DoDIN-A data. However, the areas of operations are friendly networks and incident management data, which have limited risk of exposing identifying information, with regulations and processes for handling evidence involving U.S. persons or operational requirements.

Incident response operations narrowly focus on resolving the immediate incident. Often, the process merges into the next incident without anyone conducting a structured analysis to capture details or create an understanding of the incident in a broader context relating to the DoDIN-A. Integrating intelligence into the incident management process allows the information obtained during an investigation to be stored,

contextualized, and exploited without the time constraints of preparing for the next operational response. By design, the intelligence process will capture information and identify data gaps overlooked in the initial operational response and provide a more detailed understanding of the Army's visibility gaps in context with DoDIN-A threats. In conjunction with the incident management process, this analysis will help prioritize defensive measures for the DoDIN-A while making educated risk decisions.

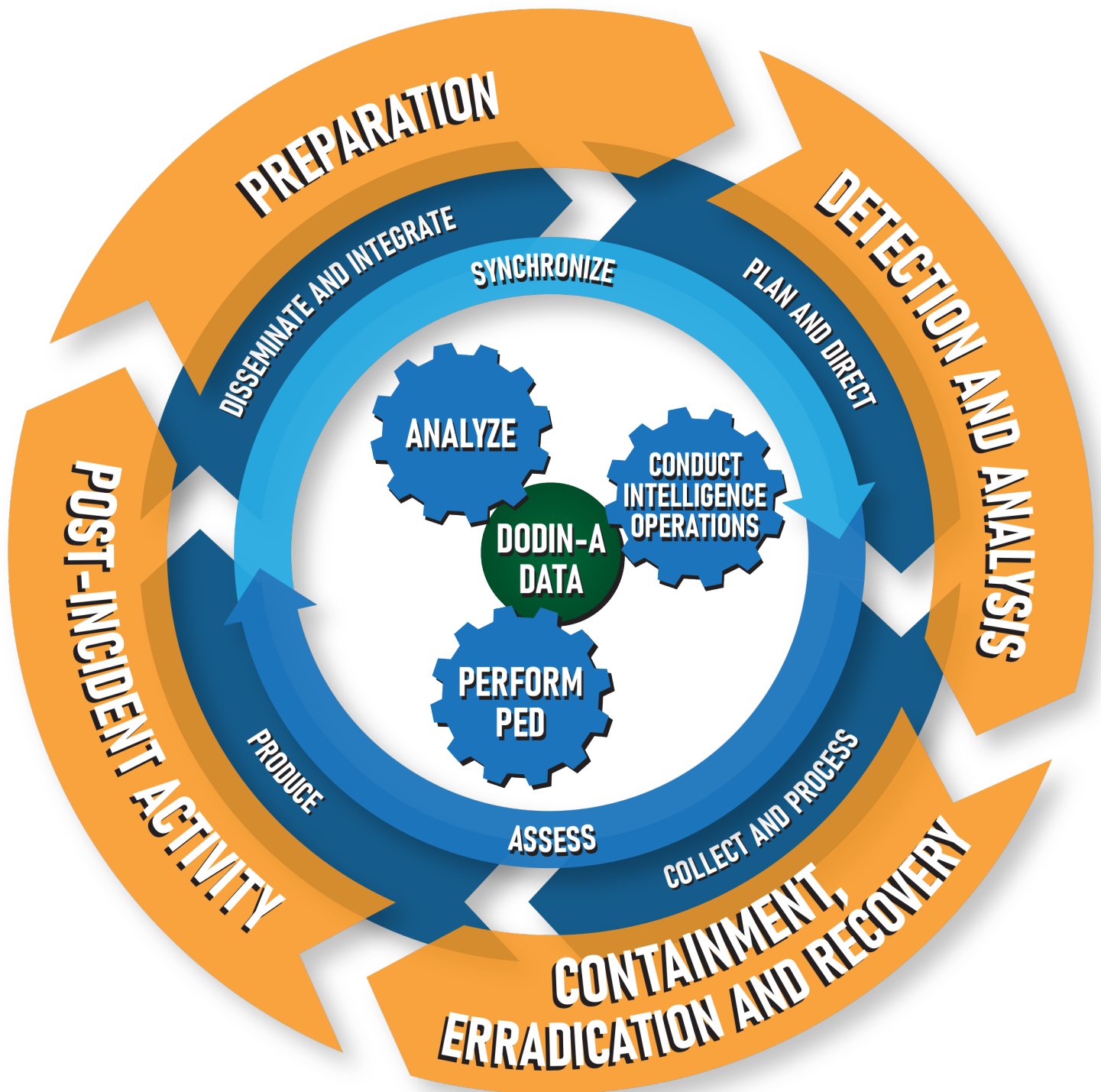
## **Successes in the Commercial Environment**

CTI's successes in the commercial domain provide lessons learned and operating guidelines for the Army to consider when developing its own CTI organizations and techniques. Commercial environment CTI teams often include individuals with a variety of skill sets who perform multiple roles simultaneously. In 2018, Microsoft Corporation revealed that their CTI team included, among other professionals, a lawyer, a traditional intelligence analyst, an experienced cyberspace analyst, and a technical writer. Other organizations incorporate unique skill sets within their CTI teams tailored to their work environments. The Army has well-defined incident management processes, but a variety of specific laws and regulations impose unique constraints. Collaboration within the limits of those constraints, however, can expedite CTI and speed implementation of commercial processes. Based on the NETCOM G-2's experience, when choosing the correct commercial process to adopt, one that nests CTI into a security operations center can overcome the need for individual analysts with multiple roles or individuals with specialized skill sets.

Another commercial CTI advantage is access to multiple data sets for analysis and enemy detection. This allows commercial CTI analysts to corroborate data sets, which delivers significantly more context to incidents and can shorten the time to understand the complex environment.<sup>3</sup> Access to operational data is a key enabler for commercial CTI operations and provides better defenses for protecting their respective networks. The commercial sector successfully highlights the importance of incident management data for completing CTI tasks, which the Army can leverage for success.

The commercial CTI sector has access to functional toolsets that assist in discerning complex information. Often, one incident management service provides the data. The commercial sector's capability to standardize incident management data and conform it to a singular toolset provides CTI professionals with familiarity and superior functionality.<sup>4</sup> This allows the commercial sector to calibrate toolsets to their mission, taking advantage of professionals with longevity within the company. These commercial successes emphasize the DoD's need to adopt a unified incident management system. They also underscore the necessity of employing a toolset and environment that allows the analyst to access, manipulate, and move information to support their mission.





#### LEGEND

**DODIN-A PED** Department of Defense Information Network-Army processing, exploitation, and dissemination

**INCIDENT MANAGEMENT PROCESS**

**INTELLIGENCE PROCESS**

Overlap of the Intelligence and Incident Management Processes<sup>5</sup>

## Integrating Cyber Threat Intelligence

Although many of the analytical techniques and processes used in commercial CTI originated with military intelligence, the Army can benefit from leveraging commercial processes because of that sector's sustained and documented successes. Several companies offer CTI techniques to deter adversaries operating on a network and improve sensors for hardening a network. The Army can successfully integrate commercial CTI structures without completely reworking current organizational structures. A dedicated effort by the Army to unify toolsets and standardize processes can significantly impact the visibility and security of the cyberspace domain. One way to accomplish this is to introduce and apply structured analytic techniques.

Intelligence professionals are already familiar with structured analysis. They use cognitive processes and analytic tools and techniques to solve intelligence problems. Multiple cybersecurity structured analytic techniques exist that can serve as a common language between the cyberspace and the intelligence communities. These include the MITRE ATT&CK Matrix, the Cyber Kill Chain, and the Diamond Model. These frameworks and techniques provide a baseline for communication and improve how intelligence professionals and cyberspace defenders approach cyberspace incidents.

Mapping an attack through the MITRE ATT&CK Matrix framework empowers analysts to communicate how an adversary attempts to penetrate the network.<sup>6</sup> It can provide the intelligence community with a way to structure adversary capabilities quickly, identify how they apply to friendly networks, and present that information to cyberspace defenders. Implementing a common language between incident management and intelligence will result in a better understanding of attacks against the DoDIN-A and provide data in a structure that analysts can leverage to prioritize network defense, identify future capability requirements, and enable proactive decisions by leadership.


An integral component of Lockheed Martin's Intelligence Driven Defense model, the Cyber Kill Chain provides intelligence analysts with a method to examine cyberspace attacks and advise cyberspace operators on adversarial actions targeting friendly networks. It is a framework that deconstructs a cyberspace attack into seven steps to understand the adversary's actions and objectives.<sup>7</sup> Viewing intrusions through the lens of the kill chain ensures cyberspace defenders capture all relevant information about an attack. A detailed kill chain allows intelligence analysts to use the same information to conduct trend analysis on successful threat techniques and friendly visibility gaps. Mapping an attack to gain visibility of flaws is critical for enabling the Army to prevent future attacks.

The Center for Cyber Threat Intelligence and Threat Research created the Diamond Model of Intrusion Analysis to depict

cyberspace attacks.<sup>8</sup> The tool relies on four different subsets of an attack: infrastructure, victim, capability, and adversary. Viewing an intrusion through this framework allows analysts to provide context to an attack through behavioral and technical choices. This strategy reveals similarities between attacks and enables intelligence professionals to identify related incidents, differentiate possible threat relationships, and identify unique traits. These capabilities are especially important because a sizable proportion of intrusions remain unattributed. The Diamond Model, when coupled with the Cyber Kill Chain, enables in-depth questioning of incident data, which can support operational and strategic requirements.

Combining these three structured analytical techniques—the MITRE ATT&CK Matrix, the Cyber Kill Chain, and the Diamond Model—provides a foundational process to gain an advantage in the cyberspace domain and capture quantifiable data to which analysts can apply analytical methods, an approach that is currently missing from DoDIN-A operations and the intelligence enterprise. These commercial techniques can help address a CTI shortfall left by a gap in regulations, training, and doctrine. The Army intelligence community can benefit from using these additional structured analytic techniques to expand the incident management and reporting processes, thereby enriching data with threat context as operations in the cyberspace domain are further developed. Integrating structured analytic techniques into cyberspace and intelligence operations sets the stage for defining requirements for a unified toolset and serves as the basis for standards.

## Conclusion

The Army faces continuous competition and conflict in the cyberspace domain; the need for unified reporting structures and processes further challenges the Army to gain an information advantage. By implementing and enforcing structured analytic techniques, the Army can better exploit the information from the cyberspace domain to achieve strategic, operational, and tactical results. Using structured analytic techniques will also drive requirements for architectural and procedural standards needed to implement viable solutions. NETCOM G-2 is currently conducting training and implementing analytic techniques to improve network defenses and enhance incident management and reporting processes. NETCOM G-2 plans to capture their CTI tactics, techniques, and procedures and share them with the intelligence community. Developing and implementing CTI techniques will significantly improve the Army's defenses in the cyberspace domain because they enable a more proactive posture. 

## Endnotes

1. Government Accountability Office, *Information Technology and Cybersecurity: Significant Attention Is Needed to Address High-Risk Areas*, GAO-21-422T (Washington, DC, 2021), 1, <https://www.gao.gov/products/gao-21-422t>.

2. Government Accountability Office, *DoD Cybersecurity: Enhanced Attention Needed to Ensure Cyber Incidents Are Appropriately Reported and Shared*, GAO-23-105084 (Washington, DC, 2022), highlights, <https://www.gao.gov/products/gao-23-105084>.
3. Larry G. Wlosinski, "Cyberthreat Intelligence as a Proactive Extension to Incident Response," *ISACA Journal* 6 (Online Exclusive, November 2, 2021), <https://www.isaca.org/resources/isaca-journal/issues/2021/volume-6/cyberthreat-intelligence-as-a-proactive-extension-to-incident-response>.
4. Adam Zibak, Clemens Sauerwien, and Andrew Simpson, "A Success Model for Cyber Threat Intelligence Management Platforms," *Computers & Security* 111 (December 2021), <https://doi.org/10.1016/j.cose.2021.102466>.
5. Figure adapted from original by author, Joseph Rudell.
6. "ATT&CK," The MITRE Corporation, accessed June 27, 2023, <https://attack.mitre.org/>. An open knowledge base of adversary tactics and techniques based on real-world observations used for developing threat models and methodologies.
7. "Cyber Kill Chain," Cyber, Lockheed Martin, accessed June 27, 2023, <https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html>. A framework for understanding an adversary's cyber-attack tactics, techniques, and procedures.
8. Sergio Caltagirone, Andrew Pendergast, and Christopher Betz, *The Diamond Model of Intrusion Analysis* (Hanover, MD: Center for Cyber Intelligence Analysis and Threat Research, 2013), <https://apps.dtic.mil/sti/citations/ADA586960>.

CW2 Travis M. Whitesel is the U.S. Army Network Enterprise Technology Command (NETCOM) G-2 Regional Cyber Center Coordinator. He received his appointment as a warrant officer in February 2019 and served as an all-source intelligence technician for Delta Company, 65<sup>th</sup> Brigade Engineer Battalion, 2<sup>nd</sup> Infantry Brigade Combat Team, 25<sup>th</sup> Infantry Division. He holds a bachelor's degree from American Military University.

Mr. Joseph S. Rudell is a former Department of the Army Civilian Cyber Threat Intelligence Analyst. He led the NETCOM G-26 Cyber Threat Intelligence Team. He began his Army career in 2008 as a defense contractor with the Theater Network Operations and Security Center Continental United States (CONUS) performing intrusion analysis and later overseeing the U.S. Army CONUS sensor grid. He is currently a solutions integration engineer at the University of Arizona's College of Applied Science and Technology Cyber Convergence Center.

### Contributors

LTC Brian J. Lenzmeier, NETCOM G-2 Analysis and Control Element Chief

CPT Jason L. Scaglione, NETCOM G-2 Analysis and Control Element Deputy Chief

CW2 John W. Becker, Regional Cyber Center-Pacific Intelligence Support Element

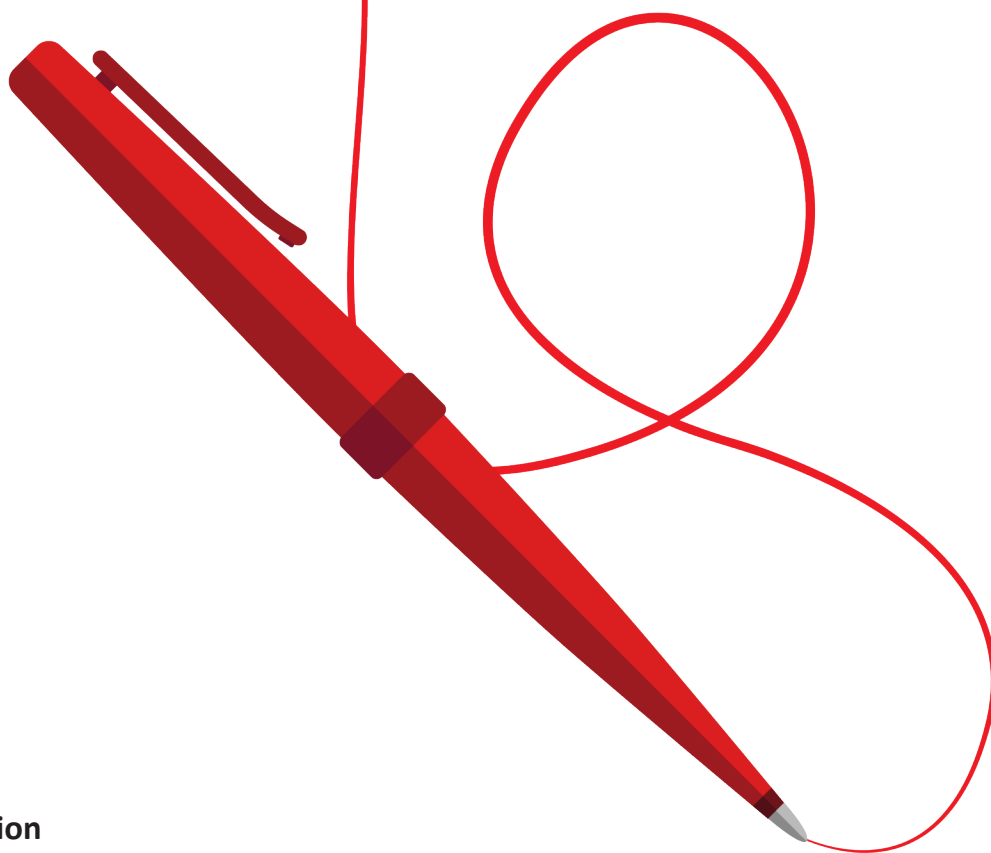
CW2 Jeff B. Newsome, Regional Cyber Center-Europe Intelligence Support Element

SFC Trestan Savoy, Regional Cyber Center-Pacific Intelligence Support Element



# Get Your Red Pen Ready.

*By Lieutenant Colonel Matthew J. Fontaine*



## Introduction

Everyone knows the S-2/G-2 must provide only two enemy courses of action (COAs) during the mission analysis brief, and it is a job well done. These two COAs, the most likely and most dangerous, provide the commander and staff with everything they need to know about how the threat will fight against friendly actions throughout the execution of a complex operation, right? Sure, we know that doctrine asks us to “identify the *full* set of courses of action available to the threat,”<sup>1</sup> but who does that?

The intelligence cell should do that, of course. This article recommends that intelligence cells continuously develop and refine three categories of enemy COAs, instead of the two standard most likely and most dangerous enemy COAs, to better account for the tactical and operational options available to a thinking enemy in large-scale combat operations.<sup>2</sup> Better enemy COAs result in better friendly plans. Better plans result in friendly forces more likely to seize opportunities or avoid disaster during the execution of operations. So, get your red pen ready! The three enemy COA categories are:

- ◆ Operational enemy COAs.
- ◆ Critical event enemy COAs.
- ◆ Transition enemy COAs.

Now, don't get me wrong. The intelligence cell must still designate the most likely and most dangerous enemy COAs, but they must do so for *each category*. Identifying the most likely and most dangerous enemy COAs is essential because they enable the commander to develop optimized friendly plans in environments that are often time constrained.<sup>3</sup> The staff then develops contingency options (think branches, sequels, or alternate COAs) should the enemy execute any other *valid COA* available to the threat for each category.<sup>4</sup> (I will discuss the value of the most likely and most dangerous designations in the context of the three enemy COA categories again near the conclusion of this article.)

In this article, I will explain why the typical enemy COAs drafted by many intelligence cells do not meet the challenges of large-scale combat operations. I will then describe each enemy COA category in detail. I will then conclude with a discussion on developing logical priority intelligence requirements (PIRs) to detect any valid enemy COA selected by the threat.

## The Problem with "Two and Done"

The standard two enemy COAs typically developed by intelligence cells often do not provide the complete conceptual narrative and details the commander and staff need to create an effective plan. Effective plans posture the unit to overcome the current enemy challenge *and* execute critical future transitions, like branches or sequels, without unnecessary risk.<sup>5</sup>

Enemy COAs often come up short because they try to provide too much information from the start but do too little to support the development of effective plans. This tendency is especially true for enemy COAs developed for command post exercises, large-scale combat operations scenarios at the division and higher echelons, or the initial COA a brigade creates before an Army combat training center rotation. Here is what I mean: the typical command post exercise or initial combat training center enemy COA often focuses on how the threat will achieve its operational or strategic end state from start to finish. I dub this enemy COA the *operational enemy course of action* (OECOA, pronounced OH COA); it

is an essential COA.<sup>6</sup> However, an operational enemy COA only tells part of the story to the commander and staff. The intelligence cell uses the operational enemy COA to portray how the enemy could achieve its overall mission and end state. It has limited utility for developing effective plans for two primary reasons.

First, an operational enemy COA cannot provide the necessary details for good staff work because it must cover so much ground, literally and figuratively. It is not uncommon for an operational enemy COA in a typical large-scale combat operations scenario to describe how an enemy division, corps, or even army will execute an entire operation—from invasion to the destruction of the friendly forces over hundreds or even thousands of square kilometers! Intelligence cells often describe an operational enemy COA using a single paragraph or PowerPoint slide. How valuable can this analysis be in supporting detailed, friendly planning?

Second, the intelligence cell drafts operational enemy COAs during mission analysis before developing friendly COAs. Given this arrangement, operational enemy COAs only consider opposing forces in the most general sense, as the detailed, friendly plan does not yet exist. From its inception, an operational enemy COA is of limited value because the intelligence cell did not construct it in relation to friendly actions.

But we know war, particularly large-scale combat operations, must be considered from both friendly and enemy perspectives. Carl von Clausewitz imagined war as a match between two wrestlers: "Each [wrestler] tries through physical force to compel the other to do his will; his *immediate* aim is to *throw* his opponent in order to make him incapable of further resistance."<sup>7</sup> Clausewitz's analogy evokes an image of a violent fight. One sees two competitors locked in a fierce back-and-forth struggle to gain advantage before one side imposes its will in a final tremendous effort to emerge victorious.

Our enemy COAs should account for this dynamic nature of war—but often, they do not. Instead, many intelligence cells develop operational enemy COAs without understanding the friendly plan. And how could this not be the case? S-2s/G-2s present enemy COAs during mission analysis before friendly COA development. Look at many operational enemy COAs (and friendly COAs, for that matter) to see how little we take our opponent's actions into account. Most enemy COAs have a few blue opponent icons or tasks at the end of a sequence of enemy steps as if the friendly forces were just along for the ride. Some include no friendly icons or tactical tasks at all!

Developing a friendly COA with just an operational enemy COA is akin to a wrestler preparing for a live opponent based solely on a session with a wrestling dummy.<sup>8</sup> Like wrestling against a dummy, typical operational enemy COAs provide no sense of the dynamic reactions and counteractions necessary to spur commanders' and staffs' thinking on how best

to design a friendly operation considering the complete set of options available to a threat. The limited utility of operational enemy COAs becomes readily apparent after being briefed during mission analysis. The S-2/G-2 receives a deluge of “how” questions from the commander and staff: how will the enemy react to a particular aspect or critical event of a friendly COA? How long will an enemy transition take? And so on.

I know what you think; the war game will address many of these questions. After all, the purpose of the S-2/G-2 during the war game is to project how the enemy will react to the friendly COA, including its constituting critical events.<sup>9</sup> But do they always? And how far do staff get during war gaming in time-constrained environments or under demanding conditions (if the war game even happens)? If a war game does occur, is the S-2/G-2 prepared to execute the basic war-gaming “action, reaction, and counteraction methods of friendly and enemy forces interaction”<sup>10</sup> for *every* critical event described in doctrine, armed with only a most likely and most dangerous operational enemy COA? I am not convinced based on my experience. Many of us have been guilty of using the same enemy COA paragraph or PowerPoint we initially showed during mission analysis for the operations order at the end of the military decision-making process (MDMP). We all agree that this should not occur if the command and staff truly wrestle with the problem presented by the enemy.

Suppose you are an S-2 or G-2 that comprehensively updates the intelligence preparation of the operational environment products at the end of war-gaming. (There should be significant changes, correct?) In that case, you are ahead of the game!

Whether or not you update your products, don’t you wish you had more depth in your enemy COAs before the war game so as not to provide shallow responses or, to put it politely, baloney? Or that you had better enemy COAs during mission analysis to give the commander and staff a better starting point for developing more comprehensive friendly COAs, branches, and sequels, with the idea that better input—both friendly and enemy—will result in a better war game output?

One thing is sure: no G-2 or S-2 wants to find themselves at a war game considering for the first time the enemy’s reaction to some critical event, like a wet gap crossing! The enemy fights to win in large-scale combat operations and will use every technically and tactically ingenious method to prevail. We must think deeply to beat these opponents, so broad enemy COAs alone will not cut it. The solution to providing better enemy COAs—and better friendly COAs as a result—is to start with the big picture.

## Operational Enemy Courses of Action

The first set of enemy COAs to develop are the operational enemy COAs. Even though I just seemingly maligned them, creating quality operational enemy COAs is essential to understanding the threat from a complete narrative perspective. Operational enemy COAs describe how the enemy might achieve its desired operational or strategic end state from start to finish, arranged along a line of operation (LOO). It is a conceptual product that lets the staff visualize how an enemy operation could evolve holistically. Operational enemy COAs are also essential to anticipating how enemy forces can enter and exit the unit’s deep area or flanks (a vital aspect for targeting and intelligence handover line coordination). The intelligence cell derives the operational enemy COAs from the enemy COAs developed by its higher headquarters.<sup>11</sup>

For example, a division’s analysis and control element derives its operational enemy COA from the corps enemy COAs, with a *slight* emphasis on the forces templated in the division’s area of operations (AO). I say slight because the purpose of the operational enemy COA is to gain a holistic understanding of the big picture, so focusing just on one’s own AO misses the point, potentially obscuring how the enemy in one’s area of interest (AOI) could present a risk to the mission or forces. Operational enemy COAs are the first enemy COAs presented during mission analysis and serve as the foundation for all future enemy COA development.

Importantly, if an intelligence cell has no higher enemy COAs on which to base its operational enemy COAs, that cell must produce them. If a unit disagrees with the enemy COAs of the higher team, it cannot simply change or ignore them. To do so would contravene the necessity of having a common understanding of the threat. Instead, every intelligence cell must collaborate through both staff and command channels to arrive at a common understanding of the threat with their higher headquarters before moving on with planning.

Figures 1–5 provide simplified examples of higher echelons’ enemy COAs and associated operational enemy COAs developed by the fictional YOUR UNIT. Ideally, the intelligence cell would produce multiple operational enemy COAs, each nested within the higher echelon’s read of the situation.

Operational enemy COAs frame the possible range of valid enemy COAs to include the most likely and most dangerous available to the threat based on the friendly’s understanding of the enemy’s mission, intent, key tasks, and end state within the AO and AOI. As mentioned, this is usually as far as intelligence cells get at the start of any large-scale combat operations scenario, but we know more is needed. Therefore, the next step is to develop more detailed enemy COAs. Key to this is understanding the likely critical event of a given LOO.

**Mission:** Enemy forces attack to seize OBJ RED (friendly capital city) to install a politically favorable regime.

**Enemy Commander's Intent:** Gain rapid control of OBJ RED while minimizing the loss of combat power.

**End State:**

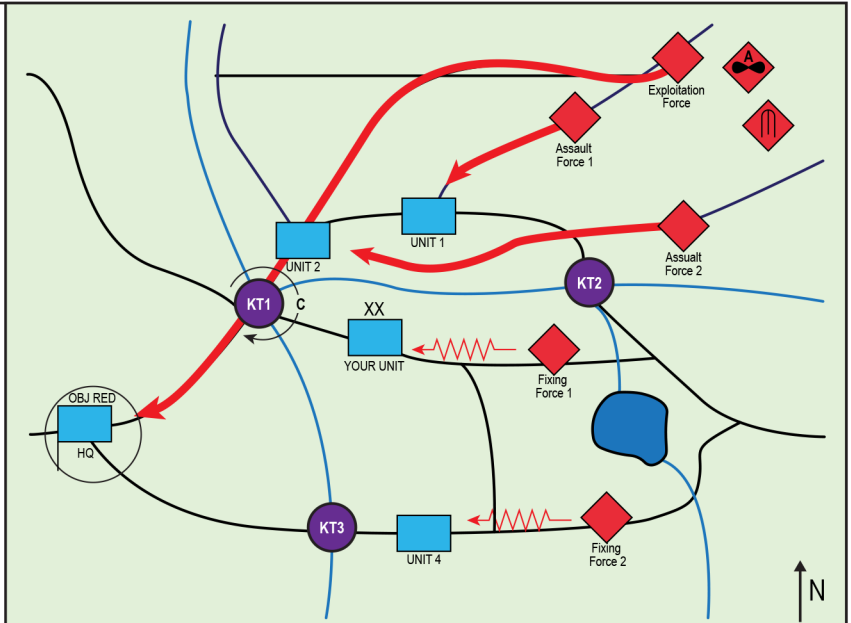
**Enemy:** Friendly forces cleared in OBJ RED.

**Friendly:** Combat effectiveness above 60% with an established area defense at OBJ RED to defeat the HIGHER FRIENDLY RESERVE.

**Terrain:** River crossing sites at KT 1, 2, 3, are intact.

#### LEGEND

COA	course of action
ECOA	enemy course of action
HQ	headquarters
KT	key terrain
OBJ	objective



This figure is a simplified representation of an ECOA YOUR UNIT may receive from its higher echelon. Enemy forces attack to seize OBJ RED, a friendly capital city. The enemy weights its efforts along the northern axis in this COA. The higher echelon designates this ECOA, ECOA 1 - HEAVY NORTH.

Figure 1. Higher Echelon Enemy Course of Action One: Heavy North<sup>12</sup>

**Mission:** Enemy forces attack to seize OBJ RED (friendly capital city) to install a politically favorable regime.

**Enemy Commander's Intent:** Gain rapid control of OBJ RED while minimizing the loss of combat power.

**End State:**

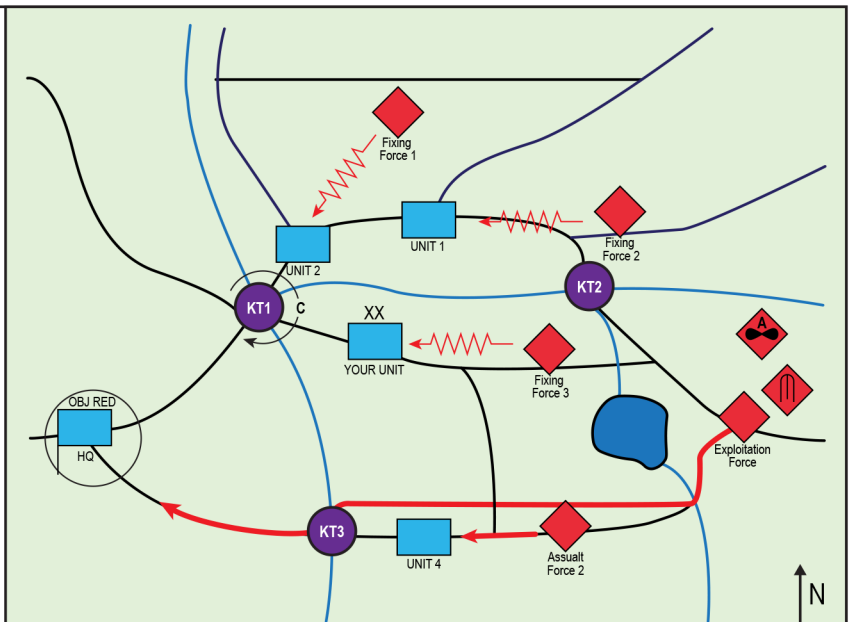
**Enemy:** Friendly forces cleared in OBJ RED.

**Friendly:** Combat effectiveness above 60% with an established area defense at OBJ RED to defeat the HIGHER FRIENDLY RESERVE.

**Terrain:** River crossing sites at KT 1, 2, 3, are intact.

#### LEGEND

COA	course of action
ECOA	enemy course of action
HQ	headquarters
KT	key terrain
OBJ	objective



This figure is a simplified representation of a second ECOA a unit may receive from its higher echelon. Enemy forces attack to seize OBJ RED, a friendly capital city. The enemy weights its efforts along the southern axis in this COA. The higher echelon designates this ECOA, ECOA 2 - HEAVY SOUTH.

Figure 2. Higher Echelon Enemy Course of Action Two: Heavy South<sup>13</sup>



**Mission:** Fixing Force 1 attacks to fix YOUR UNIT to prevent the massing of combat power on the Exploitation Force in the northern axis.

**Enemy Commander's Intent:** Rapidly fix YOUR UNIT with limited infrastructure damage.

**End State:**

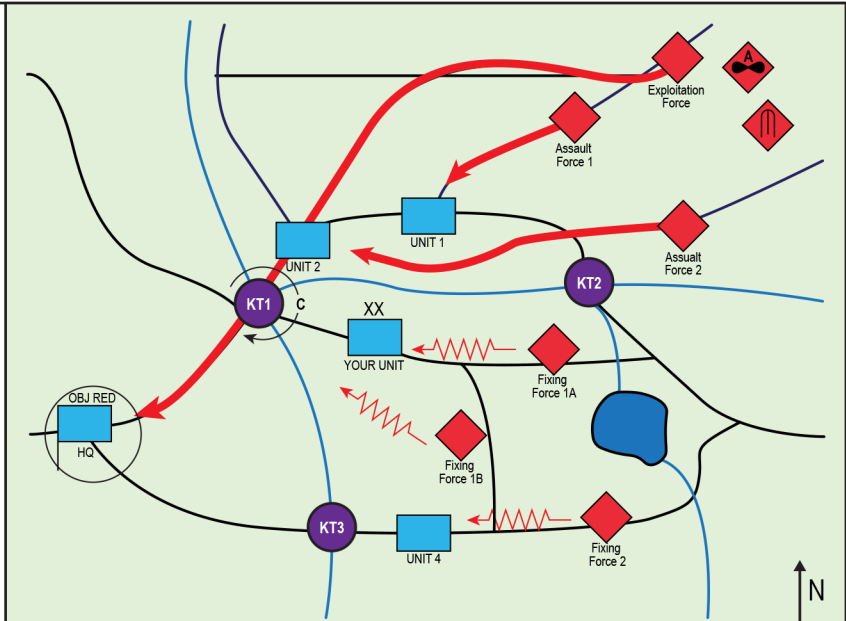
**Enemy:** Friendly forces unable to interfere with the seizure of OBJ RED.

**Friendly:** Combat effectiveness above 60% and postured to conduct wet gap crossing.

**Terrain:** The river crossing site at KT 1 is intact.

#### LEGEND

AO	area of operation
COA	course of action
EOCA	enemy course of action
HQ	headquarters
KT	key terrain
OBJ	objective
OEOCA	operational enemy course of action



This figure is a simplified representation of an OEOCA YOUR UNIT developed. Enemy forces attack to seize OBJ RED, a friendly capital city. The enemy weights its efforts along a northern axis in this COA. In the YOUR UNIT AO, Fixing Force 1 attacks to fix YOUR UNIT to prevent the massing of combat power on the Exploitation Force in the northern axis. YOUR UNIT designates this ECOA, OEOCA 1 - HEAVY NORTH, SOUTHERN FIX. YOUR UNIT adds additional detail to OEOCA 1, represented here by the delineation of Fixing Force 1 into Fixing Force 1A and 1B while ensuring OEOCA 1 is nested within the higher echelon's ECOA 1.

Figure 3. Operational Enemy Course of Action One: Heavy North, Southern Fix<sup>14</sup>

**Mission:** Fixing Force 3A attacks to fix YOUR UNIT to prevent the massing of combat power on the Exploitation Force in the southern axis.

**Enemy Commander's Intent:** Rapidly fix YOUR UNIT with limited infrastructure damage.

**End State:**

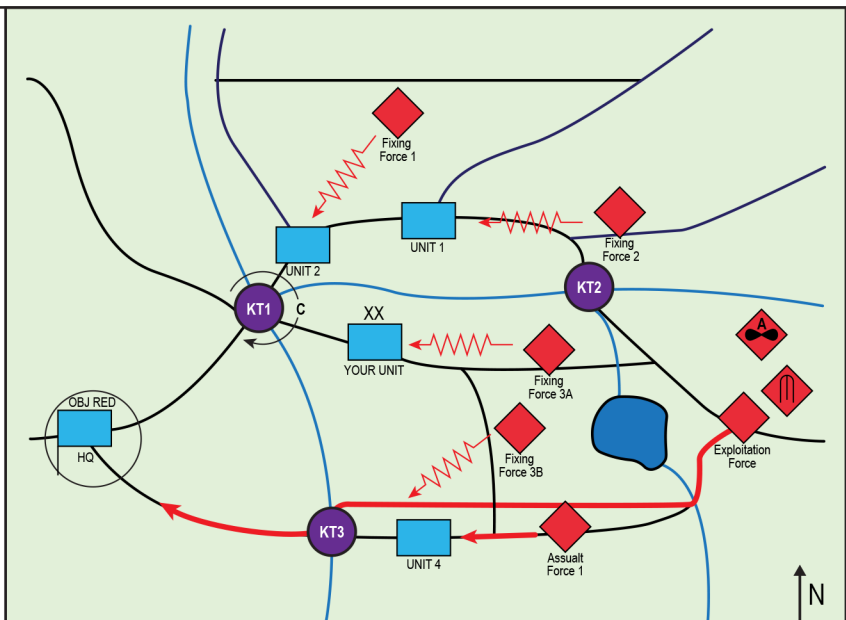
**Enemy:** Friendly forces unable to interfere with the seizure of OBJ RED.

**Friendly:** Combat effectiveness above 60% and postured to conduct wet gap crossing.

**Terrain:** The river crossing site at KT 1 is intact.

#### LEGEND

AO	area of operation
COA	course of action
EOCA	enemy course of action
HQ	headquarters
KT	key terrain
OBJ	objective
OEOCA	operational enemy course of action



This figure is a simplified representation of a second OEOCA YOUR UNIT developed. Enemy forces attack to seize OBJ RED, a friendly capital city. The enemy weights its efforts along the southern axis in this COA. In the YOUR UNIT AO, Fixing Force 3A attacks to fix YOUR UNIT to prevent the massing of combat power on the Exploitation Force in the northern axis. YOUR UNIT designates this ECOA, OEOCA 2 - HEAVY SOUTH, SOUTHERN FIX. YOUR UNIT adds additional detail to OEOCA 2, represented here by the delineation of Fixing Force 3 into Fixing Force 3A and 3B while ensuring OEOCA 2 is nested within the higher echelon's ECOA 2.

Figure 4. Operational Enemy Course of Action Two: Heavy South, Southern Fix<sup>15</sup>

**Mission:** Assault Force 1 attacks to defeat YOUR UNIT to enable the Exploitation Force seizure of OBJ RED in the southern axis.

**Enemy Commander's Intent:** Rapidly defeat YOUR UNIT with limited infrastructure damage.

**End State:**

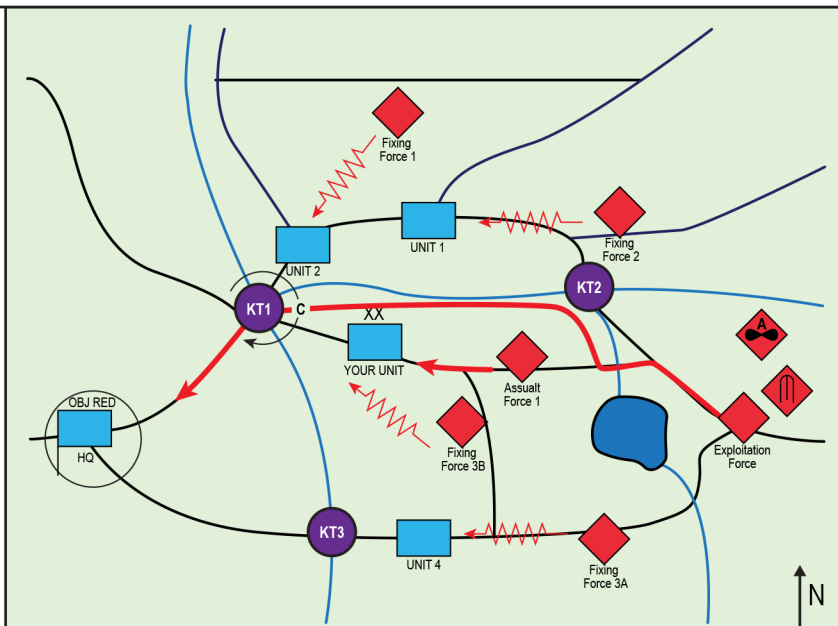
**Enemy:** YOUR UNIT unable to interfere with the seizure of OBJ RED.

**Friendly:** Combat effectiveness above 60% and postured to conduct wet gap crossing.

**Terrain:** The river crossing site at KT 1 is intact.

#### LEGEND

AO	area of operation
COA	course of action
ECOA	enemy course of action
HQ	headquarters
KT	key terrain
OBJ	objective
OECO	operational enemy course of action



This figure is a simplified representation of a third OECO YOUR UNIT developed. Enemy forces attack to seize OBJ RED, a friendly capital city. The enemy weights its efforts along the southern axis in this COA. In the YOUR UNIT AO, Fixing Force 3B attacks to fix YOUR UNIT. Once fixed, Assault Force 1 attacks to defeat YOUR UNIT to enable the seizure of OBJ RED by the Exploitation Force. YOUR UNIT designates this ECOA, OECO 3 - HEAVY SOUTH, SOUTHERN DEFEAT. YOUR UNIT modifies OECO 2, represented here by shifting the avenue of approach of the Exploitation Force within the southern axis, to account for the possibility of the main attack against YOUR UNIT.

Figure 5. Operational Enemy Course of Action Three: Heavy South, YOUR UNIT Defeated<sup>16</sup>

## Critical Event Enemy Courses of Action

The second set of enemy COAs to develop is what I will dub *critical event* enemy COAs (CECOA, pronounced “SEE COA”). Critical event enemy COAs are like the “snapshots in time” situation template described in doctrine that represent a “potential threat COA as part of a particular threat operation.”<sup>17</sup> Like a situation template, a critical event enemy COA describes how the enemy might achieve its desired *tactical* end state in pursuit of its *operational* end state. The difference between a critical event enemy COA and a situation template is that a critical event enemy COA emphasizes the anticipated enemy COA’s *relationship* to the anticipated friendly COA or action during a specific critical event. Critical event enemy COAs are detailed products that enable the staff to visualize the separate ways (actions, reactions, and counterreactions) the enemy will seek to gain the advantage (win) during a particular portion of a LOO given a friendly action.<sup>18</sup> Critical event enemy COAs ensure we approach enemy COA development from the back-and-forth perspective of Clausewitz’s wrestlers.

For example, imagine the LOO in figure 6 (on the next page) associated with a simple operational enemy COA and a *failure* operational enemy COA (more on failure COAs later). The example LOO has three critical events with these possible friendly actions and enemy counteractions:

- ◆ Critical Event 1.
  - ◆ Friendly Action: Seize OBJECTIVE ONE (Capital City).
  - ◆ Enemy Counteraction: Defend OBJECTIVE ONE.

The enemy can defend OBJECTIVE ONE broadly via a maneuver defense (CECOA 1 for CE 1) or an area defense to retain the capital (CECOA 2 for CE 1).

#### ◆ Critical Event 2.

- ◆ Friendly Action: Execute Wet Gap Crossing.
- ◆ Enemy Counteraction: Defeat Wet Gap Crossing.

The enemy can defend key crossing sites of the wet gap via an area defense (CECOA 1 for CE 2) or, broadly, via a maneuver defense (CECOA 2 for CE 2).

#### ◆ Critical Event 3.

- ◆ Friendly Action: Seize OBJECTIVE TWO.
- ◆ Enemy Counteraction: Defend to retain OBJECTIVE TWO. (CECOA 1 for CE 3) or retrograde (CECOA 2 for CE 3).

This is simple stuff. The intelligence cell develops multiple *initial* critical event enemy COAs for each critical event to present during the mission analysis brief that they refine throughout the MDMP. The S-2/G-2 designates each critical event enemy COA as the most likely, most dangerous, or some other valid enemy COA for that critical event. The result is that the S-2/G-2 will develop the most likely and most dangerous critical event enemy COAs (and other valid critical event enemy COAs) for the most likely operational enemy COA, and the same goes for the most dangerous critical event enemy COA (and other valid operational enemy COAs). Given the already high demands on an intelligence cell for the mission analysis brief, this is a tall order, but it will pay dividends. If not possible, the intelligence cell should begin developing or refining critical event enemy COAs immediately after the mission analysis brief as the friendly plan takes form. The enemy critical events will likely be a mirror image of the friendly anticipated critical events.

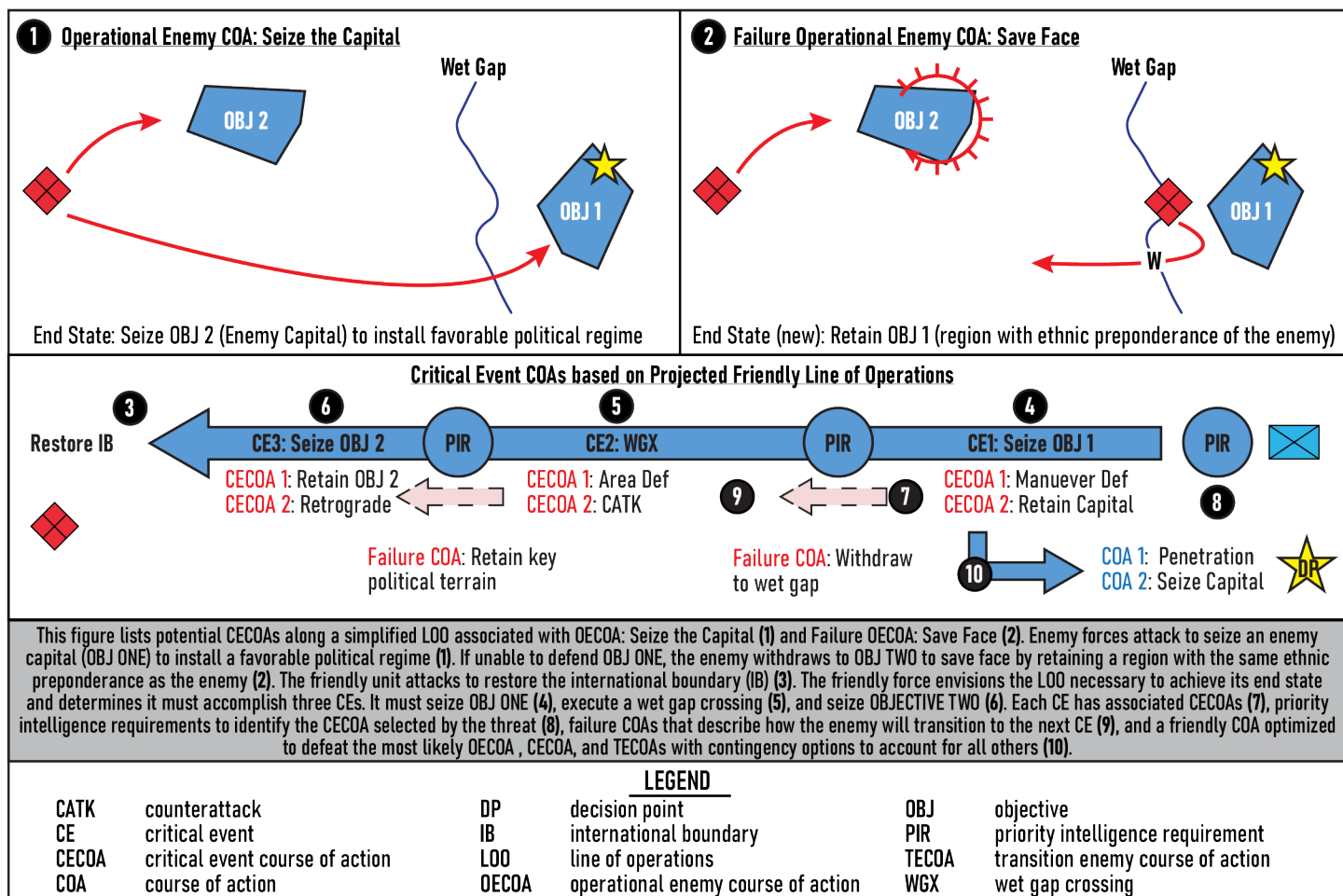


Figure 6. Simplified Line of Operations<sup>19</sup>

How can the S-2/G-2 recognize friendly actions during mission analysis to develop the initial critical event enemy COAs when COA development has not started? My advice is not to overthink the initial critical event enemy COAs. If a piece of key terrain is essential enough for the enemy to defend it, friendly forces will likely have to seize it. If a large river flows through the AO, both sides may have to cross it. Therefore, it becomes necessary for the intelligence cell to describe how enemy forces would react to friendly actions at that objective if the staff is to build an effective plan. Hopefully, in their initial planning guidance, the higher echelon's order or the unit commander will identify or at least indicate likely critical events for the unit. If not, ask the commander and staff to get thinking!

If prepared correctly, the critical event enemy COAs will supercharge friendly COA development after mission analysis. The staff will better understand the risk to the mission and force during critical aspects of the overall operation from the start within the context of the general enemy's operation, thanks to the operational enemy COA. Critical event enemy COAs also focus on the detailed planning of all warfighting functions in more concrete situations within the larger enemy and friendly picture. For example, given a particular critical event enemy COA, a member of the protection cell will have to think deeply about how to shield forces during

a wet gap crossing while staying nested within the general scheme of protection for the overall friendly COA, which itself is designed to account for the most likely operational enemy COA. Detailed planning like this is essential to understanding and mitigating risk.

Critical event enemy COAs are the intelligence cell's primary input to the war game; the war game refines them. Providing draft critical event enemy COAs during mission analysis ensures that the staff has already had an opportunity to think deeply about the valid, serious problems the unit will likely encounter during different portions of the operation, including the most likely and most dangerous ones. Quality critical event enemy COAs ensure that the COA analysis of the MDMP includes a genuine war game instead of what can be a series of ad hoc responses to inch-deep tactical dilemmas.

The next step is to consider what happens if the threat fails (or succeeds) in achieving its objectives.

## Transition Enemy Courses of Action

The third set of enemy COAs to develop is what I will dub the *transition* enemy COA (TECOA, pronounced "TEE COA"). A transition enemy COA anticipates what actions the enemy might take initially if unable to achieve a critical event on its LOO. Or, a transition enemy COA might envision how an enemy could seize an opportunity because the enemy completed

**Failure transition enemy course of action.** The failure transition enemy COA describes how the enemy will attempt to regain the conditions necessary to achieve the current end state described in the operational enemy COA or a modified end state based on the new battlefield realities.<sup>20</sup> Stated another way, the failure transition enemy COA describes how the threat will *transition* from a state of relative disadvantage to a situation of relative advantage to the friendly force.<sup>21</sup> The Save Face COA in figure 6 is an example of a transition enemy COA at the operational level. The enemy sought to seize OBJECTIVE ONE but transitioned to retaining OBJECTIVE TWO when it could not. Remember: the enemy constantly fights to win, and our enemy COAs must always reflect this.

Figures 7 and 8 (on the next page) provide simplified examples of transition enemy COAs developed by the fictional YOUR UNIT. Ideally, the intelligence cell would produce multiple transition enemy COAs for each operational enemy COA and critical event enemy COA while also designating the most likely and dangerous instances.

One staff only designs a plan for crossing the wet gap against the threat described in the critical event enemy COA. This isn't bad; it's certainly better than only planning against an operational enemy COA or only planning for the critical event enemy COA after publishing the base operations order. But, as we will see with the following staff scenario, a critical event enemy COA only improves a friendly plan by so much.

Here is where things get interesting. A third staff receives a wet gap critical event enemy COA and a *failure* transition enemy COA. The commander and staff listen with great interest







their approach if they want to win. The wrestler expects their opponent to do the same. Notably, some wrestlers may only commit to an initial approach once the match begins, when both opponents first receive cues about what the other might do. However, as a rule, we expect those wrestlers who have planned and prepared for alternate approaches to win more matches.

We can draw three simple points from the wrestling analogy to inform the development of PIRs. First, planning and preparation are essential even in uncertain environments.<sup>25</sup> Second, the uncertain nature of war is partially due to the sometimes unpredictable outcomes resulting from the clash or posturing of forces. We cannot predict with 100 percent accuracy how we or our opponent will react or counteract in a situation. Third, because both sides approach war knowing that they select COAs based on many friendly, enemy, and environmental factors, it would be foolish to assume that our opponent has already determined what they will do from the start. Instead, the enemy may keep their options open for as long as possible. In other words, we cannot tell what COA our opponent will pick with complete certainty from the get-go because the enemy may still need to commit to a decision or may transition to an alternate COA partway through execution. Because forces react unpredictably and can make decisions based on a wait-and-see attitude, units must develop collection plans that constantly scan the environment for multiple enemy COA possibilities. Commanders and staff cannot simply pick one enemy COA and ignore the rest—or they do so at their peril.

Staff must design PIRs to determine what the enemy is doing now (critical event enemy COA), next (transition enemy COA), and within the big picture (operational enemy COA) to reduce the unavoidable uncertainty of war. PIRs ensure units use their scarce collection assets to answer the commander's most important questions.<sup>26</sup> What else would be worth prioritizing our limited collection assets against than determining what COA the enemy is undertaking or will undertake (besides support to targeting to enable our selected COA)? Nothing in my mind.

The description of a PIR offered in FM 3-0, *Operations*, supports this reasoning. FM 3-0 states that PIRs “identify information about the threat and operational environment that a commander considers most important to making decisions in a specific context.”<sup>27</sup> Certainly, the set of enemy COAs described in this paper qualifies as requiring friendly decisions!

However, the straightforward process of drafting PIRs to identify which enemy COAs the enemy selects breaks down too often. Many PIRs (even well into execution) often say nothing of enemy COAs at all and instead use generic or unhelpful statements like:

- ◆ PIR 1: Where will the enemy employ its reconnaissance?
- ◆ PIR 2: Where will the enemy employ its fires?

Knowing where the enemy reconnaissance or fire assets are located is beneficial, but why? Read on.

Let's return to our wet gap crossing example. Recall that our third staff worked through the whole gamut of enemy COAs. The intelligence cell prepared critical event enemy COAs for the threat's anticipated defense: a failure transition enemy COA if the threat could not defeat the friendly crossing operation and had to withdraw, and a success transition enemy COA if the enemy defeated the crossing operation and transitioned to the offense.

To provide support for the commander's decision making, a better set of simplified PIRs for this phase of the friendly operation might look like this:

- ◆ PIR 1: Will the enemy conduct an area defense (critical event enemy COA 1) or maneuver defense (critical event enemy COA 2) to oppose a friendly wet gap crossing? Friendly Decision: Execute a COA to defeat the most likely critical event enemy COA 1 option with a contingency option should the threat adopt the second, less likely COA. (This PIR may be broken into two separate requirements).
- ◆ PIR 2: Is the enemy transitioning to defensive operations east of the wet gap (failure transition enemy COA)? Friendly Decision: Pursue withdrawing forces and disrupt defensive preparations in depth (success sequel COA).
- ◆ PIR 3: Is the enemy transitioning to offensive operations west of the wet gap (success transition enemy COA)? Friendly Decision: Execute a defense west of the wet gap (failure sequel COA).

Instead of looking for reconnaissance or fires assets as the sole purpose of collection as we did in the first sample set of PIRs, these examples focus collection efforts to broadly identify what the enemy is doing (enemy COA). Collection still looks for fires and reconnaissance assets, in addition to other critical systems and activities, but now they serve as indicators to support the assessment of which COA the enemy is executing. Next (or concurrently, if possible), the unit focuses collection via additional PIRs to target assets on the high payoff target list, which enables the execution of the optimized friendly COA. Too often, the tendency is to jump right into targeting without understanding what the enemy is trying to do as a combined arms team, both operationally and tactically.<sup>28</sup> The collection approach represented in the second set of PIRs fixes that.

For any operation, a generic PIR framework that considers the uncertainty inherent to large-scale combat operations would look like figure 9 (on the next page). While seemingly complicated, it has clear advantages over the standard two-and-done enemy COAs often generated at the start of many large-scale combat operations scenarios. Figure 10 (on the next page) suggests how to keep the number of PIRs more manageable throughout an operation's execution.

PIR	Most Likely OEEOA	Most Dangerous OEEOA	Other Valid OEEOA
<b>Step 1: Determine the OEEOA the enemy will execute</b>			
#1	Will the enemy execute the most likely OEEOA—or-	...the most dangerous OEEOA —or-	...some other valid OEEOA X (as necessary)
<b>Step 2: Determine the CEEOAs the enemy will execute nested within each OEEOA</b>			
#2-X (X is critical events)	Will the enemy execute the most likely, most dangerous, or other valid CEEOA for the most likely OEEOA	Will the enemy execute the most likely, most dangerous, or other valid CEEOA for the most dangerous OEEOA	Will the enemy execute the most likely, most dangerous, or other valid CEEOA for all other valid OEEOAs
<i>Note: Some CEEOAs may be the same or similar across the Most Likely, Most Dangerous, and other Valid OEEOAs</i>			
<b>Step 3: Determine the TEEOAs the enemy will execute at the operational level (OEEOA) and by critical event</b>			
#X+1	Will the enemy execute a failure or sequel TEEOA during the most likely OEEOA	Will the enemy execute a failure or sequel TEEOA during the most dangerous OEEOA	Will the enemy execute a failure or sequel TEEOA during all other valid OEEOAs
<i>Note: S-2 and G-2s should prioritize TEEOA development at the operational level (OEEOA) and work TEEOAs by critical event as they can because the operational TEEOA will likely be associated with enemy failure or success at some critical event</i>			
This figure demonstrates a PIR framework that takes the most likely, most dangerous, and all other valid EOAs of the three categories into account (OEEOA, CEEOA, and TEEOA). This framework ensures an intelligence cell has considered the complete set of EOAs available to the threat. Each OEEOA will have its unique set of most likely, most dangerous, and other valid CEEOAs and TEEOAs that may or may not overlap with those of the other OEEOAs. S-2s and G-2s must carefully prioritize how much planning and collection resources are devoted to each category and their nested CEEOAs and TEEOAs while remembering that failing to consider a valid EOA increases the risk to friendly forces and mission accomplishment.			
<p style="text-align: center;"><b>LEGEND</b></p> <div> <div>CEEOA</div> <div>critical event course of action</div> </div> <div> <div>OEEOA</div> <div>operational enemy course of action</div> </div> <div> <div>TEEOA</div> <div>transition enemy course of action</div> </div>			

Figure 9. Priority Intelligence Requirement Framework<sup>29</sup>

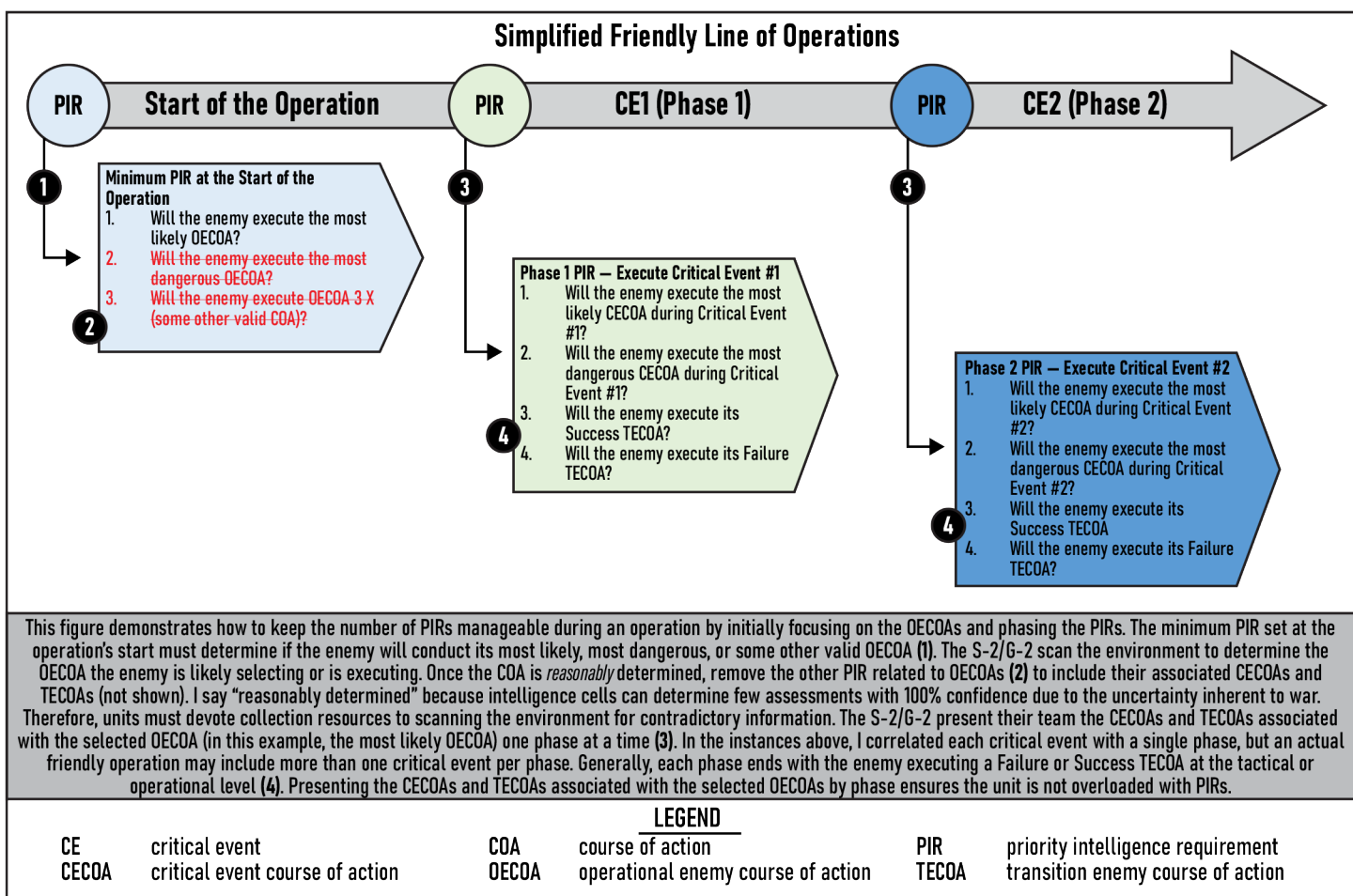


Figure 10. Managing Priority Intelligence Requirements by Phase<sup>30</sup>



## Return to the Most Likely and Most Dangerous Enemy Course of Action

How do you position friendly planning efforts against all these enemy COAs? Here is where the most likely and most dangerous labels return to the picture. S-2s and G-2s evaluate and prioritize all valid enemy COAs within the three categories.<sup>31</sup> Prioritization is essential for two reasons. First, as discussed at the beginning of this article, prioritization ensures that most planning time is devoted to developing the most likely and most dangerous enemy COAs when time is limited.<sup>32</sup> Second, prioritization enables the staff to develop a *single* friendly COA “optimized to counter the most likely threat COA, while allowing for contingency options should the threat choose another COA.”<sup>33</sup> So, if we do our enemy COA development correctly, we wind up with one very resilient friendly COA with the necessary number of contingency options to account for every valid enemy COA in our three categories over an entire operation. This optimized COA is far preferable to a friendly critical event COA that does not take the big picture into account or an operational COA that lacks the details of the tactical situation, with just a single contingency option to account for the most dangerous enemy COA.

## Conclusion

Intelligence cells must commit to determining the complete set of valid enemy COAs to support effective decision making in the uncertain conditions of large-scale combat operations. Drafting operational enemy COAs guarantees we never lose sight of the big picture. Operational enemy COAs serve as the basis for all future COA development. Critical event enemy COAs ensure we execute detailed planning on the areas that matter most. Transition enemy COAs force us to consider what happens next and account for dangerous what-if scenarios. We leverage this understanding, gained during planning, to recover or gain an advantage in every valid situation during execution. The three enemy COAs acknowledge that the enemy *and* friendly have a vote and incorporate this dynamic into their narratives.

The inescapable result of the recommendations in this article is that the staff will make many enemy COAs and friendly branches and sequels. That’s okay. Staff need to adopt the view that COA development is never finished. Once the team wrestles with one COA, they move to understand the operational, critical event, and transition enemy COAs tied to the next most likely or most dangerous situation—situations that large-scale combat operations are guaranteed to produce in abundance. As enemy COAs are updated, so are the PIRs prioritizing the unit’s limited collection assets to determine which COA the enemy will select.

If all these COAs sound too intimidating, start small. Develop a failure transition enemy COA and a success transition enemy COA to go with the standard most likely and most dangerous

enemy COA during the mission analysis brief. Move to critical event enemy COAs and additional permutations of the three enemy COA categories as your commander, staff, and you see the benefits that the three categories bring to planning and execution.

So, grab some red pens. You’re going to need them! ✎

## Endnotes

1. Department of the Army, Army Techniques Publication (ATP) 2-01.3, *Intelligence Preparation of the Operational Environment* (Washington, DC: U.S. Government Publishing Office [GPO], 1 March 2019), 6-5. Change 1 was issued on 6 January 2021. Change 2 was issued on 23 January 2024. (emphasis added).
2. Department of the Army, Field Manual (FM) 5-0, *Planning and Orders Production* (Washington, DC: U.S. GPO, 16 May 2022), 2-1. Please review the discussion cited here for the distinction between warfare’s tactical and operational levels.
3. Department of the Army, ATP 2-01.3, *Intelligence Preparation of the Operational Environment*, 6-7.
4. As with friendly courses of action (COAs), valid enemy COAs must be “feasible, acceptable, suitable, distinguishable, and complete.” Ibid.
5. Many people from my daily duties and professional military education influenced my thinking for this article. I first gained an appreciation for the value of an enemy COA beyond the standard most likely and most dangerous during Intermediate Level Education at the Command and General Staff Officer Course. The curriculum exposed me to the value of the failure enemy COA. I developed and implemented those ideas as a brigade S-2. In my *Military Intelligence Professional Bulletin* (MIPB) article, “Enemy Course of Action Development,” I captured how failure and operational enemy COAs helped my team keep pace in a time-constrained environment during a Joint Readiness Training Center rotation. This article builds upon those ideas along with conversations with my co-workers (notably Majors Kyle Ferguson, Zachary Lawson, Michael Lapadot, Michael Hoffman, and LTC Patrick Vogt) and lessons gleaned from my leadership, principally MG John Meyer’s thoughts on transition points, the need for careful development of enemy COA indicators, and the need for detailed (effective) planning to understand the risk to the force and the mission. Of course, all errors are my own. You can access “Enemy Course of Action Development” at <https://mipb.army.mil/articles/2020-1qtr/fontaine-15oct2019>.
6. Matthew Fontaine, “Enemy Course of Action Development,” *MIPB* (October-December 2019): 23-24, <https://mipb.army.mil/articles/2020-1qtr/fontaine-15oct2019>. I first use the term operational enemy COA in figure 1 of this article. The operational enemy COA’s value, paraphrased in the current paper, is initially described in this article’s text as the COA belonging to the next higher headquarters.
7. Carl von Clausewitz, *On War*, ed. and trans. Michael Howard and Peter Paret (New Jersey: Princeton University Press, 1976), 75. (emphasis original).
8. Full disclosure—I am not a wrestler. But wrestling dummies exist and are helpful in some situations (much as an operational enemy COA can be!). See Kase Nipe, “Wrestling Dummies in Wrestling: Top Options,” *Wrestle Love*, <https://wrestlelove.com/guides/wrestling-dummies-in-wrestling-top-options/>.
9. Department of the Army, FM 5-0, *Planning and Orders Production*, 5-51.
10. Ibid., 5-36. The manual states, “each critical event within a proposed COA should be war-gamed.”
11. Fontaine, “Enemy Course of Action Development,” 24.



12. Adapted from author's original graphic. The figure is a simplified example of figure 6-8. Threat course of action statement example in Department of the Army, ATP 2-01.3, *Intelligence Preparation of the Operational Environment*, 6-16.

13. Ibid.

14. Ibid.

15. Ibid.

16. Ibid.

17. Department of the Army, ATP 2-01.3, *Intelligence Preparation of the Operational Environment*, 6-7.

18. Fontaine, "Enemy Course of Action Development," 24. Critical event enemy COAs are akin to the key terrain and population center microanalysis COAs described in my earlier *MIPB* article. I now prefer the term critical event enemy COA better because it encompasses a broader set of situations and includes a friendly plan to consider enemy counteractions at that event. Key terrain is still valuable, as it can be the starting point for the staff to identify critical events.

19. Adapted from author's original graphic.

20. Fontaine, "Enemy Course of Action Development," 24.

21. Department of the Army, FM 3-0, *Operations* (Washington, DC: U.S. GPO, 1 October 2022), 1-3. See this reference for a discussion on the term *relative advantage*.

22. Adapted from author's original graphic. The figure is a simplified example of figure 6-8. Threat course of action statement example in Department of the Army, ATP 2-01.3, *Intelligence Preparation of the Operational Environment*, 6-16.

23. Ibid.

24. Clausewitz, *On War*, 80, 85.

25. *Public Papers of the Presidents of the United States: Dwight D. Eisenhower, 1957: Containing the Public Messages, Speeches, and Statement of the President, January 1 to December 31, 1957* (Washington, DC: Office of the Federal Register, National Archives and Records Service, General Services Administration, 1958), 818. President Eisenhower recalled this fact during a speech to the National Defense Executive Reserve Conference on November 14, 1957.

26. Department of the Army, FM 2-0, *Intelligence* (Washington, DC: U.S. GPO, October 2023), 6-7.

27. Department of the Army, FM 3-0, *Operations*, 3-9.

28. I benefitted from presentations by COL Blue Huber on the hazards of focusing solely on targeting at the expense of the bigger intelligence picture for this insight.

29. Adapted from author's original graphic, using information from Department of the Army, ATP 2-01.3, *Intelligence Preparation of the Operational Environment*, 6-7; and Clausewitz, *On War*, 80, 85. See also Department of the Army, Army Doctrine Publication 6-0, *Mission Command: Command and Control of Army Forces* (Washington, DC: U.S. GPO, 31 July 2019), 3-7, for a discussion on "exceptional information" as the doctrinal broad category which "contradictory information" would belong to.

30. Ibid.

31. Department of the Army, ATP 2-01.3, *Intelligence Preparation of the Operational Environment*, 6-7.

32. Ibid. Prioritizing planning time for the various enemy COA permutations is critical to success and requires judgment. Even at the division level with a fully staffed analysis and control element, it is difficult to truly *identify*, let alone *analyze*, each enemy COA available to the threat. In my experience, the teams I have participated in have successfully developed the most likely and most dangerous operational enemy COAs. It has also been possible for us to develop the most essential critical enemy COAs post-mission analysis. During mission analysis, we also successfully promoted the most likely transition enemy COAs for the operational enemy COAs. I share this to inform the reader that executing the ideal framework proposed in this article is no small feat! I am still striving for it. But, keep in mind, every added COA we developed brought value to the unit, and the other extreme alternative, only developing two broad COAs and being done, is far too hazardous for large-scale combat operations.

33. Ibid.

LTC Matthew J. Fontaine is the G-2 for the 1<sup>st</sup> Infantry Division, Ft. Riley, KS. He previously served as the G-2 for the U.S. Army Joint Modernization Command, Fort Bliss, TX. His deployments include two tours to Iraq and two to Afghanistan, serving as an executive officer, platoon leader, battalion S-2, military intelligence company commander, and analysis and control element chief. He holds two masters of military art and science degrees, one in general studies and the other in operational art and science, from the U.S. Army Command and General Staff College.

## Reviewing Current Doctrine

ATP 2-01.3, *Intelligence Preparation of the Operational Environment*, provides current doctrine for conducting intelligence preparation of the operational environment (IPOE). Chapter 6, Step 4—Determine Threat Courses of Action, discusses how step 4 of the IPOE process identifies and describes threat courses of action (COAs) that can influence friendly operations.<sup>1</sup> Outputs from step 4 include situation templates, threat COA statements, event templates, and an event matrix. The following paragraphs are key take aways from the ATP.

During step 4, the intelligence staff identifies and develops possible threat COAs that can affect accomplishing the friendly mission. The staff uses the products associated with determining threat COAs to assist in developing and selecting friendly COAs during COA steps of the MDMP [military decision-making process]. Identifying and developing all valid threat COAs minimizes the potential of surprise to the commander by an unanticipated threat action.

Failure to fully identify and develop all valid threat COAs may lead to development of an information collection strategy that does not provide the information necessary to confirm what COA the threat has taken and may result in friendly forces being surprised and possibly defeated. When needed, the staff should identify all significant civil considerations (this refers to those civil considerations identified as OE [operational environment] significant characteristics) to portray the interrelationship of the threat, friendly forces, and population activities.

The most important element in determining threat COAs is understanding threat operational art and tactics. U.S. forces may encounter regular, irregular, and hybrid threats. The process for determining the COAs these threat forces may employ mirrors friendly COA development and consists of the following:

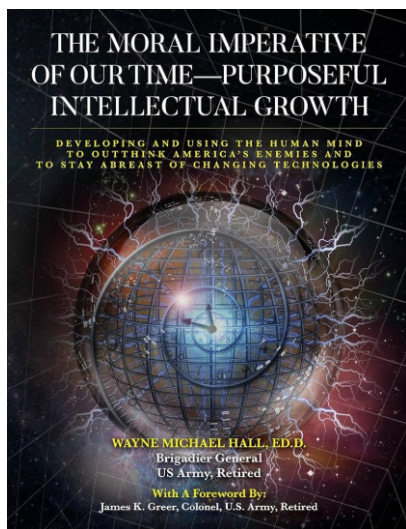
- ◆ Identify likely objectives and the end state.
- ◆ Determine threat battlefield functions.
- ◆ Determine threat capabilities available to perform each battlefield function.
- ◆ Identify the full set of COAs available to the threat.
- ◆ Evaluate and prioritize each threat COA.
- ◆ Develop each COA in the amount of detail time allows.
- ◆ Identify high-value targets for each COA.
- ◆ Identify initial collection requirements for each COA.

When determining a threat COA, the intelligence staff accounts for all relevant threat activity, including but not limited to the analysis of the following:

- ◆ Current threat situation and mission (includes task and purpose).
- ◆ Threat objectives, methods and functions, and end state.
- ◆ Commander's intent, purpose, and end state.
- ◆ Task organization, capabilities, vulnerabilities, and high-value targets.
- ◆ Decision points (essential in determining branches and sequels).
- ◆ Decisive points (source of strength, power, and resistance).
- ◆ Critical events, branches, and sequels.
- ◆ Intent for (includes task, purpose, method, and end state)—
  - ◆ Movement and maneuver.
  - ◆ Reconnaissance and surveillance.
  - ◆ Fires support.
  - ◆ Logistics.
  - ◆ Threat C2 [command and control].
  - ◆ Protection.
  - ◆ Information activities.
  - ◆ Denial and deception.
- ◆ How terrain and weather affect threat operations.
- ◆ How civil considerations affect threat operations.
- ◆ How displaced civilians and displaced persons affect threat operations.
- ◆ How the presence and actions of U.S. forces affect threat operations.

### Endnote

1. Department of the Army, Army Techniques Publication 2-01.3, *Intelligence Preparation of the Operational Environment* (Washington, DC: Government Publishing Office, 1 March 2019), 6-1–6-24. Change 1 was issued on 6 January 2021. Change 2 was issued on 23 January 2024.



# *The Moral Imperative of Our Time— Purposeful Intellectual Growth: Developing and Using the Human Mind to Outthink America's Enemies and to Stay Abreast of Changing Technologies*

by Wayne Michael “Mike” Hall

Reviewed by John W. Smith

Palmetto Publishing, 2024, 448 Pages

ISBN-13: 979-8822935938

*The Moral Imperative of Our Time* is about improving thinking. Anyone who has read one of Mike Hall's books understands that is the driving force in his work. His life force, his vision, is to be a key influencer of both the development and commonplace acceptance of a “twenty-first century altered state of thinking.” This is the latest in a series of six books; each one contributes to bringing that vision to reality. This one is a series of five essays that update some of his earlier writing to address the increasing influence of the information age along with the implications of exploding new technology and their combined impact on how one might—should—think about fighting and winning on yet-untested—in some cases not-yet-imagined—21<sup>st</sup> century battlefields.

As a warm-up to digesting and embracing his thinking about intellectual preparation to win in this century's competitive environment, the reader can take comfort in the reality that there is no single person in the current generation of military thinkers who brings more credibility to the task. Credibility has several fathers; it can be born of what people think, what they say, and what they do. The author has distinguished himself in each of these categories over a lifetime as an intelligence professional.

As a junior Army intelligence officer, his baptism was naked exposure to the reality of his new profession: supported commanders expected consistently superior judgments from their intel guy—judgments that would confidently enable superior decisions and thus regularly lead to good prospects for mission success. Simple, right? That has been the job from the days of Clausewitz; it still is the job. The problem is just this: making it all come together into a coherent, complete, “perfect” intelligence picture is not trivial. Complicating factors abound: the enemy—the competition; the means to gather data and information; quality thinking to make sense of what you think you know...and don't know; the savvy and judgment to know what matters; adequacy of support from the larger “institution” or too frequently lack of it; and the ability to work through the various complexities and impediments to provide the commander or decision-maker with the “perfect” product...on time.

In a military career that spanned over three decades, be assured that the author experienced not only straightforward intelligence problems but some of the most perplexing, hidden puzzles. His lived experience speaks volumes to his credibility. Mentoring subordinates along the way added to his broader esteem and license to speak with authority. In this, the “give-back” phase of his adventure, the author has attracted attention across the intelligence and national security community. He is arguably the single best authority to speak about the influence that “thinking” will have on modern warfare—warfare that is unfolding before our very eyes at an unprecedented speed and with a momentum that will have implications for the military and the nation that extend beyond what anyone is talking about or doing anything about right now.

It is important to note that this book is a capstone to his previous work. Considered together, his efforts are rooted in a philosophy that “will anchor both people and organizations to the ground in the hurricane of change.” The “hurricane of change” is the author's perspective that we are at war in an ongoing competitive environment that differs from earlier wars. War now and for the foreseeable future will not be limited to what is considered to be traditional combat power. It will be characterized first and significantly as mental combat—a war of wits. Winning remains the focus, but the new battlefield is akin to “a play in motion.” The context of mental combat, as such, will present infinite complexities including nimble, passionate, intelligent enemies often enabled with technology as capable as ours. And significantly, the battlespace will not always be defined by things that can be seen, located and killed, but first signaled by insightful “reads” of intangibles, “reads” executed by thought warriors who are able to gain and maintain control, of the “intellectual high country.”

These new hurdles, opportunities, challenges—call them what you will—helped guide the author toward his theory of intelligence—a vision of the “whole” needed to wage and win mental combat. A few key pillars shape his theory—some old with a new twist, some new, all significant. Central to his theory: “will;” purpose; the vital-to-grasp relationship between data-information-knowledge and understanding. He also advocates the need for two new domains of war—vertical domain silos (an information domain and a cognition domain) that each represent combat power as much as the existing domains of war. Further, he proposes change to the three traditional doctrinal levels of conflict—splitting the strategic level into two new ones: resulting in tactical, operational, strategic (military) and strategic (policy).

Threaded through these theoretic pillars is his relentless focus on how to think better and his never-at-rest exhortation that winning for the intel guy always involves aiming for the impossible-to-reach yet nonetheless nonnegotiable goal of “perfection.”

Easy, right? Not quite.

To the soundbite crowd, eager for one-size-fits-all simplistic solutions, Hall’s in-depth treatment and explanation of the need for a philosophical, theoretical under-pinning might seem excessive. But it is the bedrock foundation for all that follows: conceptualizations; definitions; thought models; priceless visualizations that lead the dedicated thinker through a maze of complexity not to an approved solution, but instead to the intellectual high ground needed to confront all such difficult thought problems in multiple contexts. Particularly noteworthy among the detailed approaches that a serious thinker might put to immediate use is his 14-step thought model on what it takes to define and successfully impose one’s “will” upon a thinking enemy. Central to and running from beginning to end of this thought model is one’s “purpose.” As the author ponders “what one can do about the enemy’s determination and perseverance,” he offers: “purpose is preeminent because it provides the overarching rationale and moral ‘heft’ for conflict.”

While the preceding is useful, it remains abstract. Fortunately, a key feature of the author’s work is that he is not content to assert the relevance of abstract thinking without also leading the horse to water, so to speak. His commitment to help people “do,” to reach their intellectual high ground, is evidenced particularly in an entire series of other valuable thought models that permit serious thinkers to begin their own experimentation with the author’s approaches to improved thinking. His best implementation model? His advocacy for and description of an approach he labels “matrix war,” a matrix formed by the intersection of his proposed “new” domains of war with his modified levels of conflict. As envisioned by the author all such wars of wits will occur in one or several of these cells. Thus, the matrix approach offers a point of departure for the serious thinker to explore the relevance of a particular problem. Specifically, the approach enables high-level thinking about whether the presence of a problem affects “purpose,” and if so, why, how, and what might be done, from a “thinking” perspective, to mitigate or change its presence or impact.

While the author’s focus is squarely focused on improving the thinking necessary to help those in the thought trenches of mental warfare—analysts, commanders, policy makers—he also addresses another reality. Meaningful solutions to many hard intel problems implicit in today’s information- and technology-driven warfare reside beyond the purview of the practitioners of high-level thinking. In particular, the “institution” has a major role to play. The author articulates and confronts the challenges and impediments that the “institution”—both organizations and the people in them—pose to progress. He offers harsh criticism, and he rebukes the “arrogant,” “ignorant” that peacefully slumber. He appreciates that it is long-time respected organizations that have the authority, the means and the talent to bring improved thinking to bear in the form of doctrinal change, man-machine connections that routinely capitalize upon the power of both mind-blowing technology advances and the awesome power resident in the human mind. But he is perplexed. While he does not refer to these organizations and their denizens as troglodytes, it seems that this nasty label could be perched on the tip of his tongue. Their collective amnesia and avoidance of the need for better thinking—better thinking that can reveal itself as intangible, but real combat power—is virtually smothered by the “routines” of government and their self-satisfied, smug, vacuous outward-facing pontification, ineffective policies, and sadly short-sighted initiatives and investments.

The lines of discussion above are mostly developed and discussed in detail and represented in whole or in part in his previous books. The rationale behind this lengthy characterization of the author’s body of work has a simple, straight-forward explanation. Each of this book’s five essays includes in varying degrees the themes detailed in earlier books. But in this book, one profits from new perspectives emerging from the author’s never-at-rest brain. Some readers may find it useful to explore those earlier works. In most cases, this is easy to do, because the author liberally points the reader to his original discussions.



For readers who have not read any of his earlier work, *The Moral Imperative of Our Time* is a good place to start. The author, as characterized in the *Foreword*, writes for three purposes: to learn, to educate, and to persuade. Thus, this book reveals the maturation of some of his thinking from earlier work. In fact, it is refreshing to read in his own words how he has learned over time. For instance, in *Essay Four: A Vortex of High-Level Thinking—Q and A with a Young Analyst*, General Hall reveals his total commitment, not to selling a book, but instead to educating and persuading others to think better. In a dialogue that lasted over three years, the young analyst asked him: How did you develop the definition of “will” and its intricacies? In response, he said, in part:

*I did not seriously think about ‘will’ ... until I retired from the Army. ... I mouthed the word with something akin to willpower, but ‘will’s’ true meaning was not forthcoming. ... I looked in both Army and Joint doctrine for definitions and explanations but came up empty handed. ... I have worked seriously on defining ‘will’ since 2007. ... I have [improved it but] [t]he long road to attain a successful definition of ‘will’ remains a work in progress.*

A caution to readers: For those of you who read the title of this essay and think about skipping it, resist the urge. It consists of 14 Q’s and A’s; half of them elaborate on the evolution of the author’s own thinking and the back-and-forth with himself as he reaches the point where he believes ‘will,’ and its offspring ‘purpose,’ if ignored, handicap not just analysts but their supported commanders.



Woven into the fabric of his exchanges with the analyst, the author introduces the subject of matrix war. But, in *Essay Five: A Discourse between a Master and Apprentice—About War Per Se*, he elaborates in great detail. He explains how various cells house centers of gravity (COGs), how COGs move and morph, and how, when considered as a whole, they can offer pure gold to a ‘thinking’ commander. The commander who uses the matrix approach to tease out the exact purpose of his mission, what matters and what doesn’t, will soon realize that it offers not just a point of departure for his thinking. Coming along for the ride, he will realize that it offers solutions to the hardest of thought problems—all hiding in plain sight. It will guide the thoughtful commander to understand precisely what kind of war he’s in, to refine his purpose, and in brief to think about and understand the “whole” before, during and after he makes a decision and takes decisive action.

The commander who employs the matrix approach as a guide to winning the battle of wits will soon find himself face-to-face with an unforgiving reality: to win, he must be able to move fast and seamlessly between domain silos and levels of conflict. Each cell houses data and information that can become knowledge...but only if he is able to access it, adapt to it and act decisively. The shallow reader might be tempted to breeze past this discussion as an unnecessary side trip to purposeful intellectual growth. Ignore the temptation. Mike Hall characterizes his treatment of these terms as “the heart of the essay,” adding there “is an absolute need to know the difference among data, information, and knowledge.” He goes on to explain—to both the commander and the institution—why that’s the case.

Data, information, and knowledge collectively represent an ever-present influencing factor on mission success or failure. But—but—to experience a “win,” also requires improved institutional engagement and support. The author characterizes what an institution typically provides as ‘macro’ or ‘micro’ solutions. At this point in time, he labels institutional support as outdated and largely macro—one-size fits all—solutions that do not work in the complex mission reality of mental war. Unchanged, such institutional support is akin to one hand clapping: there will be no applause for a winner, because there will be no winner. To get to the intellectual high ground, the institution will need to focus instead on enabling ‘micro’ solutions. The author urges institutional focus on three things. First, in the various school houses, there must be a decided shift from what-to-think to how to think. This is the central point of the book. In his *Epilogue*, Hall continues to hammer the point. He characterizes the existing military thinking environment as an “intellectual wasteland.” The way out, he says (p.382):

*...humankind must learn how to think and engage in serious lifelong learning as a matter of personal and cultural survival. It is a moral imperative to be a lifelong learner and a high-level thinker along with helping one’s subordinates and organizations learn and keep learning ‘how to think’ ....*

Second, the institution must give serious attention to current organizational designs that—instead of enabling commanders to move seamlessly up, down and sideways in matrix war—bureaucratically impede performance. Needed, he observes, are “agile,” “flexible” organizations. Third, the author exhorts the institution to take steps necessary to develop and deploy technology in a manner that can continuously bring data, information, and knowledge to bear for the commander as a “weapon system.” One approach he advocates is virtual knowledge environments (VKE). Such an initiative would provide analysts, commanders and other decision-makers access—on demand—to data and information that could become the

knowledge needed to inform superior analyst “reads” about the operational context surrounding a mission and thus inform a commander’s superior decisions. Although VKEs are easy to conceptualize, the lack of access to data and information is a critical—perhaps the critical—issue standing in the way of effective matrix war as described and envisioned by the author. Committed institutional leadership is “the” key to making such an initiative reality. This and other issues are discussed in *Essay Five*. For the serious, committed thought leader, the leader who knows that consistently winning mental combat is essential but does not appreciate where or how to start, reading *Essay Five* is a good place to start.



*Essay Two: Implications for Intelligence Collection—Irregular and Asymmetric Warfare* builds upon the author’s book, *Intelligence Collection: How to Plan and Execute Intelligence Collection in Complex Environments*. *Essay 3: A “Journey” to the Edges of Advanced Intelligence Analysis—2007-2014* also builds upon an earlier book, *Intelligence Analysis: How to Think in Complex Environments*. Both essays provide new insights and implications that build on the earlier books.

Together, these essays describe how the two main actors—analysts and collectors—must think about their job and what they must do as a well-oiled functioning team to enable a commander to both viscerally understand the context of his mission and to regularly make superior decisions. These are great essays for both analysts and collectors, because they offer the author’s latest thinking since the publication of his two books several years ago. Having said that, his two earlier books remain essential for analysts and collectors to have handy. They continue to offer thinking that is pertinent and timeless.

At a glance, the titles to these two essays might suggest they have little to offer commanders or the institution. Warning: do not skip them. Hall’s message and the tone of his message is aimed at both audiences. To see why, let’s back up and look at the big picture—the need to understand the “whole” that Mike Hall evangelizes throughout all of his writing. If the goal is to inform a commander’s superior decisions, it follows that assessments provided to him would likewise aim to be flawless. Despite the impossibility—due in large part to an enemy with a vote—of attaining “flawless,” that remains the timeless goal of any analyst-collector team. From the start, the pursuit of “flawless,” “perfect,” is a “mental phenomenon.” It is true as well that analysts “lead the fight for initiative.”

Thus, a thinking analyst would bring to his task a large dose of reality about how the world works. He would grasp that it’s his job to fully understand and explain to his commander the “logic of the mission’s operational context.” As part of “context,” the real world contains what the author labels “linear” problems—if-this-then-that problems. Many of those problems are complicated but eventually can be made to surrender to logic and analysis—given, of course the right data and information. Unfortunately, the real world—including the real world surrounding a commander’s decision-making—also includes nasty, complex problems. Hall calls them nonlinear complex adaptive systems, CASs.

For instance, while a commander might need to know how an enemy artillery unit continues to escape detection and avoid being located, linear factors certainly come into play: distance relationships and links (guns to targets, guns to fire direction, ...), patterns (movement times, movement routines, communication patterns, ...). Sorting out this kind of problem is in an analyst’s wheel house, and it promises to be complicated. But with time and the right knowledge at the right time, they might be solved. The same straightforward situation might, however, also become complex. Let’s say, communications indicators tend to vaguely locate the unit in the evening near the same town. Its communications interestingly also fall silent around the same time. A thinking, but frustrated, commander who directs his intel team (his analyst-collector team) to find out everything about the enemy commander might eventually unscramble the puzzle. They may learn from a host of sources that the commander lives in the town and is known to frequently return home in the evening. In such situations where possible but uncertain human behavior might help locate the enemy battery, the author views such problems as a complex adaptive system.

Complex problems thus are characterized by factors that extend beyond the linear if-this-then-that problem mold. The author goes to extreme efforts to detail factors that should be of interest to an analyst-collector team in their work to confront and understand such real-world linear and non-linear situations. Hall defines CASs as having links, relationships, causes, effects, patterns and more. He charges the analyst-collector team as central to accessing all relevant information, breaking it all apart—analysis—and reassembling it—synthesis—into a composite picture and, most critical, making the output of their effort available to the commander.

The brief description above is a straightforward, logical—but wavetop—laydown that should leave the reader with an appreciation of a simple fact. The task confronting the analyst-collector team varies from simple linear types of problems to complex ones that defy prediction. Nonetheless, simple or hard, their task is to corral knowledge of the whole. To do so requires their ready access to all manner of data and information from all types of sources that with analysis and synthesis

can be used to build a reliable picture, story, narrative upon which a commander can make a superior decision. The ability of an analyst-collector team to do this forms the basis for judging their performance—good or bad. Execution becomes the coin of the realm, and that is the hard nut that confronts mental warfare in the 21<sup>st</sup> century.

The author repeatedly makes the point that knowledge created by the intel team's access to data and information while often intangible is nonetheless quite real, essential combat power. Without a good picture of the operational—and especially relevant for institutional leaders, the bureaucratic—context, supported commanders and other decision-makers have been, are, and will continue to be acting in the blind. Commanders of combat units would never go into an operation knowing that their tanks or artillery had insufficient ammunition; effective, sustained fire power is essential to their mission success. Yet the same commanders too often—for years, for decades—have gone into battle with an analyst-collector team that fell short of being able to deliver expected, necessary intel-related knowledge “fire power.”

The Army, the larger Defense establishment and the national and service intelligence communities have by and large ignored the vital requirement to confront the main issues standing in the way of informing and enabling decision-makers of all stripes—commanders, policy-makers, institutional leaders. Each should have a superior understanding of the real-world contexts that surround the problems they wish to solve and thus the factors that shape their decision-making. Two key drivers demand immediate attention if combat commanders, policy-makers, and institutional leaders want to win in the technology-driven, information age that is everywhere today...a reality that only shows signs of continuing unabated.

General Hall explicitly addresses both.

First is the need for an intelligence enterprise. In his 2023 book, *Whispers from the Arrow of Time*, he elaborates extensively on the need to “[d]evelop and employ virtual knowledge environments” or VKEs described above. In this book's *Essay Two*, he introduces the *intelligence enterprise* as a vehicle to make them a reality. He states, “a distinct need exists for an intelligence enterprise that focuses intelligence support from the national level to the small unit tactical level.” His description of the need for a *hive mind* is a simple yet powerful notion. He describes it as analogous to preparing a beehive to move. Each bee requires information to perform its function—“stay with the hive.” Yet the performance of individual bees benefits the mission of the whole—move the hive.

The author describes the intelligence enterprise as a means to fulfill several purposes. Chief among them is the pursuit of a philosophy that “sharing is good.” Unfortunately, there is a mindset in intelligence organizations—particularly in national organizations—that they exclusively “own” data, information, and access to expertise resident in the organization. That dog won't hunt in today's increasingly competitive, information-, technology-rich mental war settings. The author rightly asserts, “Many minds working in a unity of effort toward a common goal constitute a force far superior to any one mind.”

So, one might ask, “Why not just do it?” Naturally, there are valid reasons to protect the sharing of everything all the time everywhere. But those reasons do not need to stand in the way of common-sense initiatives to better enable commanders and other decision-makers with an understanding of the context surrounding their various missions. The author makes an implicit, persuasive argument that the various U.S. service and national intelligence organizations that largely support narrow, isolated user communities, fail when examined from the perspective of the whole that could—and should—benefit from the country's massive investment in talent and capability that is essentially wasted by not being made available to the units and organizations that could and should benefit.

The way forward might not have been feasible just a few short years ago. Technology is available today to make the author's notion of an intelligence enterprise a reality. What's missing it seems is the will to move forward and a champion—or a few of them—to run with the idea.

The second key driver needing aggressive attention is an intelligence community-wide effort to improve the quality of thinking that persists throughout the intelligence community—especially by analysts. In the second half of *Essay Three*, the author includes a description of his take on a series of 52 two-week seminars for about 1250 advanced analysts. It is a compelling read; it captures, in close-up detail, two main themes that run through the book. First is the unfortunate fact that good thinking is scarce among analysts.

*As a confession, after fifty-three years of being an intelligence officer, I am worried. [M]any analysts neither think deeply, nor critically; many do not read critically (many don't read difficult subject matter at all), and many prove so consumed with organizational directed 'hair on fire' ... processes ... that they admit that they don't have time to engage in 'deep thinking'.... [T]hey do not know how to think via synthesis and holism, both essential to supporting warfighters in the information age.*

Second is the equally troubling fact that the institution's support is, in a word, inadequate.

*When an analyst fails to think, they have little hope of understanding the consequences of their actions. ... Without ... nimbleness of thought and cognition, the power inherent in advanced analysis lays [sic] dormant. ... But intelligence analysts cannot be blamed for this situation. They are wonderful people, full of potential and altruistic motives. The fault lies squarely with poor leadership and the mindless bureaucracies that tend, through powerful position and influence of bureaucratic administration, to debilitate creativity, innovation, civil discourse, and expansion of knowledge...*

Reacting to the above, the author advocates for thought leaders—commanders and individuals leading the institution—to do three things: they need to understand that they themselves need to be lifelong learners; they need to help subordinates learn with purposeful efforts and development programs; and they need to help their organization learn with the intent to “value human intellect” and “decry mediocrity.” The author sees these efforts as essential to prepare the analyst intellectually for the overarching task of understanding the operational context surrounding a unit’s mission and enabling him or her to actually deliver “knowledge firepower” to commanders. The author advances a system of thought with definitions, thought models, powerful visuals and illustrations to make his suggestions reality. So, what’s the problem, you might ask? Just like the way forward to fashion an intelligence enterprise boils down to leadership, so too does righting this ship.

Unit commanders—those in direct contact with their analyst-collector intel team—bear a critical responsibility to become one of two credible drivers of better thinking by their intel teams. The author hits the nail on the head: “Regardless of ... what needs to be accomplished to optimize analysts’ performances, the difficult part involves convincing people in leadership positions, who have a stake in the status quo of existing programs, to acknowledge that a significant problem exists.”

It is normal for commanders to undertake mission rehearsals of various aspects of a unit mission, perhaps at the operational level a deep strike assault, one focused on coordinating ground and air fires and other aspects of the mission. At the tactical level, an analogous rehearsal might involve infantry-armor maneuver formations. Why not do the same with the unit’s intel team? Would it not make sense for a corps commander to walk his intel team through the entrails of an enemy’s command and control...their likely reactions to the deep strike? Too frequently, such initiatives are never pursued, or if pursued they are coupled with force-fed, canned information instead of knowledge that can only be informed by having had access to experts and their real-world data and information.

In spite of such handicaps, it is incumbent upon unit commanders to maintain constant pressure on his intel team to deliver a complete picture of the situation surrounding his decision-making. And, critically, when such commander-intel team thinking sessions are precluded because of institutional lethargy or, in the words of the author, inability to perform seamlessly as an intelligence enterprise, commanders must speak up. In this age of competitive, mental warfare it is unacceptable for unit commanders to shrug their shoulders and willingly accept the institution’s inability to enable serious thinking about what was described earlier as the *micro* problems that must be identified and resolved routinely inside a unit.

The era of the institution developing and providing *macro*, one-size-fits-all solutions, tossing them over the transom to units, and puffing their collective chests out in the false belief that they have really helped a unit intel team deliver knowledge to the commander is over. It’s been over for decades. But without aggressive action to right this ship, knowledge firepower will continue to be largely a nonplayer in this fast-evolving competitive battlefield that features thinking more than things that go bang. Just as with the need for leadership to move forward in making an *intelligence enterprise* reality, so it is with the need to see a massive spurt of focused energy from the institution in establishing performance standards that settle for nothing less than excellence in thinking and the means to make it so. Just as with the enterprise the need for better thinking calls for a number of champions to step up, and simply say, “I got it!”



Finally, a few words about the author’s *Essay One: 1985—A Visit to Verdun—A Young Army Officer’s Impressions*. In this essay, General Hall deals with the connection, the relationship between the theory of war and its physical reality. [Moral Imperative, p.xx] This relationship permits him to talk directly to moral imperatives, the linkage between good—and too often bad or no—thinking and unnecessary, resultant soldier deaths. The basis for the essay was his 1985 visit to Verdun as a young officer. The author’s main point: neither French nor Germans generals seriously thought about what they were doing; in so doing, they contributed directly to the deaths of more than 300,000 soldiers between February and December 1916. In particular, the author concentrates on the need for “purpose” to drive war. He credited the six-month stalemate as resulting from one thing: a weak German lack of purpose. The German chief of the general staff, Erich von Falkenhayn, had one thing in mind: “bleed the French Army white.” What he did not take into account was that the French had a vote. He failed to account for French resolve. For the French, the “offensive was sacrosanct.” This led to their “egregiously poor thinking,” thinking that included “not being concerned about what the German strategic aims, goals, objectives ... could be....” Emphasizing that mindset, Hall quotes historian Alister Horne, saying: “From top to bottom, the [French] army was impregnated with ... extravagant, semi-mystical nonsense. ... *What the enemy intends to do is of no consequence.*”



Such lack of thought, evidenced by a lack of meaningful purpose on both sides, underpins General Hall's message throughout *The Moral Imperative of Our Time*. It is probably safe to say too that the author's experience, now almost 40 years ago, inspired his post-Army writing—writing concentrated on the need for improved thinking. The guts of the five essays in this book simply underscore why this need is so accentuated in the 21<sup>st</sup> century. And poor thinking, evidenced in weak, undefined purposes did not take a rest after WWI. Poor thinking was also prominent during the U.S. war in Vietnam.

In *Essay Five*, the author discusses American mental errors that stand out from its involvement in Vietnam. Under the leadership of the U.S. architect for the war, Secretary of Defense Robert McNamara, the author describes our "fatal fascination with numbers and disregard of the nature of the enemy's 'will' in North Vietnam.

*President Lyndon Johnson, his advisers, McNamara, Dean Rusk (Secretary of State), national security advisor McGeorge Bundy, the Joint Chiefs of Staff, and General William C. Westmoreland, Commanding General of all U.S. forces in Vietnam proved intellectually inept. ... [A]ll had in common the mistaken proclivity to think quantitative analysis would yield the right, rational conclusions, the right assumptions, the right actions....*

Referring to *Dereliction of Duty*, a book authored by retired Army general H.R. McMaster, Hall characterizes a dilemma faced by McNamara's "wonder boys." While:

*all their numbers pointed to [U.S.] victory in Vietnam, ... they slowly concluded America was losing and did not know why. The reason for failure was their arrogance and ignorance about the definition, conceptualization, and employment of 'will' ....*

As mentioned earlier, the author's intent concentrated on educating and persuading. He has succeeded. This is a book for serious professionals, readers who bring a commitment to excellence to what they do. Reading this and his earlier books is not a walk in the park. It requires reading, thinking, re-reading, and serious contemplation about what it will take to pursue excellence—excellence whether you are an analyst, a collection expert, a unit commander, a strategist or policy-maker, or a member of one of the institutional organizations discussed in this review or highlighted in General Hall's work.

Serious effort will be needed to bring about changes the author proposes. It will take not just efforts to improve how people directly or tangentially involved in intelligence think. It will also take some breaking of china: 1) actions that seriously address the effectiveness of institutional support to intel professionals in units; and 2) related actions that assess the feasibility of existing organizations to support the proposed notion of a national to tactical intelligence enterprise. Changes such as these will not be straightforward actions. They will entail significant cultural change that embraces new ways to think inside long-standing institutional organizations.

As a consequence of the scope and nature of the implications to embracing the author's thinking, the most important requirement is for leadership that wants to win in the changed landscape of 21<sup>st</sup> century information- and technology-driven mental warfare. Champions are needed to effect such change, leaders who want to win and are willing to take unpopular stands to make it happen. This book is for those folks.

*John W. Smith is a retired U.S. Army Brigadier General. He is a long-time friend and former colleague of the author.*

Students in the Fort McCoy Cold-Weather Operations Course start their skiing orientation and familiarization at Whitetail Ridge Ski Area, Fort McCoy, WI. (U.S. Army photo)



# INTELLIGENCE PREPARATION OF THE OPERATIONAL ENVIRONMENT IN THE SUBARCTIC

BY MAJOR MICHAEL EVERETT

## Introduction

Intelligence preparation of the operational environment (IPOE) is the fulcrum for all Army tactical intelligence support. It is the driving process for deliberate, effective, and efficient intelligence operations for brigade combat teams and lower echelons. During initial entry training, the Army teaches all-source military intelligence professionals about the four steps of IPOE. The Army then reinforces these foundational skills throughout their careers at most levels of professional military education. IPOE is a tried-and-true method for systematically assessing both the environment and the threat that produces outputs directly impacting all aspects of an operation.

Current IPOE doctrine, however, is lacking in one significant area: considerations for extreme environments, including the arctic, desert, and jungle environments. These operational environments (OEs) present unique challenges that require more careful consideration of their characteristics and effects by military intelligence professionals as they conduct IPOE. The four steps of IPOE and their outputs do not change; however, intelligence professionals must address the unique aspects of supporting operations in the extreme environment using a fundamentally different approach to IPOE.

This article specifically addresses the unique qualities of the subarctic environment. The subarctic is not simply a cold climate; it is an extreme environment with rugged mountainous terrain, glaciers, and novel hazards such as avalanches and temperature inversions. Geographically, the subarctic zone lies between latitudes 50°N and 66°33'N, just south of the Arctic Circle.<sup>1</sup> Many of the most strategically important territories in Alaska, northern Europe, and northern Canada fall within this band. Because operations further north in the Arctic Circle would be difficult to sustain for a significant period, the subarctic is the most likely setting for any conflict in the far north.

## Preparing for IPOE: Pre-Mission Analysis

*To perform IPOE and the other important intelligence tasks that support operations, the intelligence staff must conduct a significant amount of analysis before receipt of mission.<sup>2</sup>*

Research and pre-mission analysis are necessary before conducting IPOE in any environment, but they are critical in an extreme environment like the subarctic. Preparatory research fosters a comprehensive understanding of the OE throughout the IPOE process. Reviewing manuals on cold weather operations from prior conflicts allows analysts to draw on lessons learned, and it provides valuable insight into how armies have overcome the unique challenges presented



Paratroopers from the 2<sup>nd</sup> Infantry Brigade Combat Team, 11<sup>th</sup> Airborne Division jump onto the Malemute Drop Zone, Joint Base Elmendorf-Richardson, AK. (Photo by CPT Michael Everett)

by past cold weather maneuvers. For example, the German *Handbook on Winter Warfare*<sup>3</sup> and the U.S. Army Corps of Engineers' *Special Report 93-12: On Winter Warfare*<sup>4</sup> provide a good baseline on the environment's impact on warfighting. When reviewing these and other similar documents, analysts should focus on the aspects of the OE that make these environments different and make note of which strategies were most successful.

The value of old doctrine, publications by service schools (e.g., Northern Warfare Training Center in Black Rapids, Alaska), and nonfiction literature should not be underestimated. Publications like these encompass a wide variety of experiences and information and can provide a wealth of knowledge on the subarctic. These documents add value because they not only present the unique operational challenges posed by these environments, but they also offer valuable solutions to those challenges.

Although few conflicts have transpired in the subarctic, historical information is available on, for example, the Russo-Finnish War and multiple conflicts in Scandinavia throughout history. The unique consideration for IPOE in this extreme environment is that the military challenges rarely change at the pace of those in a temperate climate. Regardless of technological advances, the elements are always the most significant challenge, and the lessons learned in the 13<sup>th</sup> century are as relevant today as they were then.

## IPOE Step 1: Define the Operational Environment

*During step 1 of the IPOE process, the intelligence staff identifies for further analysis the significant characteristics of or activities within the OE that may influence friendly and threat COAs [courses of action] and command decisions, as well as the physical space the mission will occupy. Within an OE, Army forces may face large-scale ground combat operations, which simultaneously encompass multiple domains, military engagements, and populations.<sup>5</sup>*

A unit's higher headquarters designates its area of operations (AO). In the subarctic, expect unit boundaries to follow mountain ridgelines, valleys, rivers, and other challenging terrain features. These are natural boundaries in a sparsely populated environment that lacks extensive road networks and contains pronounced terrain features.

The AO overview should highlight significant terrain features and address realistic time-space analysis. This approach considers the current snow depth, upcoming weather, terrain slope, road or trail conditions, and friendly and threat over-the-snow movement capability. A general analysis is not sufficient, however. This level of analysis during IPOE step 1 requires some information not identified until step 2; therefore, an analyst must return later to the step 1 analysis to update the information.

The area of interest will impact the difficulty of traveling over long distances. Threat units will not be as capable of reinforcement or mutual support over long distances as they would be in a less restrictive environment. Depending on the



road networks, weather conditions, and over-the-snow capability of the threat, it can take days for mounted elements and weeks for dismounted elements to traverse a 200-kilometer straight-line distance in the subarctic. The logic learned during initial entry training or other professional military education cannot be applied to extreme environments. The tactical commander will issue their planning guidance based on the time-space analysis presented during the briefing on the area of interest. Unrealistic timelines desynchronize a friendly operation before the line of departure.

## **IPOE Step 2: Describe Environmental Effects on Operations**

*Step 2 of the IPOE process determines how significant characteristics of the OE can affect friendly and threat operations. The staff begins evaluation by analyzing existing and projected conditions in the AO and AOI [area of interest], and then determining effects on both friendly and threat operations.<sup>6</sup>*

Extreme operational environments have a significant impact on step 2. This is where a mission analysis brief can add the most value. It is also a crucial step early in an operation, before extensive, on-ground reconnaissance. The staff relies on a thorough analysis of all aspects of the OE that will affect them and their ability to support all elements of their war-fighting functions. Terrain analysis in the subarctic will leverage standard IPOE methodology; however, analysts must consider additional niche factors to prepare Soldiers to face the most dangerous threat on the battlefield: the environment.

The subarctic experiences unique seasonal weather patterns that affect the terrain. Environmental trends suggest that summer or winter are the best times to conduct military operations in this region. Spring and fall are especially problematic due to the thaw-freeze cycle, known as “wet cold” (+39° F to +20° F).<sup>7</sup> This cycle occurs when daytime temperatures are warm enough to melt snow and ice, and nighttime temperatures then freeze this standing water, creating hazardous and challenging conditions. The tactical intelligence officer must recognize and acknowledge this aspect of the OE and ensure that decision makers know the risks associated with military operations during this period. Vehicles will fail due to frozen parts or lines; weapons will malfunction more often due to frozen components; and service members will be at a higher risk of frostbite.<sup>8</sup>

Step 2 should also focus on tenable command posts, logistics nodes, firing positions, and tactical assembly area points in this environment. Finding these locations in the subarctic using imagery can be difficult because open areas may not be cleared of snow and winter debris. Imagery gathered within 12 to 24 hours is preferred (e.g., synthetic aperture radar or electro-optical overhead systems), as it can indicate where the threat has cleared the snow and suggest locations where friendly forces can establish positions. Soil composition and surface content, like gravel or pavement, can reveal suitable

locations where vehicles will not continue to sink after snow clearance. This information is vital to commanders as it prevents the loss of mobility, provides options based on near real time information, and may signal the location of threat command posts, artillery, or logistics nodes. Requests to the geospatial intelligence cell should be made early and often to assist in proper analysis.

Elevation significantly affects operations in cold weather and mountainous regions like the subarctic. Providing topographic relief models and maps is critical to ensuring leaders understand the importance of topography to the operation. Topographic maps that display relief three-dimensionally offer the best means to illustrate the impact of elevation on the friendly force scheme of maneuver. Tools such as the Distributed Common Ground System-Army Capability Drop-1 or similar commercial-off-the-shelf software can provide reliable heat maps displaying land surface earth science data overlaid on maps of the Earth as elevation in two dimensions, such as hard copies or a PowerPoint presentation.<sup>9</sup>

Road accessibility is the most significant limiting factor when operating in the subarctic. Less terrain-restrictive environments allow for limited to extensive off-road movement for wheeled and tracked vehicles. When conducting IPOE step 2 in the subarctic, the most recent imagery and real-time reporting is the only reliable method of predicting route trafficability. Consider recent weather, civilian traffic in the area, and local snow removal capabilities. In the subarctic, roads will likely remain the only method to move standard Army vehicles (wheeled and tracked) across the terrain. Over-the-snow vehicles provide additional options and should be addressed in terrain analysis; however, do not assume that all over-the-snow vehicles can travel across all snow-covered landscapes. The snow’s density, consistency, and degree of grooming will factor into the trafficability and speed at which an over-the-snow vehicle can move. Assess the local recreational and utility trail networks during mission analysis and initial IPOE. Reassess as the mission progresses to determine whether the trail network’s accessibility is affected by weather conditions. To identify these trails, use local maps, overhead assets, and commercial applications designed for recreational activities. Knowing which trails are accessible and which are not is invaluable. Use intelligence reach and collaboration with other organizations to fill information gaps and clarify trafficability when possible.

Weather ties heavily to subarctic terrain conditions. The intelligence cell’s ability to articulate the weather’s impact in step 2 of IPOE is critical to its value. “A mountain environment is generally categorized as an area where altitude, relief, and weather significantly degrade normal military activities....A cold weather environment is characterized by low temperatures, fog, freezing rain, snow, ice, frozen conditions, and a series of freeze and thaw cycles.”<sup>10</sup> The impact of temperature



and precipitation can be deadly in the subarctic as it combines the dangers presented by mountainous terrain and cold weather. “Wet cold” tends to be more dangerous than any other condition except extreme cold.<sup>11</sup>

Overall, the subarctic contains frozen and non-frozen hydrology, snow drifts, snow accumulation, severely restricted off-road vehicular movement, ranging line of sight based on drastic elevation shifts, and minimal concealment in the winter months. This only scratches the surface of the challenges the staff face during IPOE step 2 in the subarctic; it can become the most crucial step to ensuring that friendly forces prepare physically, mentally, and materially for the challenges they will encounter. The staff should conduct extensive analysis that fully incorporates their understanding of the subarctic region’s effects on threat forces and friendly operations.

### **IPOE Step 3: Evaluate the Threat**

*Step 3 of the IPOE process determines threat force capabilities and the doctrinal principles and TTP [tactics, techniques, and procedures] threat forces prefer to employ. This may include threats that create multiple dilemmas for U.S. maneuver forces by simultaneously employing regular, irregular, and terrorist forces and criminal elements, using a variety of traditional and nontraditional tactics.<sup>12</sup>*

Under the intelligence staff’s direction, the entire staff should participate in IPOE by analyzing their opposing force counterpart. This whole-of-staff analysis is a crucial element to the overall success of IPOE. The subarctic environment may include unique mission variables and uncommon aspects to threat models or key systems, making it impractical to rely solely on the S-2 section to analyze all relevant aspects of the threat. While a whole-of-staff analysis by warfighting function is an excellent method to get the staff sections involved in mission analysis and IPOE, it is even more essential in the subarctic. Each warfighting function requires unique templates with questions or prompts to generate relevant information to set a foundation for step 4. The intelligence staff should push these templates out at the beginning of mission analysis or IPOE, ensuring adequate time for each staff section to research, record, and produce quality products.

The threat templates also merit special attention. The OE Data Integration Network (ODIN) provides an adequate baseline for arctic capabilities and assets attributed to multiple nation-states.<sup>13</sup> In addition to these real-world resources, ODIN offers the Decisive Action Training Environment scenario equivalent, which can assist S-2 sections in adapting their situation to the appropriate arctic threat.

In the subarctic, the intelligence staff must research over-the-snow vehicles and capabilities to understand how, where, and when the threat can move. How effective are specific types of over-the-snow vehicles in the distinct types of snow? How many over-the-snow vehicles does the threat have, and how will this change their task organization across all maneuver and support units? Extreme environments tend

to be a laboratory for experimentation, leading to constant change and adaptation. The threat templates are important but avoid tunnel vision. The threat’s task organization down to the lowest level will change as the enemy commander changes his tactics.

The subarctic also significantly affects key systems. Any vehicle or asset floating over or through the snow becomes essential; this does not only apply to troop movement and infantry fighting vehicles. Logistic support relies upon timely resupply at the edge of the battlefield, and vehicles such as the Small Unit Support Vehicle have proven invaluable for friendly force resupply and casualty backhaul. The threat will use similar vehicles in an equivalent manner. Radio retransmission, or retrans, in a snow-covered, mountainous environment will also require over-the-snow capability to ensure proper site emplacement for long-range, secure, line-of-sight voice communications. Reconnaissance elements must remain undetected, moving off route, and the only way to accomplish this in the subarctic is to use over-the-snow vehicles. However, intelligence analysts should not focus solely on movement and maneuver. Infantry Soldiers can walk on skis and snowshoes; food, water, fuel, and ammunition cannot—and that is where over-the-snow vehicles find their true value.

Although a threat template depicts a threat’s actions without the impact of the mission variables discovered in steps 1 and 2,<sup>14</sup> it is not prudent to use a typical threat template in an extreme environment. The topography is complex, the environmental conditions are unique, and the equipment used by the threat is often obscure. These factors contribute to an enemy playbook full of nonstandard threat templates that leverage creativity and the environment. Intelligence professionals should not dismiss the threat template but consider the unique challenges and assets presented. This will ensure a usable framework in step 4. Forcing the available threat templates to bend to the subarctic scenario will lead to failure.

Finally, the high-value target list, one of the culminating products of IPOE step 3, will likely emphasize over-the-snow capability at the tactical level above many of the more traditional tactical assets. Artillery, antiaircraft artillery, and command and control will remain essential to the enemy in the subarctic; nevertheless, moving on and accessing specific areas rely heavily on over-the-snow vehicles. Place these vehicles high on the high-value target list, especially if the asset is essential to resupply operations. Smaller vehicles, such as snowmobiles, may help move troops, but the threat commander can accomplish his mission without them. Larger tracked vehicles meant to move on snow are crucial for resupply and casualty evacuation. Consider these variables when populating the high-value target list.

## IPOE Step 4: Determine Threat Courses of Action

*Step 4 of the IPOE process identifies and describes threat COAs [courses of action] that can influence friendly operations.<sup>15</sup>*

The entire IPOE process converges at the threat course of action (COA). ATP 2-01.3, *Intelligence Preparation of the Operational Environment*, explicitly states that “the staff develops and prioritizes as many valid threat COAs as time allows but, at a minimum, develops the most likely and most dangerous COAs.”<sup>16</sup> Due to time constraints, many S-2 sections elect to produce only two threat COAs during step 4. However, operations in the subarctic contend with so many variables that the most likely and most dangerous COA cannot adequately cover potential threat tactics. Limiting COAs to two leaves a significant gap in the possible threat actions and disregards the creativity the threat commander can use in extreme environments.

Time-space analysis and battlefield geometry become much more essential in subarctic operations. An obstacle may slow down or slightly alter an enemy’s plan in a typical environment, but in the subarctic an obstacle can completely derail an operation. Snow, ice, and cold are enduring obstacles. Usually, they are not intentionally emplaced on a battlefield; in the subarctic, they *are* the battlefield. These environmental obstacles can cause a unit to abandon COAs completely. When conducting a time-space analysis using a map or other digital tools, it is prudent to overestimate the time a movement will take in subarctic conditions. Even over-the-snow vehicles can get bogged down and fail to move in specific types of dry snow. If the threat is on the offensive, do not assume they can move faster than 500 to 1500 meters per hour off-road, on foot, especially in hours of darkness. S-2 sections must access every piece of information available to determine the real-time, on-ground conditions and their impacts on the threat. The subarctic tends to fool even the best analysts into believing that conditions are much more tenable for movement than they truly are. Analysts should build these factors into their threat COAs, as the threat timeline will drive the friendly commander’s decision cycle.

## Conclusion

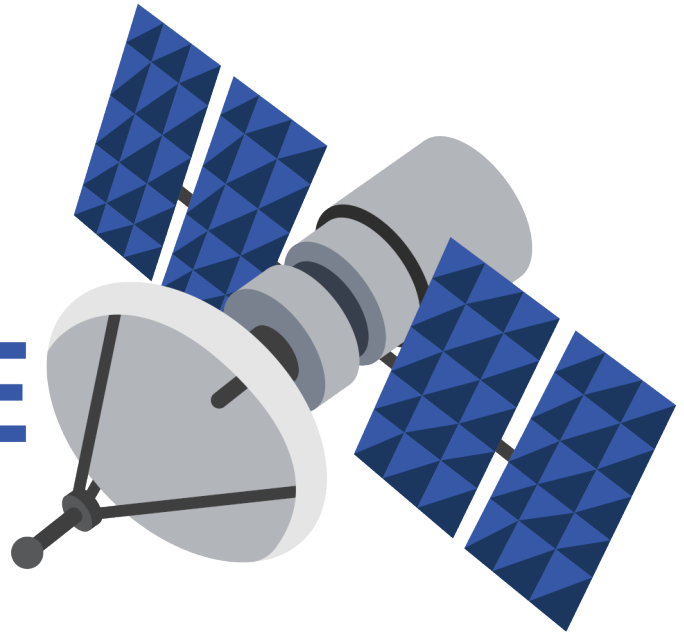
The subarctic is one of several extreme environments where intelligence professionals operate. Currently, there is no up-to-date manual highlighting special considerations for conducting IPOE in extreme environments, so the battalion and brigade S-2 section are responsible for adapting IPOE to the unique considerations of the subarctic at the tactical level. IPOE has a very scalable and adaptable framework. Still, military intelligence professionals working in the subarctic must think more creatively to adequately prepare their commanders and formations for the fight in this unforgiving environment. ❄️

## Endnotes

1. U.S. Army Northern Warfare Training Center, “Cold Weather (CWLC, CWOC, & CWIC)” (student handout, Cold Weather Training Course Winter 2022-2023, Black Rapids, AK, 2022), 5-6.
2. Department of the Army, Field Manual 2-0, *Intelligence* (Washington, DC: Government Publishing Office [GPO], 1 October 2023), 5-13.
3. German Army High Command, *Handbook on Winter Warfare*, trans. and ed. U.S. War Department Military Intelligence Division (Washington, DC: U.S. GPO, 1943), <https://archive.org/details/GermanWinterWarfare1943>.
4. George K. Swinzow, *Special Report 93-12: On Winter Warfare* (Philadelphia, PA: U.S. Army Corps of Engineers Cold Regions Research & Engineering Laboratory, 1993), <https://apps.dtic.mil/sti/pdfs/ADA270031.pdf>.
5. Department of the Army, Army Techniques Publication (ATP) 2-01.3, *Intelligence Preparation of the Operational Environment* (Washington, DC: GPO, 1 March 2019) 3-1. Change 1 was issued on 6 January 2021. Change 2 was issued on 23 January 2024.
6. Department of the Army, ATP 2-01.3, *Intelligence Preparation of the Operational Environment*, 4-1.
7. Department of the Army, ATP 3-90.97, *Mountain Warfare and Cold Weather Operations* (Washington, DC: GPO, 29 April 2016), 1-8.
8. Ibid.
9. “Earth Science Data Visualizations—How to Read a Heat Map,” Education, Jet Propulsion Laboratory California Institute of Technology, NASA, <https://www.jpl.nasa.gov/edu/teach/activity/earth-science-data-visualizations-how-to-read-a-heat-map/>.
10. Department of the Army, ATP 3-90.97, *Mountain Warfare and Cold Weather Operations*, 2-1.
11. Ibid., 1-8.
12. Department of the Army, ATP 2-01.3, *Intelligence Preparation of the Operational Environment*, 5-1.
13. OE Data Integration Network (ODIN), U.S. Army Training and Doctrine Command, version 3.10.1, <https://odin.tradoc.army.mil>.
14. Department of the Army, ATP 2-01.3, *Intelligence Preparation of the Operational Environment*, 5-18.
15. Ibid., 6-1.
16. Ibid., 6-7.

MAJ Michael Everett is currently attending the College of Naval Command and Staff for Intermediate Level Education. He previously served as the Military Intelligence Company Commander in the 2<sup>nd</sup> Infantry Brigade Combat Team (Airborne), 11<sup>th</sup> Airborne Division at Joint Base Elmendorf-Richardson (JBER), AK. Additionally, he served as the S-2 in 1<sup>st</sup> Squadron, 40<sup>th</sup> Cavalry at JBER, AK and as an assistant S-3, platoon leader, and executive officer in 1<sup>st</sup> Infantry Brigade Combat Team, 10<sup>th</sup> Mountain Division (Light Infantry) at Fort Drum, NY. He recently earned his master’s degree in Intelligence Studies.

# INTEGRATING SPACE DOMAIN CONSIDERATIONS INTO INTELLIGENCE PREPARATION OF THE OPERATIONAL ENVIRONMENT



FIRST LIEUTENANT TAYLOR A. REIHELD  
& CHIEF WARRANT OFFICER 3 ANDREW R. GARLAND

## Introduction

The importance of the space domain to the 21<sup>st</sup>-century military has been well-documented and thoroughly described. Unfortunately, all too often it is considered a separate entity, distinct from the established warfighting functions. This is, however, a misguided perception. In fact, the space domain provides both complementary and reinforcing capabilities to the warfighting functions. This artificial distinction leads to many aspects of the space domain being overlooked or inconsistently applied, if not intentionally disregarded, especially among the warfighting elements whose connection to space may not be immediately apparent.

Maneuver commanders have a variety of factors to consider as they make decisions. They rely on their intelligence staff to supply fully developed intelligence preparation of the operational environment (IPOE) products to support that decision making. The intelligence staff can improve their standard IPOE products by integrating space domain considerations. They can then present these products to maneuver commanders in familiar ways without requiring any specific training.

## Intelligence Preparation of the Operational Environment

Chapter 8 of ATP 2-01.3, *Intelligence Preparation of the Operational Environment*, contains considerations for the space domain within operational environments. It focuses on the relevant physical aspects of the environment, space weather, and space weather phenomena.<sup>1</sup> This article, while not claiming to be all-inclusive, intends to expand the Army Techniques Publication's discussion.

**Step 1: Define the Operational Environment.** Analysts can incorporate space domain considerations meaningfully when describing the significant characteristics of the area of interest and the area of operations. Topography, terrestrial weather, and space environmental effects can all affect signal transmission between orbiting satellites and the users below. Will the sheer size of the area of operations require satellite-enabled communication? Does the area of operations include terrain features that could inhibit direct, point-to-point communications? Will the prevailing climate conditions influence those communications? Analysts should also consider space-related

facilities when assessing critical infrastructure, as an unassuming neighborhood office building could be the access point to worldwide communication and influence.

## **Step 2: Describe the Environmental Effects on Operations.**

The five military aspects of terrain are observation and fields of fire, avenues of approach, key terrain, obstacles, and cover and concealment, commonly referred to by the acronym OAKOC.<sup>2</sup> Space domain considerations influence all five aspects, which can, in turn, influence some space systems.

**Observation and Fields of Fire.** Space-based and space-enabled assets can expand the conditions under which the battlefield can be observed. Radar can penetrate cloud cover, haze, smoke, darkness, and even foliage to provide persistent, near real time observation beyond line-of-sight. The commercialization of space has made these capabilities available to nonstate actors and states that may not have access to governmental reconnaissance satellites. At least one commercial imagery provider offers synthetic aperture radar imaging with frequent updates available.<sup>3</sup>

**Avenues of Approach.** Space-based and space-enabled assets can also shed new light on potential ground-based avenues of approach. Besides the obvious benefit from updated overhead photography, commercially available assets can provide polarized imagery. Polarization can help, for example, by differentiating between trafficable grassland and severely restricted forests, despite both appearing as similar “green spaces” on overhead visual imagery.

**Key Terrain.** Key terrain can include threat communications nodes that restrict information flow. At least seven countries have tried, or intend to try, to isolate their civilian population by restricting internet connectivity through a centralized, state-controlled infrastructure.<sup>4</sup>

**Obstacles.** Electromagnetic obstacles are an entirely new entry in this category. Intentional adversary action is a more usual concern, but terrain conditions can also impinge electromagnetic signals. Most notably, global positioning systems (GPS) are susceptible to multipath errors, which occur when a GPS signal reflects to a GPS receiver and provides information based on the reflected location instead of the actual location. This is a common phenomenon in cities, where the vertical metal and concrete in tall buildings and overpasses create “urban canyons” that can confuse and disorient GPS systems, but the issue can also arise over mountainous terrain, cliffs, and lakes. Inaccurate positioning can have disastrous consequences. As an example, the margin of error roughly doubles for GPS position fixes taken under coniferous trees versus open areas.<sup>5</sup> Careful terrain analysis should include areas where GPS signals may be disrupted or degraded, and these areas can be depicted on the modified combined obstacle overlay in the same way as restricted terrain.

**Cover and Concealment.** Traditional obscuration and camouflage can be effective from ground level but may present a different view to overhead assets. Space platforms surround the planet without regard for borders and boundaries, potentially providing adversaries with clear views of concealed positions. Additionally, space-based platforms may offer added sensor capabilities, unlike those expected to be available to the adversary. For example, as previously mentioned, commercial assets can provide polarized imagery that may discern differences between foliage and camouflage netting, with its value limited only by the turnaround time from imaging to exploitation.

**Space Environmental Effects.** Events in the space environment, sometimes known as “space weather,” can impact maneuver operations. Radio and navigation signals can be disrupted, high-altitude aircraft in support roles may have to alter flight plans, and intelligence, surveillance, and reconnaissance (ISR) capabilities provided by satellites may be degraded by space weather. To varying degrees, analysts can incorporate these effects into the weather brief and weather effects matrix using information provided by the National Oceanic and Atmospheric Administration’s Space Weather Prediction Center.<sup>6</sup>

Just as the space environment can affect terrestrial operations, the terrestrial environment can affect space operations. For example, some space assets are enabled by mobile transporter-erector-launcher vehicles, which are constrained by the well-known vulnerabilities inherent to ground vehicles. As another example, anyone who has used a modern satellite television service understands how severely Ku band frequencies can be affected by moderate to heavy rain. The high bandwidth of the Ku band makes it attractive for deployable satellite communication, but the wavelength is especially susceptible to interference from rain.<sup>7</sup>


**Step 3: Evaluate the Threat.** The purpose of this step is to identify capabilities available to the threat, and that must include space-enabled capabilities. Does the adversary have access to precise positioning, navigation, and timing? Can the adversary access national or commercial imagery sources to support their version of IPOE? Predicted overflights of adversary satellites are available using satellite reconnaissance advanced notice reports from the Army Space Support Team, typically found at echelons division and above.<sup>8</sup>

High-value and high-payoff targets are identified in this step and could include access points for space-based capabilities. For example, disrupting the electrical supply to a ground station could neutralize an otherwise unreachable multimillion-dollar orbital platform. The type, quantity, status, and location of any GPS and satellite communications signal jamming equipment should be identified to the greatest extent possible.



**Step 4: Determine Threat Courses of Action.** It is unlikely that space-enabled assets will significantly alter the adversary's objectives and desired end-state, but they could influence the selection of specific courses of action. Improved ISR may allow the adversary greater situational awareness, thereby increasing the feasibility of some courses of action. To properly consider the feasibility of potential threat courses of action, they should be fully developed so the impact of space-enabled assets is discernible. The likely courses of action should be compared to determine where events may occur that would differentiate between the potential courses of action. This will help support intelligence planning and collection.

## Conclusion

The traditional steps of IPOE are complete, but the process is cyclical and iterative. As time and information allow, continue to refine and develop the product. Incorporating space domain considerations into this iterative process as early as possible can only improve the commander's decision making. 

## Endnotes

1. Department of the Army, Army Techniques Publication (ATP) 2-01.3, *Intelligence Preparation of the Operational Environment* (Washington, DC: Government Publishing Office, 1 March 2019), 8-4. Change 1 was issued on 6 January 2021. Change 2 was issued on 23 January 2024.

2. Department of the Army, ATP 2-01.3, *Intelligence Preparation of the Operational Environment*, 3-6.

3. Umbra Lab, Inc., <https://www.umbra.space/>.

4. Liam Scott, "Repressive Regimes around the World Are Nationalizing the Internet and Isolating People," *Authoritarian Tech*, Newsletter, Coda, 18 October 2022, <https://www.codastory.com/newsletters/breaking-up-global-internet/>.

5. Christopher Deckert and Paul Bolstad, "Forest Canopy, Terrain, and Distance Effects on Global Positioning System Point Accuracy," *Photogrammetric Engineering & Remote Sensing* 62, no. 3 (March 1996): 317-321, [https://www.asprs.org/wp-content/uploads/pers/1996journal/mar/1996\\_mar\\_317-321.pdf](https://www.asprs.org/wp-content/uploads/pers/1996journal/mar/1996_mar_317-321.pdf).

6. Space Weather Prediction Center, National Oceanic and Atmospheric Administration, <https://www.swpc.noaa.gov/>.

7. Patrick Gannon, "What Is Rain Fade?" *Satellite Industry Latest* (blog), *BusinessCom Networks*, 14 February 2018, <https://www.bcsatellite.net/blog/what-is-rain-fade/>.

8. "Army Space Forces—Enabling the Joint Warfighter," Association of the United States Army Background Brief No. 100, October 2004, <https://www.ausa.org/sites/default/files/BB-100-Army-Space-Forces.pdf>.

*1LT Taylor A. Reiheld is an intelligence officer and assistant S-2 for the 1<sup>st</sup> Space Brigade at Fort Carson, CO. She holds a bachelor's degree in construction management.*

*CW3 Andrew R. Garland is an all-source intelligence technician assigned to the 1<sup>st</sup> Space Brigade S-2 at Fort Carson, CO. He previously provided intelligence support at the battalion, division, combatant command, and national agency levels, including three combat deployments. He holds a master's degree in U.S. history.*



# Contact & Article

## Submission Information



*This is your professional bulletin. We need your support by writing and submitting articles for publication.*

**When writing an article, select a topic relevant to Army MI professionals.**

Our goals are to spark discussion and add to the professional knowledge of the MI Corps and the intelligence community. Articles about current operations, TTPs, and equipment and training are always welcome as are lessons learned, historical perspectives, problems and solutions, and short “quick tips” on better employment of equipment and personnel. Explain how your unit has broken new ground, give helpful advice on a specific topic, or discuss how new technology will change the way we operate.

**When submitting articles to MIPB, please consider the following:**

- ◆ Feature articles, in most cases, should be between 1,000 and 3,000 words, double-spaced with normal margins without embedded graphics.
- ◆ We cannot guarantee we will publish all submitted articles.
- ◆ Please do not send overly large and complicated or small print graphics/PowerPoint slides. What looks good as a PowerPoint presentation doesn't always translate well to an 8 1/2" x 11" article format.
- ◆ 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 memorandum is available from the MIPB Staff. Contact us at the email address at the bottom of the page.
- ◆ **(Within USAICoE)** Contact the Doctrine/MIPB staff (at 520-533-3297) 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@army.mil](mailto:usarmy.huachuca.icoe.mbx.mipb@army.mil). For any questions, email us at the above address or call 520-533-7836/DSN 821-7836.



**MIPB**  
**DOTD, USAICoE**  
**550 Cibique St.**  
**Fort Huachuca, AZ 85613-7017**

**Headquarters, Department of the Army.**  
**This publication is approved for public release.**  
**Distribution Unlimited**

**PIN: 220127-000**