
MILITARY INTELLIGENCE
PROFESSIONAL BULLETIN
JULY
—
DECEMBER
2025
COLLECTION

Jimmy Carter and United States officials meet with the Shah of Iran and Iranian officials. Taken on December 31, 1977, brightened for visual clarity. (Photo courtesy of National Archives and Records Administration, colors adjusted by MIPB staff)

Reclaiming Strategic Imagination: Enhancing U.S. Military Planning and Execution

by Captain Nader Z. Badran

Introduction

In recent years, the U.S. military has faced considerable challenges in maintaining effective and insightful strategic analysis at the operational and tactical levels. This stagnation is often attributed to H.R. McMaster's "strategic narcissism" concept, which describes the tendency to view all potential adversary actions or end states primarily from the perspective of their effects on the United States or Western goals.[1] The problem is exacerbated by a lack of deep strategic understanding of the adversary's capabilities and goals at operational and tactical levels, leading to overly simplistic analyses focused narrowly on when and where the enemy "will attack" without a broader contextual analysis of the adversary's overall strategic goals, history, and priorities.

The focus on immediate capabilities and probabilities, to the exclusion of detailed evaluation of historical context and actual end states, leads to the repetition of assessments like "the enemy will attack in the next 12 to 48 hours," which assume a considerable number of strategic goals in the ultimately tactical and capabilities-based conclusion of why, or even if, the enemy will attack. These bottom-line assessments are often wrong, and even when accurate, they do little to inform higher-level strategy beyond the immediate tactical area of operations. This leads to a top-down "Simon says" analytical framework in the way intelligence assessments are briefed.

Left: A protester giving flowers to an army officer during the Iranian revolution. Right: Iranian armed rebels during the Iranian revolution. (Public domain photos from Wikipedia)

This article proposes that revitalizing strategic imagination requires rededication to a nuanced understanding of adversaries' end states, historical contexts, adaptive planning, and the capacity to anticipate and adapt to unpredictability in warfare. Conducting capabilities-based assessments without a deep understanding of context, end states, and imagination is not analysis but merely reporting.

The Role of Historical Context in Strategic Analysis

Historical context plays a critical role in strategic analysis but frequently gets short treatment compared to capabilities-based bottom-line upfront assessments in a tactical setting. Wars and conflicts often arise from deep-seated geopolitical, cultural, and ideological tensions; ignoring these historical dynamics can obscure essential insights into adversarial behavior.

To illustrate this point, Iran's ambitions are shaped by a unique historical trajectory, including its traditional rivalries, colonial experiences, and the Islamic Revolution of 1979. The 1953 Central Intelligence Agency-led coup that overthrew Prime Minister Mohammad Mossadegh left a legacy of distrust of Western powers and further solidified Iran's anti-Western stance, as well as its desire to project power in the Middle East—not by modeling foreign relations on international norms, but by possession of the means and methods to exclude foreign influence. These events point to a deep, long-standing mistrust of what are often pitched by Western powers as neutral or status quo solutions based on international conventions and diplomacy. While a fair interpretation may be that Iran distrusts Western powers, an equally fair reading might be that Iran has a cultural mistrust of any security arrangement based on agreements since, historically, such arrangements have failed miserably to protect its interests. Understanding this historical context allows analysts to better grasp the motivations behind Iran's actions and craft more nuanced and compelling responses rather than assuming that Iran is simply hostile to every United States force in the area as its de jure enemy.

Unmasking the Adversary's Desired End State

A fundamental aspect of effective strategic planning is accurately identifying an adversary's end state. U.S. military analysts at the operational and tactical levels often view adversarial goals through a Western-centric lens, leading to a simplistic and flawed understanding of their motivations. Additionally, Western military strategy focuses on capabilities and effects, leading analysts to believe that our bigger guns will always win the fight. This reductive analysis results in low-value assessments, which add little to raw analysis. Where, how many, and what kind of equipment the adversary possesses is certainly important information, but it is simply regurgitated data. Proper analysis requires understanding how all this data plays into the adversary's end state. The current conflict with Iran demonstrates flawed binary reasoning: Iran opposes the United States; therefore, every end state necessarily involves attacks on United States troops. While it is true that Iran often directs its network of militias to attack American troops, it is equally valid that Iran's goals are more complex than merely opposing America—and some of their most important goals are achieved without attacks at all.

Analysts have consistently underestimated Iran's ambitions to establish itself as a dominant regional power, driven by a complex interplay of religious ideology, historical grievances,

and nationalistic pride. Iran's end state involves more than mere survival or military dominance; it seeks to fundamentally reshape the Middle East according to its vision of an Islamic Republic that challenges Western influence. Iran's support for proxy groups across the region is part of a broader strategy to influence regional politics and shift the balance of power in its favor, irrespective of that end state's ultimate effect upon the United States. Analysts who fail to grasp this underlying motivation may misinterpret Iran's actions as reactionary or opportunistic rather than as part of a long-term strategy for regional dominance. For example, Iran's support for groups like Hezbollah and the Houthis is not only about immediate military objectives but also about building a network of influence that extends Iran's reach and destabilizes rival powers, regardless of individual tactical engagements by the proxies and equally unrelated to whom those proxies target.

If we view the proxies as Iran's public projection of force, in the same way that a United States carrier group is a representation of American power, their mere existence and presence are as helpful as their actual utilization because the goal is to demonstrate regional influence more than to achieve specific tactical objectives. Understanding this intent is crucial for accurate assessments and effective counterstrategies. This is especially true when Iran's interests align with those of other regional actors—for example, Hamas—with little or no interest in United States troops.

While Iran and Hamas may align against common adversaries, conflating their ultimate strategic goals can lead to significant miscalculations because one involves direct conflict with United States troops, and one does not. Iran's goals focus on establishing itself as a dominant regional power with substantial influence over the Middle East. In contrast, Hamas is a militant Palestinian organization focused on issues related to Palestinian self-determination and resistance against Israeli occupation. Hamas's goals revolve around achieving Palestinian statehood and resisting Israeli control over Palestinian territories. While Hamas and Iran occasionally cooperate, their objectives are fundamentally different. Hamas's focus is on the Israeli-Palestinian conflict and Palestinian sovereignty, while Iran's ambitions are broader, aiming to reshape the balance of power in the Middle East.

Understanding this distinction is crucial for U.S. military analysts. Misinterpreting the alignment between Iran and Hamas as indicative of a unified strategy can lead to flawed analysis. For instance, Israeli actions targeting Hamas might not necessarily affect Iran's broader regional ambitions and could even strengthen Iran's position if it appears as a defender of Palestinian causes. Accurate differentiation between countering Iran's regional hegemony and addressing the Israeli-Palestinian conflict requires that analysts have a deeper understanding of the regional actors' goals, which, in turn, requires a renewed and deeper focus on history and context instead of capabilities and reassessing the assumption that every adversary of the United States is working in concert. Arming our tactical and operational analysts with a deeper understanding of the adversary's objectives and strategic aspirations allows them to craft more astute analyses.

Backward Planning: A Useful Tool for Analysts

As determined through historical context, the end state provides the raw material for one of a planner's most important tools: backward planning. Backward planning is a strategic process that begins with an adversary's end state and works backward to identify potential actions and interventions. For Iran, this involves first understanding its goal of regional dominance and influence, which includes supporting proxy groups, leveraging economic sanctions as propaganda, and manipulating regional conflicts. Without this historical context, backward planning is starved of the antecedent facts necessary to make the assumptions required to use the process effectively. In other words, backward planning enables military planners to anticipate Iran's moves by considering how the country might use its resources and influence to achieve its strategic objectives based on its end-state goals, which are, in turn, based on historical context. For example, if Iran aims to project power through proxy groups, planners can anticipate where these proxies might be active and develop countermeasures accordingly. By adopting this approach, planners can improve their strategic foresight and prepare more effectively for potential scenarios beyond merely reacting to specific tactical objectives by any single proxy.

Understanding Flukes

Finally, the analyst or planner must acknowledge the predictably unpredictable nature of the strategic environment. In his 2024 book *Fluke: Chance, Chaos, and Why Everything We Do Matters*,[2] Brian Klaas includes one striking example of how small, seemingly random events can shape history. During World War II, United States Secretary of War Henry Stimson was deeply involved in discussions surrounding the use of atomic bombs in Japan. Stimson had a personal connection to Japan: he and his wife had visited Kyoto during a pre-war trip and developed a fondness for the city's cultural and historical significance. This personal experience led Stimson to advocate strongly for sparing Kyoto from the bombing list, citing his affection for the city and the memories of his visit with his wife. As a result, Kyoto was removed from the list of potential targets for the bomb, and Hiroshima became one of the final cities selected.

Klaas uses this anecdote to illustrate how chance and personal experience can dramatically shape decisions that have profound global consequences. In this case, one man's attachment to a place helped determine the course of history, demonstrating how individual human choices, shaped by

unpredictable life events, can have monumental impacts in war's chaotic and complex context. This example underscores the need for flexibility in planning at all levels, as fluke events can dramatically alter the strategic landscape. Planners must be prepared to adapt to sudden changes and reassess strategies in light of new developments. To do this, planners must concern themselves with history, culture, and societal influences as much as capabilities and probabilities. Knowledge of the personalities and histories of the leaders and significant actors is also a critical element in effective analysis, but one which is often simply not included in typical tactical briefings.

Summary

Reclaiming strategic imagination among tactical and operational analysts requires a nuanced understanding of adversaries' historical contexts, end-state goals, and the ability to anticipate and adapt to unpredictable events. By integrating these elements into military operations and incorporating backward planning from the adversary's perspective, U.S. military leaders can make more informed, flexible, and creative decisions. This approach not only enhances the effectiveness of military strategy but also ensures that the United States remains adaptable in the face of evolving threats and dynamic geopolitical environments. For the intelligence community, this means fostering a culture of strategic imagination that embraces complexity and unpredictability, ultimately leading to more robust and resilient defense strategies.

Endnotes

1. H.R. McMaster, *Battlegrounds: The Fight to Defend the Free World* (New York: Harper Collins Publishers, 2020).

2. Brian Klaas, *Fluke: Chance, Chaos, and Why Everything We Do Matters* (New York: Scribner, 2024).

CPT Nader Badran is the officer in charge for the Joint Security Area Analysis Branch, U.S. Army Europe and Africa Theater Analysis and Control Element, 24th Military Intelligence Battalion, 66th Military Intelligence Brigade-Theater. He previously served as the brigade S-2, 401st Army Field Support Brigade at Camp Arifjan, Kuwait.

THE MARKET KNOWS BEST: USING DATA FROM PREDICTION MARKETS TO ASSESS NATIONAL SECURITY THREATS

by Commander Stephen P. Ferris, U.S. Navy (Retired)
and Captain Raymond M. Ferris, U.S. Army

Introduction

Prediction markets, also known as information markets or event futures, are being used to forecast events as diverse as sporting outcomes, election results, macroeconomic forecasts, and geopolitical events.[1] By aggregating diverse opinions and incentivizing prediction accuracy with financial gain through successful trading, these markets demonstrate remarkable usefulness and accuracy. The data generated by contract trading in prediction markets can serve as a new source of information for intelligence analysts to identify and assess national security threats. Platforms like Polymarket and Kalshi,[2] which allow trading on a wide range of event-based contracts, provide an opportunity for intelligence professionals to collect a novel type of data to identify new threats and assess the changing nature of existing national security risks.

In this article, we begin by explaining the nature of a prediction market and how it operates. We then discuss the information that intelligence analysts can extract from contract trading in these markets, as well as the types of contracts that analysts will find most useful. We'll review the techniques intelligence analysts can apply to this data to enhance the quality of their analyses, then move on to a discussion of how prediction market data can be integrated with traditional sources of military intelligence, with a specific focus on all-source analysis. Finally, we'll conclude with commentary on how prediction markets might evolve in the future and their increasing relevance to intelligence professionals.

Understanding Prediction Markets

Prediction markets operate on the principle that collective intelligence, when combined with financial incentives, can yield highly accurate forecasts.[3] Participants buy and sell contracts based on their expectations of future events. The mechanics of these markets are designed to ensure efficiency and accuracy. Each contract represents a binary outcome—the event either occurs or it doesn't. When the event occurs, the contract pays $1; if it doesn't occur, the contract pays nothing. This simple pay-off scheme creates a direct relationship between contract prices and probability estimates. For example, a contract trading at $0.45 suggests the market estimates a 45 percent chance of the event occurring.

Polymarket, the world's largest prediction market platform, offers investors a wide array of contracts to trade covering issues such as elections, economic indicators, and geopolitical developments. The data generated through trading provides valuable insights into the collective expectations of informed individuals. This effect is comparable to the "wisdom of crowds" as described by James Surowiecki in his 2004 book of the same title.[4]

What makes prediction markets especially informative is their self-correcting nature. If participants believe a contract is mispriced relative to the true probability of an event, they have a financial incentive to trade and move the price toward what they believe is the correct probability. This process, known as price discovery, helps ensure that contract prices reflect the most current information available about an event.[5]

The liquidity and trading volume of contracts in a prediction market also provide important signals.[6] Higher trading volumes typically indicate greater certainty or interest in an outcome, while lower volumes might suggest uncertainty or a lack of investor concern about the event. Market participants provide initial liquidity for each contract and help to establish baseline probabilities of the event's occurrence. These probabilities change over time as new information is revealed; traders react to these changes by buying and selling the specific event's contract.

Usefulness of Contract Trading Data

Prediction markets function on data that intelligence professionals do not commonly collect or analyze. Unlike traditional intelligence sources, which often rely on classified information, technical surveillance, or field reports, prediction

markets aggregate insights from both the public and private sectors, drawing on multiple participants. These participants include subject matter experts, analysts, and informed individuals who may possess unique perspectives or early indicators of emerging threats.

What makes prediction market data especially distinctive is its dynamic, real-time nature. As new information becomes available or sentiments shift, contract prices adjust. Because this information directly affects potential profit, these price changes occur almost instantaneously. This immediate response contrasts with the slower, often bureaucratic processes of traditional intelligence collection.

For example, Figure 1 illustrates the time series of an event contract offered by Polymarket. The contract concerns the likelihood of a ceasefire between Russia and Ukraine in 2025. Probability varies as new information becomes available, causing the contract price to respond accordingly. For instance, we observe a high likelihood of a ceasefire in December 2024, followed by a decline in early January 2025. From mid-January through early February, the possibility of a ceasefire gradually increases, approaching its previous high. This behavior is consistent with the *efficient market hypothesis* developed by economist Eugene Fama in 1970 to explain how prices in financial markets change in response to the arrival of new information.[7] The changing likelihood of an event, as reflected in market trends, can be beneficial to intelligence analysts in assessing the risk associated with a specific threat.

The price of a contract in a prediction market reflects the synthesized expectations of market participants. It provides a probabilistic assessment based on a consensus of the contract investors' beliefs. This data can offer intelligence analysts new perspectives, enabling them to detect early warning signals, confirm other intelligence sources, or uncover trends that might otherwise be overlooked. By integrating this new data, intelligence analysts can exploit the collective foresight and knowledge embedded in event contract prices to more fully anticipate national security threats.

Contracts Most Useful for Intelligence Assessment

Within the broad spectrum of prediction market contracts, certain types of contracts are particularly valuable for military intelligence.[8] These contracts provide targeted insights into specific national security concerns, offering actionable intelligence that can improve threat identification and inform strategic response.

Contracts predicting the likelihood of military conflicts between nations or within regions are of critical importance. For example, contracts focused on potential escalations in regions such as the Korean Peninsula, the South China Sea, or Eastern Europe can provide early indicators of rising tensions. Monitoring these contracts can help intelligence analysts anticipate conflicts that may require U.S. military intervention or impact global stability.

Contracts that predict changes in political leadership, such as elections, coups, or resignations, are crucial for understanding potential shifts in national policies or alliances. A contract forecasting the likelihood of a regime change in a Middle Eastern country, for instance, can signal impending shifts in diplomatic relations, security agreements, or regional power dynamics.

Prediction markets often feature contracts related to the imposition or lifting of economic sanctions and trade restrictions. These contracts can assess the likelihood of economic sanctions on an adversarial country or how such activities might influence their foreign policy or military actions. For example, contracts predicting sanctions on Iran's oil exports can provide insights into potential retaliatory actions taken by the Iranian government.

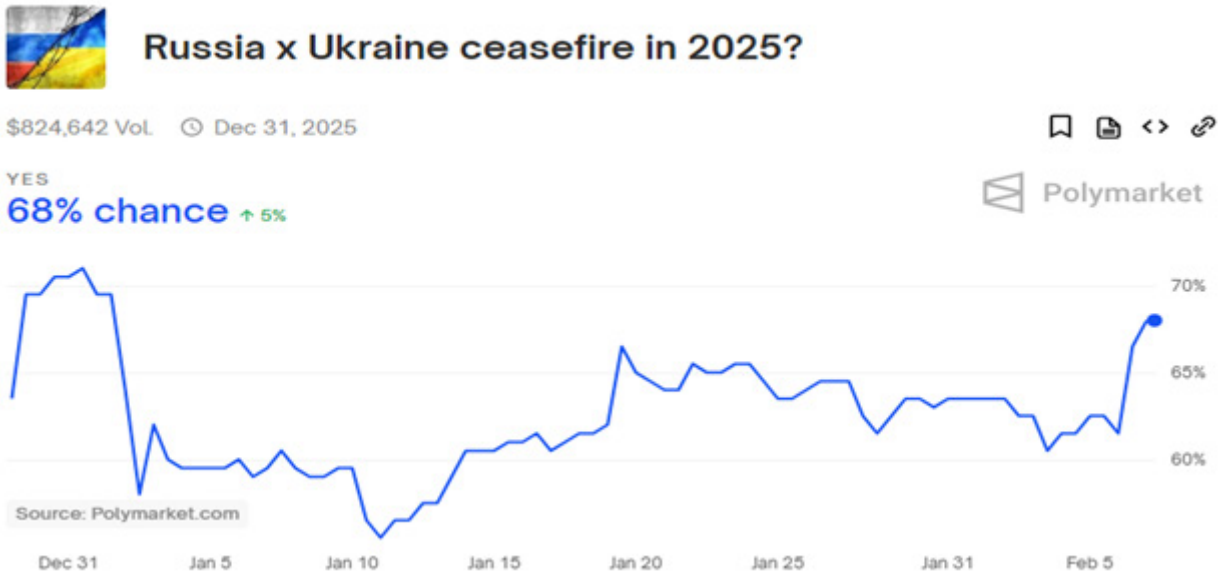


Figure 1. Contract price trend as a predictor of a Russia x Ukraine ceasefire by Polymarket, February 2025

While specific terrorist attacks are difficult to predict, contracts that gauge the overall activity levels of terrorist organizations or insurgent groups can be informative. Contracts predicting the frequency of attacks in specific regions or the operational capacity of groups like ISIS or Al-Qaeda can help intelligence analysts allocate resources and anticipate threats. Contracts predicting major cyberspace attacks on government institutions, critical infrastructure, or multinational corporations offer valuable insights into emerging cybersecurity threats. For example, a contract forecasting a significant breach of a U.S. government agency can alert intelligence analysts to potential vulnerabilities or adversary capabilities in the cyberspace domain.

Although natural disasters are not typically considered security threats, their aftermath can create conditions that are ripe for instability. Contracts predicting the likelihood of natural disasters or humanitarian crises in politically sensitive regions can help intelligence analysts prepare for secondary security challenges, such as mass migrations, resource conflicts, or opportunistic actions by hostile states or organizations.

The COVID-19 pandemic (March 2020–May 2023) demonstrated the impact that public health crises can have on national security. Contracts that predict the outbreak or spread of infectious diseases, particularly in regions with weak healthcare infrastructures, can help identify potential security challenges related to civil unrest, economic disruption, or strained international relations.

In Figure 2, we provide a small sample of contracts focused on geopolitical risk that were trading on Polymarket in early February 2025. We immediately noted the variety of contracts available for trade. The events varied across the globe and were of a military, political, or diplomatic nature. For some events, such as the Russian recapture of Sudzha, there were multiple contracts based not on whether the event would occur, but on the *date* by which the event would occur. Furthermore, some markets, for instance Kalshi, invite proposals for new contracts on events that have not been previously introduced.[9]

Using Data from Contract Trading

Intelligence professionals can utilize information from prediction markets to refine their threat assessments by applying various analytical techniques to the data. Trend analysis can track changes in the probability of an event over time. For instance, if contracts predicting a military conflict in the South China Sea show a steady increase in likelihood, this trend may indicate escalating tensions that are not yet apparent in traditional intelligence. By monitoring these shifts, analysts can identify emerging threats earlier and redistribute surveillance resources more effectively.

Contract Event	Dollar Trading Volume	Probability of Event Occuring Based on Market Trading
Will China invade Taiwan in 2025?	$1,102,655	13%
Nuclear weapon detonation in 2025.	$223,013	19%
Khamenei out as Supreme Leader of Iran by June 30.	$237,929	22%
NATO/EU troops fighting in Ukraine in 2025.	$8,571	12%
Will Russia recapture Sudzha by February 2?	$42,629	2%
Will Russia recapture Sudzha by April 30?	$20,400	25%
Will Russia recapture Sudzha by June 30?	$1,909	59%

Figure 2. Select contracts trading on Polymarket, February 2025 (figure adapted from authors' original)

Cross-market comparisons are particularly useful when analyzing interconnected events. For example, if prediction market contracts indicate a rising likelihood of economic sanctions against a country but a stable or declining probability of that country responding with military action, intelligence analysts might conclude that economic retaliation is more probable than military action. This comparative analysis of related contracts provides a broader strategic context for any single event.

Anomaly detection involves identifying sudden or unexpected changes in market behavior. A sharp increase in the probability of a terrorist attack in a specific region, for example, might suggest that market participants have gained new information about the likelihood of this event. This price data may then prompt a request for further verification through more traditional intelligence channels, such as signals intelligence (SIGINT) or human intelligence (HUMINT).[10]

Sentiment analysis evaluates the confidence and consensus among market participants. A high volume of trading with consistent probability levels might indicate a strong consensus regarding an event's likelihood. Volatile trading patterns, however, might imply uncertainty or conflicting information. These probabilistic assessments complement traditional intelligence analysis by identifying risks where consensus is strong or additional collection is necessary.[11]

Integrating Prediction Market Data with Traditional Military Intelligence

Prediction market data, while valuable on its own, becomes significantly more useful when integrated with traditional intelligence sources.[12] By combining this data with that obtained from other channels, analysts can develop a more comprehensive threat assessment.

HUMINT, which involves gathering information from human sources such as informants, defectors, and local populations, can be enriched by prediction market data. For instance, if prediction contracts suggest an increasing probability of a coup in a particular country, HUMINT resources can be directed to verify this by interacting with local contacts and generating field reports. Conversely, insights from HUMINT can validate or challenge conclusions drawn from the price behavior of event contracts. This creates a feedback loop that enhances the usefulness of both sources.

SIGINT involves intercepting communications and electronic signals to gather intelligence. Contract prices in prediction market trends can guide SIGINT efforts by highlighting areas of increased risk or emerging threats. For example, if a contract's price implies a high likelihood of a cyberattack on critical infrastructure, SIGINT operations can prioritize scanning for corroborating evidence.

Open-source intelligence (OSINT) involves analyzing publicly available information from media, social networks, and other open sources. Contract price data can help evaluate and contextualize OSINT efforts. If contract data indicates escalating tensions in a region, OSINT analysts can focus on tracking news reports, social media activity, and public statements from key figures to gather continuing intelligence.

Geospatial intelligence (GEOINT) uses satellite imagery, maps, and geospatial data to analyze physical environments. Contract data from prediction markets that signal an increasing likelihood of potential military movements or conflicts can prompt targeted focusing of satellite imagery to detect pending military action. Conversely, unexpected observations in GEOINT data can trigger a review of price movement in related contracts to confirm any initial assessments.

Measurement and signature intelligence (MASINT) focuses on detecting and measuring physical phenomena, such as radiation, chemical signatures, or acoustic signals. Event contracts that forecast specific threats, such as the use of chemical weapons, can guide MASINT efforts to monitor for relevant signatures. In turn, MASINT data can validate or contradict the expectations implied by contract prices, thus enhancing the analyst's overall situational awareness.

Integrating with All-Source Analysis

All-source intelligence analysis integrates data from multiple collection disciplines, including HUMINT, SIGINT, OSINT, GEOINT, and MASINT, to develop a comprehensive threat assessment. By combining these distinct intelligence streams, analysts can overcome the inherent limitations of any single collection method while leveraging the unique strengths of each approach. The addition of contract price data offers several distinct advantages that enhance the quality of these intelligence assessments.

Data from event contracts complements traditional all-source analysis in three primary ways. First, it provides quantitative probability assessments derived from aggregated expert knowledge that often includes perspectives not captured by conventional intelligence collection. For example, when a contract's price rises from $0.15 to $0.68 over three weeks, this represents a measurable change in the collective risk assessment that can be evaluated against other intelligence indicators.

Second, prediction markets demonstrate exceptional speed in information integration, complementing the longer processing cycles typically associated with traditional intelligence collection. While HUMINT verification may require weeks and SIGINT analysis demands extensive processing, prediction markets provide near-instantaneous probability assessments as new information becomes available. This rapid response helps identify emerging threats that might warrant increased collection through traditional channels.

Third, event contract data serves as a correlation measure within the all-source framework. Alignment between market pricing data and traditional intelligence indicators strengthens analytical confidence. Divergence can highlight gaps requiring additional investigation.

The effective integration of contract data from prediction markets enhances all-source analysis through:

- **Independent Validation.** Market-based probability assessments provide verification mechanisms for hypotheses developed through traditional analysis. These assessments are particularly valuable in complex scenarios where conventional intelligence collection is limited.
- **Collection Gap Identification.** Significant movements in contract prices can highlight areas where traditional collection efforts might be insufficient. This suggests specific directions where more focused allocation of intelligence resources is needed.
- **Analytical Timeline Compression.** The rapid price discovery mechanism of prediction markets provides early warning indicators that complement longer-cycle collection methods, allowing earlier threat identification and response planning.

When properly integrated into all-source analysis, prediction market data provides quantifiable probability assessments while capturing diverse perspectives that might be inaccessible through traditional collection methods. This complementary relationship enhances both the scope and depth of a threat assessment while offering valuable cross-validation mechanisms for conventional intelligence sources.

Conclusion and Discussion

Prediction markets represent a useful, yet underutilized, dataset for enhancing national security intelligence collection and analysis. Platforms like Polymarket and Kalshi offer unique advantages through their ability to aggregate diverse perspectives, provide real-time probability assessments, and capture the collective judgment or wisdom of informed participants. The data generated by these markets—including price movements, trading volumes, and temporal patterns—can serve as leading indicators for emerging threats and validate insights from traditional intelligence sources.

Integrating prediction market data with established intelligence approaches (i.e., HUMINT, SIGINT, OSINT, GEOINT, and MASINT) creates a more robust framework for analysis. This synthesis allows intelligence analysts to develop more comprehensive threat assessments by combining quantitative, probability-based insights from prediction markets with qualitative intelligence gathered through traditional channels. The dynamic nature of these markets, which react instantly to new information, complements the often slower-moving traditional intelligence gathering processes.

Future developments could significantly enhance the utility of prediction markets for national security. Advances in artificial intelligence and machine learning could enable more sophisticated analysis of prediction market data, identifying complex patterns and correlations that human analysts overlook. Artificial intelligence systems could monitor hundreds of related contracts simultaneously, flagging anomalous trading patterns that might indicate emerging threats before they become apparent through other channels.[13]

As prediction markets mature, specialized contracts focused on national security concerns could provide more granular and relevant data. These markets could be designed to capture insights into specific regions, types of threats, or categories of security concerns, while implementing appropriate safeguards against manipulation and adversarial exploitation. The integration of blockchain technology could also enhance the transparency and reliability of prediction market data while maintaining necessary security protocols. Smart contracts could automate the verification of events and outcomes. This would reduce the potential for manipulation while increasing data reliability.

The future might also see the emergence of hybrid systems that combine prediction markets with other crowdsourced data, creating more comprehensive early warning systems for national security threats. These systems could potentially leverage both public markets and specialized, secure platforms accessible only to intelligence professionals.

The potential benefits of incorporating prediction market data into national security analysis are compelling. As these markets continue to evolve, they are likely to become increasingly valuable to the intelligence community, allowing it to more fully anticipate emerging national threats. The future of national security intelligence might well depend on our ability to effectively harness these new sources of collective intelligence, combining them with traditional methods to create more accurate, timely, and actionable threat assessments.

Endnotes

1. Adam Borison and Gregory Hamm, "Prediction Markets: A New Tool for Strategic Decision Making," *California Management Review* 52, no. 4 (2010): 125-141, https://doi.org/10.1525/cmr.2010.52.4.125.

2. For further information on these platforms, see "What is Polymarket?" User Guide-Get Started, Polymarket, https://learn.polymarket.com/docs/guides/get-started/what-is-polymarket/; and "About Kalshi," Kalshi, 2025, https://kalshi.com/about.

3. Alasdair Brown, J. James Reade, and Leighton Vaughan Williams, "When are Prediction Market Prices Most Informative?" *International Journal of Forecasting* 35, no. 1 (2019): 420-428, http://doi.org/10.1016/j.ijforecast.2018.05.005.

4. James Surowiecki, *The Wisdom of Crowds: Why the Many Are Smarter than the Few and How Collective Wisdom Shapes Business, Economies, Societies, and Nations* (Doubleday Publishers, 2004).

5. For further information on the price discovery process, see Vernon L. Smith, Gerry L. Suchanek, and Arlington W. Williams, "Bubbles, Crashes, and Endogenous Expectations in Experimental Spot Asset Markets," *Econometrica* 56, no. 5 (1988): 1119-1151, https://doi.org/10.2307/1911361.

6. Benjamin Lester, Andrew Postlewaite, and Randall Wright, "Information and Liquidity," Supplement, *Journal of Money, Credit and Banking* 43, no. 7 (2011): 355-377, https://doi.org/10.1111/j.1538-4616.2011.00440.x.

7. Eugene F. Fama, "Efficient Capital Markets: A Review of Theory and Empirical Work," *The Journal of Finance* 25, no. 2 (1970): 383-41, https://doi.org/10.2307/2325486.

8. The range of subjects available in event contracts is extensive. Polymarket, for instance, offers contracts in sports, politics, business, economics, geopolitics, pop culture, crypto, etc. Although not all contracts are immediately relevant as intelligence sources, their price behavior can provide context or further confirmation of an analyst's assessment.

9. This raises the intriguing possibility of analysts fostering the creation of a new contract for a specific geo-political event to collect data anonymously from interested or informed individuals.

10. Ho Cheung Brian Lee, Jan Stallaert, and Ming Fan, "Anomalies in Probability Estimates for Event Forecasting on Prediction Markets," *Production and Operations Management* 29, no. 9 (2020): 2077-2095, https://doi.org/10.1111/poms.13175.

11. Mayur Wankhade, Annavarapu Chandra Sekhara Rao, and Chaitanya Kulkarni, "A Survey on Sentiment Analysis Methods, Applications, and Challenges," *Artificial Intelligence Review* 55 (2022): 5731–5780, https://doi.org/10.1007/s10462-022-10144-1.

12. Borison and Hamm, "Prediction Markets."

13. Ryan H. Murphy, "Prediction Markets as Meta-*Episteme*: Artificial Intelligence, Forecasting Tournaments, Prediction Markets, and Economic Growth," *The American Journal of Economics and Sociology* 83, no. 2 (2023): 383-392, https://doi.org/10.1111/ajes.12546.

CDR Stephen Ferris (retired) is a professor of finance at the University of North Texas. He holds a bachelor of arts from Duquesne University, a master of business administration and a doctorate from the University of Pittsburgh, and a master's degree in strategic studies from the U.S. Army War College. He also holds diplomas from the U.S. Army's Command and General Staff College and the U.S. Navy's College of Naval Command and Staff. His last active-duty assignment was with the J-4 on the Joint Staff.

CPT Raymond Ferris is the counterintelligence operations officer for 2nd Military Intelligence (MI) Battalion, 66th MI Brigade (Theater). He previously served as assistant S-2 for the 1st Armored Division, Division Artillery and as the company executive officer for Bravo Company, 532nd MI Battalion, 501st MI Brigade (Theater).

REDESIGNING MILITARY INTELLIGENCE SOLDIER ALIGNMENT

BY SERGEANT MAJOR RICHARD WILLIAMS AND SERGEANT MAJOR THOMAS GOLLIER

Introduction

Within the Army Military Intelligence (MI) Corps, Soldier professional development requires a specialized approach that creates regionally intelligent subject matter experts with the necessary skills to advise combat commanders. MI Soldiers must be capable of understanding the enemy, civilian leadership, and external influences of a region through a relevant cultural lens. Soldiers would develop this type of expertise through years of experience, providing accurate and relevant intelligence to their commanders. Unfortunately, the current career models for MI Soldiers focus on an assignment progression tailored to leadership skills development. Soldiers rotate through the major commands—U.S. Army Forces Command (FORSCOM), U.S. Army Intelligence and Security Command (INSCOM), U.S. Special Operations Command (SOCOM), and U.S. Army Training and Doctrine Command (TRADOC)—and MI assignments without ever focusing on building or maintaining regional and cultural expertise. Through their assignment rotations, MI Soldiers shift their focus from one adversary and region to another, sometimes with vastly different cultures. The traditional approach of solely focusing on rotating Soldiers through assignments to create a diversity of experiences produces a gap in their understanding of language, culture, and adversarial norms.

Regional Alignment and Talent Management

Commanders expect MI Soldiers to understand both the adversary and the complex operational environment in a way that requires a deep cultural understanding. While analytical frameworks such as PMESII-PT,[1] which focus on political, military, economic, social, information, infrastructure, physical environment, and time and ASCOPE,[2] which focuses on areas, structures, capabilities, organizations, people, and events effectively describe an operational environment, they inherently lack the depth required to understand the nuanced cultural factors that significantly influence behavior and meaning. This limitation hinders accurate interpretation and assessment of collected information. Culture is a complex variable that instructors cannot teach through annual language training, much less during pre-deployment preparation. Training Soldiers to understand a foreign culture would take the full course of an Army career. To create true subject matter experts and build cultural expertise, the Army must focus on aligning MI Soldiers to a threat area or region for the entire span of their careers.

Permanently aligning MI Soldiers' assignments to a geographic area of responsibility would improve their understanding of the target theater's relevant actors, cultural norms, and external influences. With MI Soldier assignments intentionally

aligned to an area of responsibility, Soldiers would inherently become more aware of what is normal and abnormal through continuous exposure. Through the management of MI personnel within specified geographic areas of responsibility, the Army could produce higher-quality intelligence to drive operations and build relationships with external organizations. To be effective, a model of reinforced expertise must align Soldiers' assignments across the Army from the strategic intelligence level down to the tactical military intelligence companies and detachments. Soldiers would need to study their regions through tactical, operational, and strategic lenses to understand the geography, doctrine, equipment, and capabilities common across potentially friendly and adversarial nations.

While the current career model favors a breadth of experience, a redesigned career path could focus on building depth of expertise over time. If Soldiers left their advanced individual training with an assigned area of responsibility and held to assignments focused on that mission, the Army would develop vastly superior intelligence support. Building additional skill identifiers to track MI strength across regions and reviewing the alignment of FORSCOM, INSCOM, and TRADOC would be critical first steps to implement this model. Following that, the Human Resources Command would need to track MI strength and utilize proper talent management, rather than simply managing billets, for Soldiers' assignments. The Army would also have to review theater alignments against the language and cultural training capabilities across installations to ensure that capabilities match needs. Finally, training requirements and exercises for MI Soldiers should emphasize scenarios that reinforce intelligence production through a regional and cultural understanding.

Over the last decade, the Army has discussed ideas and even considered associating language-dependent career field Soldiers with geographically aligned units. At the same time, the Army placed a renewed emphasis on language proficiency, shifting away from the Global War on Terrorism's focus on intelligence collection and production through reach-back or contracted support. The discussions about regionally aligning linguists and organizations left non-linguist MI Soldiers behind. In an Army that aims to build MI expertise through cultural knowledge, MI Soldiers must align with a specific geographic area of responsibility and maintain a singular focus on a defined problem set. In the long term, the Army would reap substantial benefits from a model that reinforces the building of knowledge throughout Soldiers' careers.

Conclusion

The initial investment of time and resources to build this type of expertise is substantial. Still, this model would generate a massive return on that investment, as Soldiers do not require complete retraining to understand their new mission when they permanently change stations. Soldiers could also continue to rotate through successive leadership roles and diverse assignments as they experience FORSCOM, INSCOM, TRADOC, and SOCOM assignments. However, as Soldiers rotate through these organizations, their noncommissioned officers would be true experts in both the missions and the adversaries they encounter, focused on strengthening the profession of arms. Additionally, over time, these leaders would build relationships with other intelligence agencies, maintaining connections through years and decades rather than months. Commanders could rely on the intelligence derived from culturally knowledgeable Soldiers who fully embrace the complexities of the operational environment.

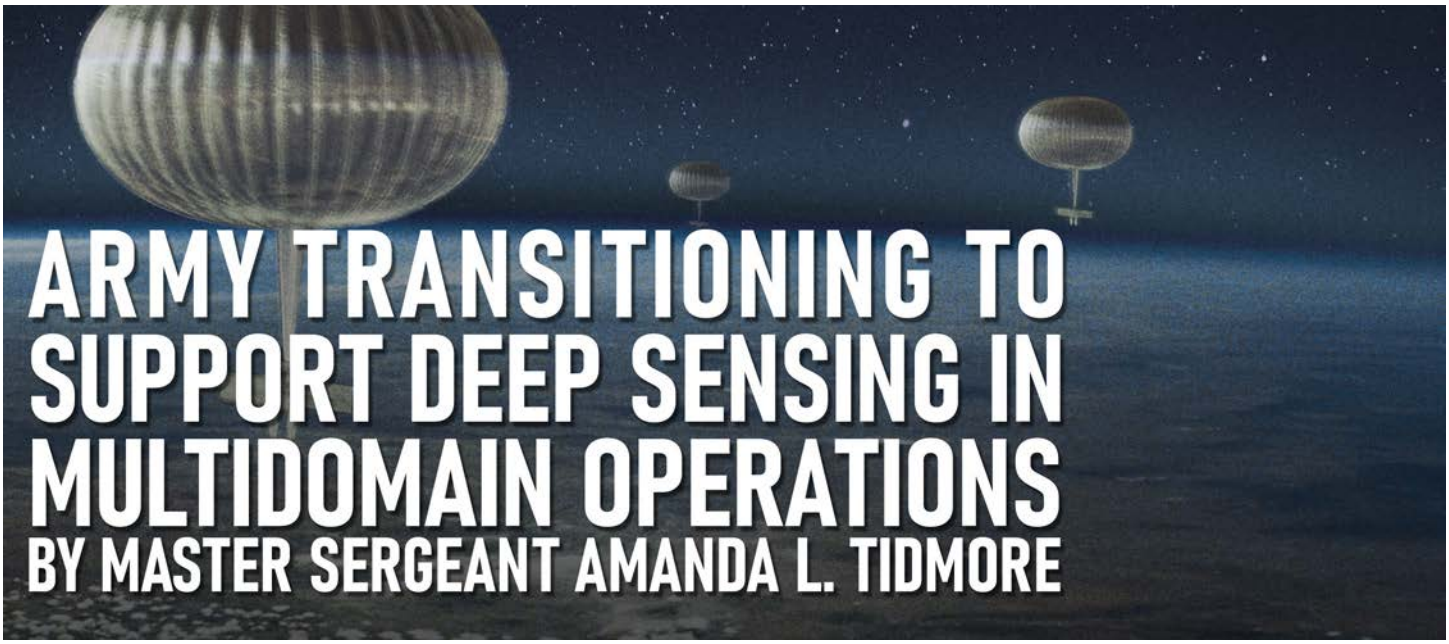
Endnotes

1. Department of the Army, Field Manual 5-0, *Planning and Orders Production* (Government Publishing Office [GPO], 2024), 5.

2. Department of the Army, Army Doctrine Publication 6-0, *Mission Command: Command and Control of Army Forces* (GPO, 2019), 3-6.

SGM Richard Williams is the G-2 sergeant major for the 1st Armored Division. He previously served at all levels of leadership, from team leader to sergeant major, and also held the position of 35F, intelligence analyst, professional development noncommissioned officer/talent manager for the U.S. Army Human Resources Command. SGM Williams has deployed numerous times to Iraq and Afghanistan, as well as for operational deployments throughout the Middle East and Europe. He holds multiple degrees, including a master of science in strategic leadership from the University of Charleston.

SGM Thomas Gollier is the G-33 operations director for the U.S. Army Intelligence and Security Command. He previously served as an action officer in the Office of the Sergeant Major of the Army, a military intelligence company first sergeant, senior enlisted leader of a technical control and analysis element, a platoon sergeant, and an infantry team leader. He deployed multiple times to Iraq and Afghanistan. He holds several degrees, including a bachelor's in leadership and workforce development from the U.S. Army Command and General Staff College.



ARMY TRANSITIONING TO SUPPORT DEEP SENSING IN MULTIDOMAIN OPERATIONS

BY MASTER SERGEANT AMANDA L. TIDMORE

Introduction

The U.S. Army strategic contexts of competition, crisis, and armed conflict correspond to and support the joint competition continuum. Currently, the People's Republic of China and Russia are in a constant state of competition with the United States, seeking to gain superiority through significant military, economic, and political advantages. The operational environment continues to evolve in response to these adversaries' increasing capabilities, and the Army must prepare to fight in contested environments. Therefore, the Army established multidomain operations as its operational concept. Multidomain operations encompass a combined arms approach to operations in the land, maritime, air, space, and cyberspace domains, while maneuvering across the physical, information, and human dimensions. The intelligence warfighting function is key to providing the Army with relative advantages and windows of opportunity to overcome adversary defenses. The extended operational environment poses significant challenges for the intelligence warfighting function. To meet those challenges, the Army must leverage big data and technology solutions to develop new sensing capabilities that can penetrate, survive, and collect information.

The Operational Environment

The operational environment encompasses the human, physical, and information dimensions within each domain. Collectively, the combination of domains and dimensions are analyzed and described through the operational variables: political, military, economic, social, information, infrastructure, physical, and time (PMESII-PT), applied within the context of the mission variables: mission, enemy, terrain and weather, troops and available support, time available, and civil considerations (METT-TC).[1] As the Army shifts strategic priorities from counterinsurgency operations to large-scale combat operations, the operational environment will be increasingly difficult to navigate for the intelligence warfighting function. Peer threats with capabilities across all domains will pose a significant challenge. "The PRC [People's Republic of China] has expanded and modernized nearly every aspect of the PLA [People's Liberation Army], with a focus on offsetting U.S. military advantages."[2] Knowledge of the future operational environment will be imperative to reducing operational uncertainty for fighting and winning in complex environments, and the intelligence warfighting function will play a vital role in supporting operations across all domains. Army intelligence professionals must understand each domain, leverage intelligence architecture, collaborate with other military services, and provide intelligence support to all echelons to be effective.

"In addition to expanding its conventional forces, the PLA is rapidly advancing and integrating its space, counterspace, cyber, electronic, and informational warfare capabilities to support its holistic approach to joint warfare."[3] Intelligence sets the conditions for theater operations; gaining situational understanding of the operational environment will drive success against future threats in multidomain operations and a potentially contested operational environment.

The Tactical Problem

Antiaccess (A2) and area denial (AD) are approaches adversaries use to prevent friendly forces from entering an operational area and then hinder their ability to maneuver within that area.[4] A2 and AD systems combine long-range capabilities, such as antiship, antiair, and antiballistic weapons, intended to impede movement into the operational environment, with short-range capabilities, such as electromagnetic warfare and integrated air defense systems, to decrease maneuverability once inside. Army intelligence faces a series of challenges in adapting to evolving A2 and AD environments and operating successfully in multidomain operations.

Commanders require accurate, relevant, and predictive intelligence to understand the threat across the strategic contexts of competition, crisis, and armed conflict. A2 and AD will pose unique problems for Army intelligence during armed conflict. Future Army intelligence collection systems will need to be survivable aerial platforms that can overcome A2 and AD systems and achieve stand-off through high altitudes. Today's Army intelligence, surveillance, and reconnaissance collection is susceptible to contested airspace and has limited collection ranges. Currently, corps and division intelligence lack sufficient organic assets capable of penetrating peer threat stand-off defenses to support targeting, situational understanding, and decision making. To be successful, the Army must be capable of penetrating the A2 and AD systems in regional areas that have spent the last decade building advanced weapon systems. In future armed conflict, peer adversary defenders will have an advantage because they will be defending specific A2 and AD zones that the United States will need to penetrate to be effective in follow-on operations.

The Tactical Solution

Army 2030 initiatives include significant changes that will enable divisions to be more effective by task organizing for purpose, modernizing key capabilities, and providing future capacities at echelon to defeat peer adversaries.[5] Multidomain deep sensing, along with other information collection, will be instrumental in successfully maneuvering to defeat adversary A2 and AD capabilities. The ability to penetrate, survive, and collect information during multidomain operations will provide early warning, current intelligence, and target intelligence to inform and drive operations. Modernization efforts for collection platforms are necessary to ensure an intelligence advantage in contested environments.

The Multi-Domain Sensing System (MDSS) will provide the Army with extended endurance over wide areas, enabling it to counter A2 and AD systems. Its sensors will collect, process, correlate, and analyze using artificial intelligence (AI) and machine learning (ML) technologies. "MDSS will use quantum communication and information technology, AI, and other autonomous solutions to rapidly ingest, sort, process and archive data at speeds and measures of performance far beyond human capacity."[6] Deep sensing capabilities will provide a military advantage on the battlefield because future collection platforms will be able not only to penetrate A2 and AD systems' defenses, but also to collect at stand-off distances, providing intelligence support to multiple echelons. The Army is currently piloting the MDSS High Accuracy Detection and Exploitation System (HADES). "HADES will address Army requirements for medium to high altitude aerial ISR [intelligence, surveillance, and reconnaissance] capabilities to rapidly gain and maintain situational understanding, freedom of maneuver, information overmatch, and decision advantage in the MDO [multidomain operations]."[7] Deep sensing capabilities will be imperative to enable the Army to generate combat power for deep operations.

The Army is also adopting the Tactical Intelligence Targeting Access Node (TITAN), a system that leverages AI and ML to process sensor data, providing direct support to targeting and battlefield situational awareness during multidomain operations. TITAN will increase the speed and accuracy of intelligence collection, processing, and dissemination. HADES and TITAN both support the Department of Defense's fiscal year 2023 data, analytics, and AI adoption strategy to accelerate decision advantages over near-peer and peer threats. "The Department's investments in data, analytics, and AI will address key operational problems identified in the 2022 NDS [National Defense Strategy], fill validated gaps to enhance the warfighting capabilities of the Joint Force, and strengthen the enterprise foundation required to sustain enduring advantages."[8]

Fighting For Intelligence

The intelligence warfighting function task list is a comprehensive but incomplete listing of the Army intelligence warfighting function's responsibilities, missions, and operations. It includes providing intelligence support to force generation, providing support to situational understanding, conducting information collection, and providing intelligence support to targeting.[9] The intelligence warfighting function faces a significant challenge when attempting to provide effective and flexible intelligence during multidomain operations due to the potential contested environment across all domains. This challenge, referred to as fighting for intelligence, drives actions by the commander and staff "to identify and ultimately open windows of opportunity at the right time and place to leverage one or more capabilities across domains,"[10] leading to exploiting a relative advantage.

Integrating AI and ML technologies is necessary to collect intelligence and provide deep sensing capabilities in A2 and AD environments. Threat A2 and AD capabilities will directly impact the Army's ability to collect intelligence on threats, challenging the ability to fight for intelligence during competition, crisis, and armed conflict. MDSS will provide the Army with a tool to fight for intelligence across echelons and facilitate intelligence support to ground commanders through deep, close, and rear operations. Although multidomain operations will present numerous challenges, the intelligence warfighting function can successfully navigate these challenges if the Army capitalizes on the advantages that AI and ML technologies will bring to intelligence collection platforms.

Endnotes

1. Department of the Army, Field Manual (FM) 5-0, *Planning and Orders Production* (Government Publishing Office [GPO], 2024), 5, https://armypubs.army.mil/epubs/DR_pubs/DR_a/ARN42404-FM_5-0-000-WEB-1.pdf.

2. Department of Defense, *2022 National Defense Strategy of the United States of America* (GPO, 2022), 4, https://media.defense.gov/2022/Oct/27/2003103845/-1/-1/1/2022-NATIONAL-DEFENSE-STRATEGY-NPR-MDR.PDF.

3. Ibid., 4.

4. Department of the Army, FM 3-0, *Operations* (GPO, 2025), 33.

5. John Dolan et. al, "Enabling the Division in 2030: Evolving Division Reconnaissance and Security Capabilities," *Armor* CXXXVV, no. 2 (Spring 2023): 13-17, https://www.benning.army.mil/Armor/eArmor/content/issues/2023/Spring/2Dolan_Pelham_Sickler_Speakes_Frederick23.pdf.

6. Army Futures Command (AFC), AFC Pamphlet 71-20-3, *Army Futures Command Concept for Intelligence 2028* (AFC Futures and Concept Center, 2020), 70, https://api.army.mil/e2/c/downloads/2021/01/05/26b729a6/20200918-afc-pam-71-20-3-intelligence-concept-final.pdf.

7. Daniel Baldwin, "The Future of Army Deep Sensing," News, U.S. Army website, January 19, 2024, https://www.army.mil/article/273077.

8. Department of Defense, *Data, Analytics, and Artificial Intelligence Adoption Strategy: Accelerating Decision Advantage* (GPO, 2023), 5, https://media.defense.gov/2023/Nov/02/2003333300/-1/-1/1/DOD_DATA_ANALYTICS_AI_ADOPTION_STRATEGY.PDF.

9. Department of the Army, FM 2-0, *Intelligence* (GPO, 2023), B-1.

10. Ibid., 1-28.

References

The AIM Initiative: A Strategy for Augmenting Intelligence Using Machines. Office of the Director of National Intelligence, 2019. https://www.dni.gov/files/ODNI/documents/AIM-Strategy.pdf.

Feickert, Andrew. *The Army's AimPoint and Army 2030 Force Structure Initiatives*. Congressional Research Service, 2022. https://crsreports.congress.gov/product/pdf/IF/IF11542.

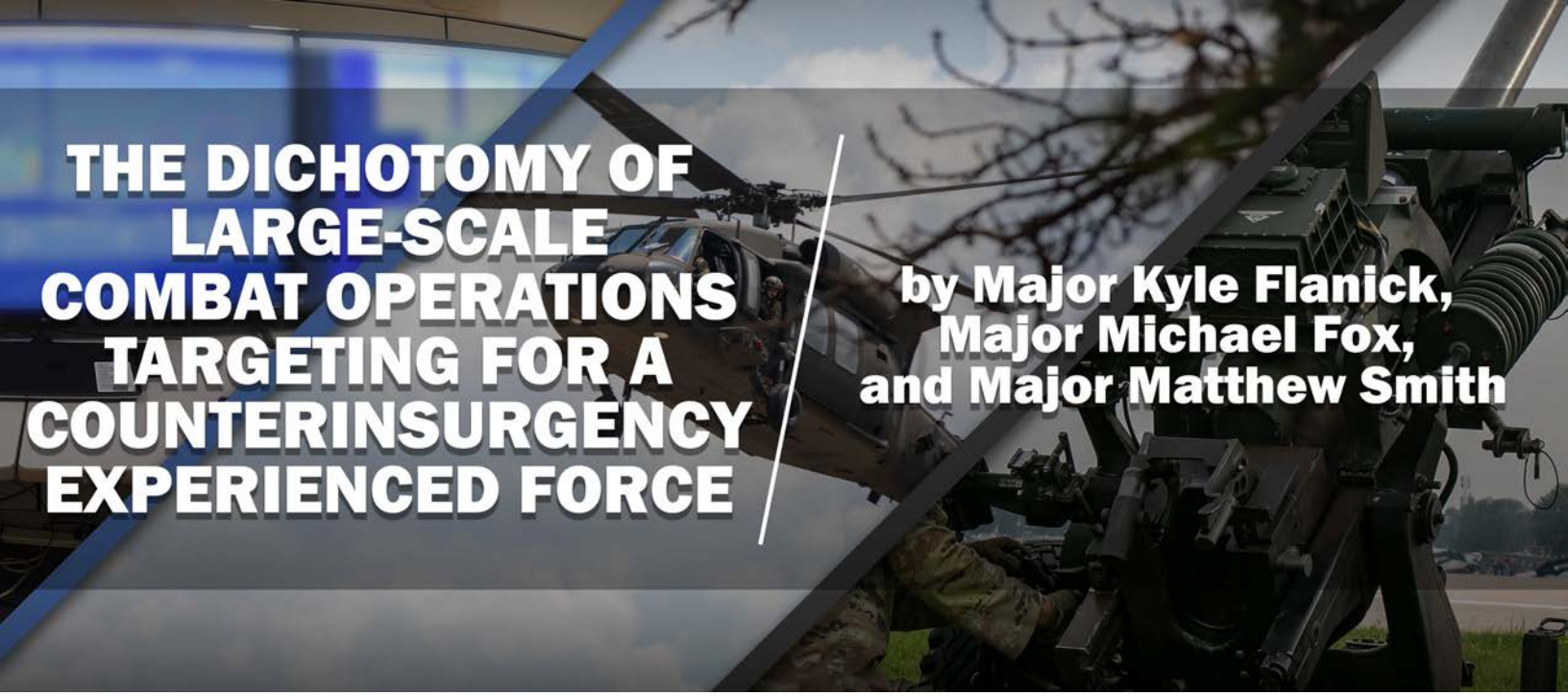
Intelligence Community Assessment: Annual Threat Assessment. Office of the Director of National Intelligence, 2024. https://www.odni.gov/index.php/newsroom/reports-publications/reports-publications-2024/3787-2024-annual-threat-assessment-of-the-u-s-intelligence-community.

Mazarr, Michael J. *Understanding Competition: Great Power Rivalry in a Changing International Order–Concepts and Theories*. Rand Corporation, 2022. https://www.rand.org/pubs/perspectives/PEA1404-1.html.

National Military Strategy 2022. Office of the Chairman of the Joint Chiefs of Staff, 2022. https://www.jcs.mil/Portals/36/NMS%202022%20_%20Signed.pdf.

Sayler, Kelley M. *Artificial Intelligence and National Security*. Congressional Research Service, 2020. https://www.congress.gov/crs-product/R45178.

MSG Amanda Tidmore serves as the 35F, Intelligence Analyst, advanced individual training program of instruction noncommissioned officer in charge, directly certifying incoming Army instructors for the Intelligence Analyst Training Committee at Fort Huachuca, AZ. MSG Tidmore's military intelligence experience is broad, encompassing both tactical and operational levels. Her experience also includes working in a joint environment, coordinating with national intelligence organizations, and collaborating with international partners. MSG Tidmore holds an associate of applied science in intelligence operations from Cochise College and a bachelor of arts in intelligence studies with a concentration in intelligence analysis from American Military University.



THE DICHOTOMY OF LARGE-SCALE COMBAT OPERATIONS TARGETING FOR A COUNTERINSURGENCY EXPERIENCED FORCE

by Major Kyle Flanick, Major Michael Fox, and Major Matthew Smith

Keeping pace with the speed of war means changing the way we approach challenges, build strategy, make decisions and develop leaders.

—Marine Corps General Joseph Dunford (Retired)

Introduction

The Army's training focus has shifted undeniably from counterinsurgency (COIN) operations to competition with pacing threats and readiness for large-scale combat operations. Most leaders of Army forces have significant COIN experience, which is invaluable; however, we must understand what the shift to large-scale combat operations means—specifically, for targeting. The typical COIN targeting practices in the U.S. Central Command (CENTCOM) area of operations (AOR) over the past decade, such as strike decisions held at the general officer level, created a requirement for a heightened degree of positive target identification. Because of this low-risk standard, there is likely to be little tolerance for collateral damage in large-scale combat operations. In general, the large-scale combat targeting mindset is distinguishable from COIN targeting by its increased speed of decision making and limited availability of information and intelligence, resulting in a greater assumption of risk. This article will refresh leaders on the targeting process and encourage them to implement organizational training on targeting processes for large-scale combat operations.

Perspectives on the Targeting Process

Joint Publication 3-0, *Joint Campaigns and Operations*, defines targeting as "the process of selecting and prioritizing targets and matching the appropriate response to them, considering operational requirements and capabilities."[1] Throughout COIN operations and the subsequent shift to readiness for large-scale combat operations, the Army's field artillery has advocated the Army targeting methodology of *decide*, *detect*, *deliver*, and *assess* to prioritize and engage enemy targets effectively.[2] This targeting process ensures that commanders fully integrate and synchronize fires and effects to set conditions, meet key objective end states, and buy down risk for the commander in both COIN and large-scale combat scenarios.

In the decide phase, commanders and their staff plan and synchronize efforts to identify, select, and prioritize targets necessary to meet the commander's intent. The detect phase addresses information requirements through a full spectrum of collection activities that identify enemy activity, assets, and locations. The deliver phase occurs during the execution of operations. It involves engaging targets that meet the criteria of the commander's high-payoff target list, attack guidance matrix, and target selection standards. The final phase, assess, is continuous throughout the operations process and gauges not only the effectiveness of the delivery system but also the collection methods used, which feed back into the commander's decision-making process.

From an intelligence perspective, the joint targeting methodology known as *find*, *fix*, *finish*, *exploit*, *analyze*, and *disseminate* (F3EAD) remains doctrinally sound for both the COIN and large-scale combat operating environments.[3] F3EAD is very well suited for targeting operations against high-value targets; however, it is equally effective against other types of combat operations targeting, including those seeking nonlethal effects. While doctrine views F3EAD as a hasty decision-making process, many units also use F3EAD during deliberate planning.

The find step establishes a starting point for intelligence collection. The fix step occurs when sufficient intelligence collection is accumulated on a target to execute a mission. These first two steps lay the foundation for successful operations against the adversary. Some examples of the finish step include lethal strikes via terminal guidance, launching a raid force, or using surrogates to close with and destroy

an adversary's forces, weapons, or equipment. The exploit step, as the main effort of F3EAD, is the most critical single step in the process, as it leads to finding, fixing, and finishing the next target and perpetuating the cycle. In the analyze step, intelligence analysts transform the collected exploitable material into intelligence reports, driving future operations. The last step of the F3EAD process is disseminate. Key to the success of the F3EAD process is creating a more comprehensive dissemination network than what the U.S. intelligence community traditionally practices.

When conducting a law of armed conflict (LOAC) targeting analysis, commanders, with the support of their staff, analyze military necessity, distinction, proportionality, and humanity. It is important to note that while the LOAC may permit certain actions, specific rules of engagement (ROE) implemented by a higher command are likely to restrict actions the LOAC permits. The decisions associated with the LOAC analysis rely heavily upon the information and intelligence provided to the staff. The quality of this information naturally feeds the accuracy and effectiveness of commanders' decisions. Accurate, timely, and reliable information used during the targeting analysis should result in targeting actions that comply with the LOAC principles and pertinent laws and regulations while simultaneously offering an acceptable level of risk to the commander.

The Counterinsurgency Experience

For the past two decades, most targeting analysis was conducted in an established operational environment in the CENTCOM AOR. Analysts within these areas of operation developed operating pictures and associated intelligence products that rotational units continually refined. Furthermore, the United States and its partner forces enjoyed significant asset superiority within these areas of operation. Consistent air superiority aided weapons delivery, intelligence gathering, redundant communications, and signal assets without consequence for the collateral digital footprint. Most operational leaders within the Army today are veterans of these conflicts and have considerable experience from operating in this environment. This is invaluable experience; however, large-scale combat operations will rarely involve countless targeting scenarios comprising various unmanned aircraft systems and intelligence, surveillance, and reconnaissance (ISR) assets that identify, track, and remain on station to evaluate effects like those seen in the CENTCOM AOR. What then might targeting decision makers expect during large-scale combat operations? Before we discuss this shift, it is important to understand the lessons learned over the past two decades of conducting COIN operations.

Field Artillery Perspective. In developed operational environments and COIN environments, fire support is characterized by precision munitions, real-time situational awareness, and an emphasis on limited collateral damage. Air superiority within a developed operational environment allows friendly forces to enjoy freedom of maneuver, aerial platforms to deliver lethal and nonlethal effects, and capabilities that can serve as additional collection assets.

Precision guided munitions were in use as early as World War II but became common during the Vietnam conflict and the First Gulf War. COIN operations dominated the first two decades of the 21st century when precision munitions became a staple in the fire support arsenal. Precision munitions, such as the AGM-114 Hellfire Missile, are delivered by aerial assets. Ground systems, like the Guided Multiple Launch Rocket System, can fire several types of precision munitions over extended distances. Other precision munitions, such as the Tomahawk Cruise Missile, are launched from naval vessels. The qualifier of a precision-guided munition is its reliance on a guidance system using a global positioning system (GPS), laser, or internal inertial sensors to increase the weapon's accuracy. Precision-guided munitions were used heavily

An AGM-114B Hellfire missile being fired off the rails of a U.S. Navy SH-60 Seahawk helicopter toward a laser designated surface target during training off the coast of San Clemente Island, CA, on August 25, 1999. (DoD photo by Petty Officer 1st Class Spike Call, U.S. Navy.)

in COIN operations to increase lethality on specific targets while minimizing effects and potential collateral damage in the targets' vicinity. Precision munitions allow commanders to assume more risk when employing lethal effects in densely populated areas or near friendly forces.

In COIN operations, modern technology, such as airborne ISR and GPS tracking, allowed commanders to achieve near-complete situational awareness of both friendly and enemy forces. The benefit of air superiority permitted a battle staff to monitor, or "soak," a target for an extended period before striking or launching a raid force. Every Soldier, asset, or platform, from the ISR system orbiting at 20,000 feet to the team leader on the ground carrying an end-user device, served as a sensor, providing data to a joint operations center. This information was continually updated to enhance the battle staff's understanding of the threat and improve the commander's decision-making process. Commanders became accustomed to this elevated level of situational awareness and would become frustrated or risk-averse when the ability to track friendly or enemy forces was diminished. Battle staff became accustomed to the plethora of tactical ISR feeds and used what they saw on screens to confirm what units on the ground reported. In this COIN environment enhanced situational awareness was normal and therefore easily exploitable, but it cannot be expected in other environments.

COIN operations were also characterized by an emphasis on reducing collateral damage to both civilian life and infrastructure. Collateral damage estimates are used to determine the anticipated effects of weapons on a target or structure and the potential collateral effects of that weapon. The desire to minimize collateral damage has led to the development of low-collateral munitions and unique tools for estimating potential collateral damage. Often in the CENTCOM AOR, the "zero collateral damage" requirement limited engagement areas and time available to target. Commanders were responsible for minimizing civilian harm by understanding the risks associated with targeting specific areas.

Overall, fire support in developed operational environments requires a clear understanding of the environment and a reliance on technology to deliver precise effects on the enemy while minimizing the impact on non-combatants and civil structures.

Intelligence Perspective. In developed operational environments, intelligence operations require a blend of advanced technology, comprehensive databases, and highly trained personnel. These operations typically follow a systematic process to gather, analyze, and disseminate actionable intelligence, thereby supporting informed military decision making. Execution of intelligence operations in developed operational environments occurs as follows:

Collection. Intelligence collection relies heavily on sophisticated technology, including satellites, drones, and surveillance aircraft. These assets provide a wide range of data, including imagery, signals, and electronic communications, enabling operators to monitor enemy activities, assess threats, and identify vulnerabilities. Additionally, human intelligence sources play a crucial role in gathering information from within threat organizations and local populations. This method of collection relies heavily on all-domain superiority.

Analysis. Intelligence, once collected, is analyzed by skilled personnel trained in various disciplines and capabilities, including imagery analysis, signals intelligence, cyberspace intelligence, and open-source intelligence. Analysts assess the information's relevance, reliability, and significance to generate accurate assessments of enemy capabilities, intentions, and vulnerabilities. Advanced analytical tools and software facilitate the processing of large volumes of data, enabling the identification of patterns and trends that may indicate emerging threats or opportunities.

Integration. Analyzed intelligence is integrated into comprehensive assessments and briefings for military commanders and policymakers. This process involves synthesizing information from multiple sources and disciplines to provide a clear understanding of the operational environment, threat behavior, and potential courses of action. Intelligence fusion centers play a crucial role in integrating intelligence from various sources and agencies to provide a comprehensive picture for decision makers.

Dissemination. Once analyzed and integrated, intelligence is disseminated using secure communication channels to relevant stakeholders, including commanders, operational units, intelligence agencies, allied partners, and government agencies involved in national security. The timely and accurate dissemination of intelligence ensures that decision makers have the information they need to plan and execute military operations effectively.

Feedback. Intelligence operations in developed operational environments emphasize the use of continuous feedback loops to evaluate the effectiveness of collection and analysis efforts. Lessons learned from previous operations are incorporated into training, doctrine, and technological advancements to enhance future intelligence capabilities. This iterative process ensures that intelligence operations remain responsive and adaptive to evolving threats and challenges.

Overall, intelligence operations in developed operational environments utilize advanced technology, analytical expertise, and institutional collaboration to provide decision makers with timely, accurate, and actionable intelligence for achieving military objectives.

The High Mobility Artillery Rocket System fires the Army's Guided Multiple Launch Rocket System (U.S. Army photo)

Legal Perspective. During COIN operations, the legal role in the targeting process must remain consistent and transparent. Legal experts determine whether commanders and staff adhere to the principles of LOAC (and any additional theater policies and guidance). However, this process depends heavily on the availability of information and intelligence concerning the targets provided to the staff. In a developed operational environment where units leverage assets and technological superiority (as was typical with CENTCOM COIN operations), timely and accurate reports greatly assist in the LOAC determination. Timely, accurate, and actionable intelligence makes deciding target distinction, proportionality, and humanity implications significantly more feasible. It allows decision makers to observe targets, make assessments, and gauge effects in real time. Ultimately, risk lies with the commander making the targeting decisions; however, the availability of assets in a developed operational environment, where allied forces enjoy superiority in multiple domains, typically reduces risk.

Adapting to Large-Scale Combat Operations

As we shift focus to competition with pacing threats and prepare our forces for potential large-scale combat operations, our targeting analysis mindset must also shift. Unlike the COIN operations in Iraq and Afghanistan, large-scale combat operations will require conducting the targeting process in a rapidly evolving operational environment where we lack asset superiority and redundancy and must sometimes make decisions informed by inadequate information. Targeting analysis will be conducted more quickly, with less available information and intelligence, causing a greater assumption of risk.

Despite the faster pace and the limited availability of targeting information associated with large-scale combat operations, leaders can promote successful targeting by recognizing the difference between operation-specific ROE and LOAC, simplifying triggers, and understanding the value of targets.[4]

Rules of Engagement Versus Law of Armed Conflict. As we teach and train, we must clearly distinguish between operation-specific ROE and LOAC. The differences can be subtle and difficult to discern. During the Iraq and Afghanistan COIN operations, Soldiers on separate deployments often operated under similar, but different, operation-specific ROE. However, it is vital to understand that, in the absence of additional theater- or mission-specific ROE, the LOAC sets a relatively low bar for decision makers. Future large-scale combat operations will undoubtedly include mission-specific ROE, wherein operational guidance regarding military necessity, distinction, proportionality, and humanity analysis remains distinct from LOAC. Put simply, the LOAC is the law that sets boundaries for permitted and prohibited actions; ROE are conflict-specific policies that the President, Secretary of Defense, or higher command imposes to restrict further the actions of subordinate forces that the law otherwise permits. The operations cell (G-3/S-3) controls and briefs mission-specific ROE, while the judge advocates from the servicing legal office advise commanders on the application of the LOAC.

Simplify Triggers. In a faster-paced environment with less available information and intelligence, we must be willing to simplify triggers in the targeting process. For example, during intelligence preparation of the operational environment, an organization may determine that the movement of an enemy battalion tactical group will be signaled by their reconnaissance element, composed of multiple BRDM-2 reconnaissance patrol vehicles, moving into a specific named area of interest (NAI 1). Ideally, if there is an interest in targeting the reconnaissance element, one trigger could be a friendly

observation asset identifying the presence of BRDM-2s in NAI 1. However, if the situation offers limited information and intelligence, can the targeting trigger be simply *movement* observed in NAI 1? This second, less specific trigger carries a greater risk. In a large-scale combat operations environment, these are concepts that leaders must understand as viable circumstance-driven options.

Understanding a Target's Value. During large-scale combat operations, the value of targets must be understood in real time. Several tools are available to assist organizations with this task, including the high-payoff target list and the attack guidance matrix. Organizations must recognize that in large-scale combat operations, factors beyond legal considerations may restrict their ability to engage a target—for example, controlled supply rates and the risk of the enemy developing countermeasures for their targeting assets.[5] These concepts are generally understood but must be emphasized when planning and developing attack guidance matrices and during targeting decisions.

The Field Artillery Perspective. In a developing operational environment, the approach to fire support differs from the approach used in the COIN environment. Large-scale combat operations present challenges that a COIN-experienced force must adapt to meet. Fortunately, the tools to succeed are already available.

In a large-scale combat environment, will there be a single source targeting solution? The speed of warfare, combined with the massing of forces, requires the layering and synchronization of multidomain effects, not only to defeat enemy protection but also to present overwhelming dilemmas for the enemy commander. Effective targeting will include layering lethal effects and integrating electromagnetic warfare, cyberspace, and space-based assets and capabilities. This requires battle staff to understand and integrate joint capabilities that were not used extensively in COIN operations. Additionally, successful multidomain integration requires close coordination and interoperability with the joint force and foreign partners. Detailed planning, shared intelligence, and synchronized execution (maximizing effects to achieve overmatch while preserving capability) are key to success.

In an underdeveloped operational environment, however, mission command may be challenging as commanders will not enjoy the same level of situational awareness that was normal in the COIN environment. The lack of air superiority and the enemy's ability to detect signal emissions may limit a commander's ability to receive continuous communication and real-time updates. Coordination and synchronization become progressively more challenging when communication is limited, GPS is denied, and electromagnetic and cyberspace warfare proliferate over vast geographical areas. Protection against collection and cyberspace access, as well as a disciplined communications plan, are essential for survivability. Commanders must become comfortable with providing guidance and then allowing subordinate units to execute their missions with limited oversight, as they will be forced to assume more risk with less situational awareness of their subordinate elements. Operators of delivery systems, such as cannon and rocket artillery, as well as air assets, must understand their targets and utilize speed and flexibility to achieve survivability and mass fires on the enemy.

Units must adjust to the complex nature of large-scale combat operations. Understanding capabilities, integrating available assets, and robust planning will help commanders manage risk effectively. Additionally, utilizing resources available throughout the joint force will empower initiative and creativity in challenging environments.

The Intelligence Perspective. In underdeveloped operational environments lacking all-domain superiority and with limited communications infrastructure, intelligence operations face unique challenges from an often sparse population, rugged terrain, cultural complexities, and limited infrastructure. Nevertheless, intelligence operations can be conducted effectively in underdeveloped operational environments using traditional methods adapted to local conditions and by leveraging available resources.

Human intelligence becomes a primary method of intelligence collection because of a lack of advanced technological resources. Collectors build relationships with local communities, tribal leaders, and informants to gather information on enemy activities, regional dynamics, and potential threats. This often involves conducting covert meetings, cultivating sources, and developing trust within the community.

Intelligence operations in underdeveloped operational environments prioritize cultural understanding and sensitivity. Collectors must navigate complex social structures, tribal affiliations, and ethnic tensions to gather accurate information and avoid misunderstandings that could escalate tensions or lead to conflicts. Cultural experts and linguists often embed with intelligence teams to facilitate communication and interpretation of intelligence. This requires flexibility and adaptation to local conditions. Collectors frequently employ unconventional methods, such as blending in with the local population, utilizing indigenous assets, or employing indigenous tracking and survival skills. This adaptive approach allows intelligence teams to gather information effectively while minimizing their footprint and avoiding detection by adversaries.

Given the rugged terrain and limited infrastructure, small-unit reconnaissance becomes essential for gathering tactical intelligence. Specialized reconnaissance teams conduct patrols, set up observation posts, and execute reconnaissance missions to gather firsthand information on enemy movements, terrain features, and potential threats.

In situations where advanced technology is unavailable, intelligence operations must rely on basic communication equipment, such as radios or encrypted messaging systems to maintain effective communication. Satellite imagery and drones may still be used where available, but their use is often limited by terrain and logistical constraints.

Intelligence operations in underdeveloped operational environments often involve collaboration with local security forces, militias, or rebel groups. By partnering with indigenous forces, intelligence operators gain access to local knowledge, resources, and networks, enhancing their understanding of the operational environment and increasing their effectiveness in gathering intelligence.

The Legal Perspective. During large-scale combat operations, commanders at all levels will likely assume a higher level of risk in their decision making, especially when targeting. The *Department of Defense Law of War Manual* notes that decision makers must view the battlespace through the "fog of war," which renders information both limited and unreliable. "The uncertainty of information in war results from the chaotic nature of combat and from the opposing sides' efforts to deceive one another, which generally is not prohibited by the law of war."[6] Because the targeting process depends on the information and intelligence available to the staff, an underdeveloped operational environment lacking asset superiority and established technology will create challenges for obtaining intelligence reports used in the targeting process. The quantity, fidelity, and timeliness of these reports directly affect the LOAC analysis and determination. Nevertheless, to conform to the law of war, commanders' decisions must be guided by certain principles.

Military Necessity. This principle recognizes the commander's need to defeat the enemy quickly and efficiently, justifying all measures taken toward that end, as long as the actions do not violate the laws of war.[7] Effective large-scale combat operations require rapid decision making; however, there is considerable risk to decision making during the targeting process when speed is combined with a limited availability of information and intelligence. Commanders must understand that they will only be judged on the information they had at the time of their actions, and whether their decisions were objectively reasonable given the facts and circumstances at that time. This concept is commonly referred to as the Rendulic Rule.[8]

Distinction. The principle of distinction requires that "parties to a conflict shall at all times distinguish between the civilian population and combatants and between civilian objects and military objectives and accordingly shall direct their operations only against military objectives."[9] This task may be difficult in a large-scale combat environment due to limited sensors and intelligence and communications assets. Those who plan or decide upon an attack are required to "do everything *feasible* to verify that the objectives to be attacked are neither civilians nor civilian objects and are not subject to special protection but are military objectives."[10] The key term here is feasible; what is or is not feasible is clearly situation dependent. In an underdeveloped operational environment with a rapidly shifting landscape, the feasibility of attaining redundant targeting information differs significantly from that of gathering information in a developed operational environment with multiple ISR assets available to provide information on a potential target.

Proportionality. The principle of proportionality directs commanders to "refrain from attacks in which the expected loss of civilian life, injury to civilians, and damage to civilian objects incidental to the attack would be excessive in relation to the concrete and direct military advantage expected to be gained;" along with the duty to take feasible precautions to limit collateral damage.[11] Furthermore, "the commander's decisions on proportionality must be reasonable. . . . The commander must be able to explain the expected military importance of the target and why the anticipated civilian collateral injury or damage is not expected to be excessive."[12] However, the *Department of Defense Law of War Manual* notes that deference should be granted to commanders during assessments regarding whether they have complied with the principle of proportionality, and any judgment of compliance with legal requirements must be based on the information available to the commander at the time.[13]

Humanity. The principle of humanity in the *Law of War* prohibits using methods of warfare that cause unnecessary suffering or superfluous injury.[14] This refers to harm that goes beyond what is necessary to disable a combatant. This concept often involves the means and methods used to achieve desired effects. Commanders should understand that, regardless of military necessity, suffering inflicted may be considered unnecessary if it is deemed inhuman or barbaric by constructs outlined in International Humanitarian Law (e.g., the Hague Conventions).

Evaluating and determining compliance with the LOAC is complicated, and it can involve a significant assumption of risk. During large-scale combat operations, decision makers in the targeting process will be required to act with limited information on an accelerated timeline. Personnel involved in the decision-making process should do what is feasible, make good-faith decisions, be prepared to explain their reasoning if prompted, and remember that their actions will be evaluated based only on information that was visible through the fog of war.

Conclusion

Targeting operations vary significantly between developed and underdeveloped operational environments because of

differences in infrastructure, technology, and the nature of conflicts. In developed operational environments, such as modern urban environments or advanced industrialized nations, operations benefit from robust communication networks, sophisticated surveillance systems, and access to comprehensive databases. The intelligence warfighting function is integral to the targeting process. In developed operational environments, military intelligence relies heavily on advanced technology, including satellite imagery, drones, electronic surveillance, and cyberspace operations. These resources provide real-time data, enabling commanders to monitor enemy movements, assess threats, and make informed decisions quickly. Additionally, developed operational environments often have well-established intelligence agencies with experienced personnel trained in sophisticated analysis techniques.

In contrast, underdeveloped operational environments, such as remote or rural regions, offer significant challenges to targeting operations. A lack of advanced technological resources often means decision makers must rely on more traditional intelligence-gathering methods associated with targeting, such as human intelligence and signals intelligence. In these environments, intelligence gathering often relies on leveraging available assets to gather information on enemy activities, while tempering expectations due to the conditions associated with large-scale combat operations.

While targeting operations share common principles across all operational environments and conflict types, the varying conditions and challenges between developed and underdeveloped environments necessitate adaptable strategies and approaches for gathering, analyzing, and utilizing available intelligence effectively in support of the targeting process. For a profession tasked with fighting and winning our Nation's wars, the reality of making rapid decisions based on limited information in large-scale combat operations is both risky and necessary. Consider, though, this comparison: the medical profession pledges to prescribe only beneficial treatments, according to their abilities and judgment, and to refrain from causing harm or hurt.[15] However, each year in the United States alone, 251,000 people are lost to medical malpractice.[16] These deaths are the collateral consequences of lifesaving medical treatment that many patients often need and a risk that most patients willingly absorb. Perhaps our expectations regarding the reality of warfare and large-scale combat operations have been skewed in the nearly 80 years since our world experienced such a global conflict.[17]

Epigraph

Jim Garamone, "Dunford: Speed of Military Decision-Making Must Exceed Speed of War," News, U.S. Department of Defense, January 31, 2017, https://www.defense.gov/News/News-Stories/Article/Article/1066045/dunford-speed-of-military-decision-making-must-exceed-speed-of-war/.

Endnotes

1. Chairman of the Joint Chiefs of Staff, Joint Publication 3-0, *Joint Campaigns and Operations* (Joint Staff, 2022), III-31.

2. Department of the Army, Field Manual (FM) 3-60, *Army Targeting* (Government Publishing Office, 2023), 2-1.

3. Department of the Army, FM 3-60, *Army Targeting*, I-1.

4. Major General David Gardner (Commanding General, Joint Readiness Training Center and Fort Johnson [Polk]), in telephone interview with author(s), April 23, 2024. The priorities discussed here are informed by MG Gardner's experience as the Commander, Operations Group and as Commander, Joint Readiness Training Center.

5. Colonel Matthew Hardman (Commander, Operations Group, Joint Readiness Training Center), in telephone interview with author(s), April 25, 2024.

6. Department of Defense, *Department of Defense Law of War Manual* (Office of General Counsel, 2015), 17, https://media.defense.gov/2023/Jul/31/2003271432/-1/-1/0/DOD-LAW-OF-WAR-MANUAL-JUNE-2015-UPDATED-JULY%202023.PDF. Change 1 was issued on December 13, 2016. Change 2 was issued on July 31, 2023.

7. Ibid., 52.

8. The United Nations War Crimes Commission, *Law Reports of Trials of War Criminals, Volume VIII* (His Majesty's Stationery Office, 1949), 68-69, https://tile.loc.gov/storage-services/service/ll/llmlp/Law-Reports_Vol-8/Law-Reports_Vol-8.pdf. For context, this "rule" was generated based on the prosecution of German General Lothar Rendulic, who conducted a scorched-earth retreat under the false belief that Soviet forces were pursuing him. "There is evidence in the record that there was no military necessity for this destruction and devastation. An examination of the facts in retrospect can well sustain this conclusion. But we are obliged to judge the situation as it appeared to the defendant at the time. If the facts were such as would justify the action by the exercise of judgment, after giving consideration to all the factors and existing possibilities, even though the conclusion reached may have been faulty, it cannot be said to be criminal."

9. International Committee of the Red Cross Database, Treaties, States Parties and Commentaries, Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977, Article 48 - Basic rule, https://ihl-databases.icrc.org/en/ihl-treaties/api-1977/article-48.

10. International Committee of the Red Cross Database, Treaties, States Parties and Commentaries, Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977, Article 57 – Precautions in attack, https://ihl-databases.icrc.org/en/ihl-treaties/api-1977/article-57. (emphasis mine).

11. Department of Defense, *Law of War*, 268.

12. Ibid., 252.

13. Ibid., 254.

14. Ibid., 367.

15. Robert H. Shmerling, "First, do no harm," Harvard Health Blog, Harvard Health Publishing, June 22, 2020, https://www.health.harvard.edu/blog/first-do-no-harm-201510138421.

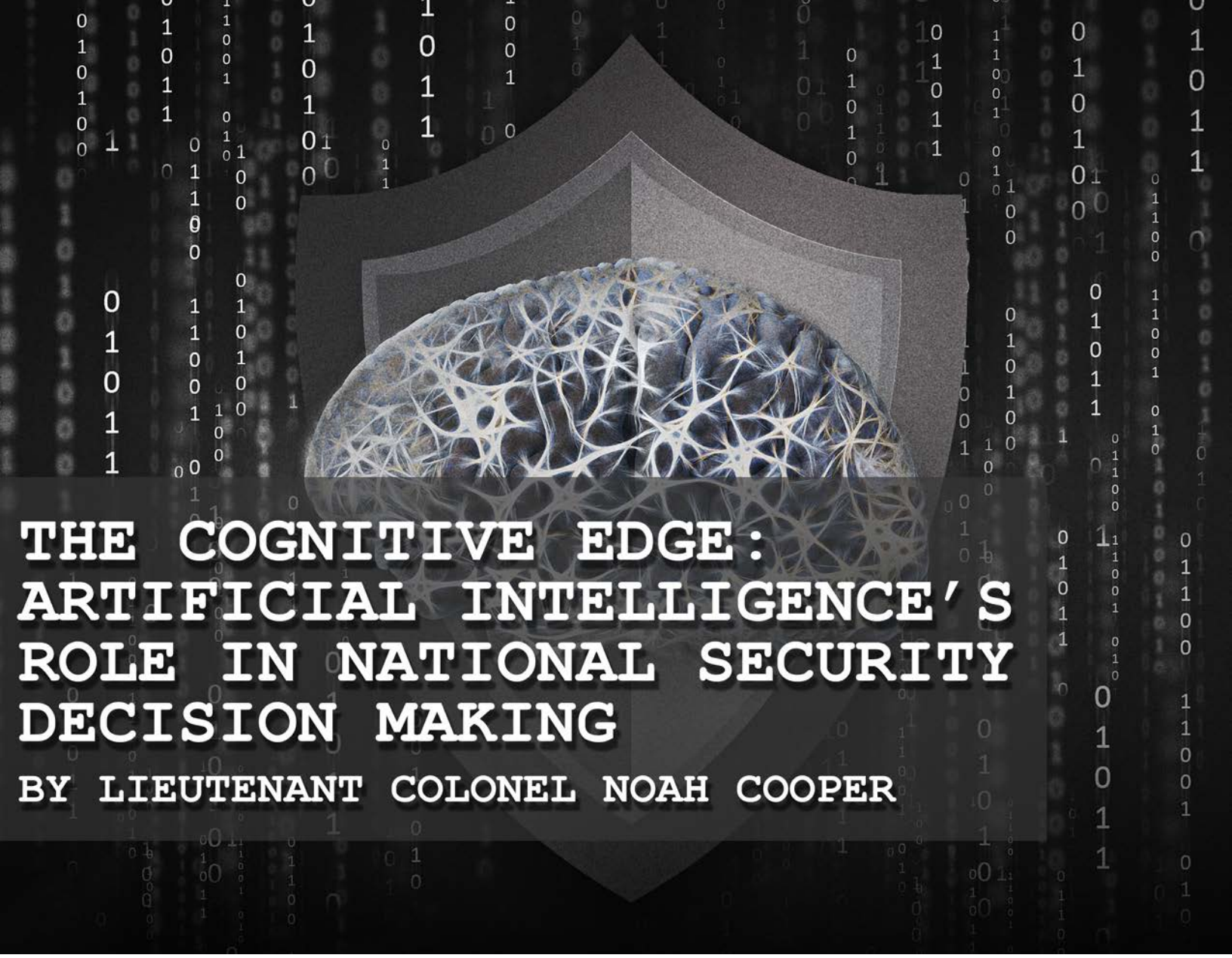
16. James G. Anderson and Kathleen Abrahamson, "Your Health Care May Kill You: Medical Errors," *Studies in Health Technology and Informatics* 234, (2017):13-17, https://pubmed.ncbi.nlm.nih.gov/28186008/.

17. Hardman, telephone interview. A point of discussion between Colonel Hardman and the authors was the cognitive dissonance associated with war and its impact on the targeting process. Although every life matters, that fact must be balanced against the desire to do the greatest good for the greatest number of people. How that dichotomy factors into the targeting process for decision makers at all levels, and to what end, is a reasonable consideration to associate with warfare, in contrast to the unnecessary consequences associated with the work of other professions (e.g., the medical profession, as referenced in the previous endnote).

MAJ Kyle Flanick's previous assignments include service as Interagency Liaison Officer to the National Capital Region for the 75th Ranger Regiment, fire support officer for the Regimental Special Troops Battalion, and Commander of E Battery, Task Force 1st Battalion, 28th Infantry Regiment, 3rd Infantry Division. MAJ Flanick's military education includes the Special Operations Terminal Attack Controller Course, Air Assault School, Airborne School, and Jumpmaster School. He is a 2025 graduate of the Marine Corps University Command and Staff College and a 2013 graduate of Messiah College.

MAJ Michael Fox is the deputy regimental S-2 for the 75th Ranger Regiment. His previous special operations assignments included serving as the 75th Regimental Special Troops Battalion S-2, assistant S-2 to the 75th Ranger Regiment, and as commander of the 75th Ranger Regiment's military intelligence company. MAJ Fox's military education includes the Signals Intelligence Course, Air Assault School, Airborne School, and Jumpmaster School. He is a 2012 graduate of The Citadel, The Military College of South Carolina.

MAJ Matthew Smith is the Chief of Military Justice at the U.S. Army Maneuver Center of Excellence. He previously served as a tank platoon leader, mortar platoon leader, and aide-de-camp as an armor officer. As a judge advocate, he served as a military justice advisor and was the Chief of National Security Law for the 82nd Airborne Division. MAJ Smith's education includes master's degrees from the Command and General Staff College and Columbus State University. He completed his legum magister (master of laws) at The Judge Advocate General's Legal Center and School, and he earned his juris doctor (doctor of law) from Boston College Law School along with a graduate certificate in cybersecurity policy and governance. He also completed the Airborne, Ranger, and Pathfinder courses. He is a 2012 graduate of The Citadel, The Military College of South Carolina.



THE COGNITIVE EDGE: ARTIFICIAL INTELLIGENCE'S ROLE IN NATIONAL SECURITY DECISION MAKING

BY LIEUTENANT COLONEL NOAH COOPER

Decision making in the context of national security occurs amidst uncertainty, ambiguous information, time and resource constraints, and other dynamics that create an admixture of variables, which, combined, impose immense pressure on those with decision-making authority. Navigating the complex factors involved in resolving an evolving and potentially escalating crisis demands a careful balance of short- and long-term strategies to counter a competitor with clear malicious intentions. Furthermore, it is essential to assess whether existing policy approaches have failed, which could prompt the difficult consideration of armed conflict to secure a more advantageous security posture. These challenges profoundly test the limits of human cognition. Decision makers employ a combination of the advice provided by subordinates, the counsel given by seasoned experts, and their own intuition to guide their thought processes to seek optimal solutions to issues under consideration. Complicating this is the requirement to contend with multiple time-constrained, rapidly evolving scenarios, which are emblematic of today's national security landscape.

To cope with these challenges inherent to guiding national security outcomes, artificial intelligence (AI) could serve as an ideal adjunct to the decision-making process. Specifically, AI could augment and overcome the limitations of human cognition in three ways: first, by providing real-time decision support through the timely analysis of the myriad data points that feed such decisions, second, through the simulation and modeling of scenarios to present alternative perspectives and outcomes or to anticipate responses, and, third, to combat the negative implications associated with cognitive biases. Accordingly, in examining AI's role in enhancing decision support, it is worthwhile to understand the impact of this emerging technology.

The Limits of the Mind

Before explaining the utility of AI support to national security decision making, it is important to understand how the human mind processes data and its associated limitations. The interaction of biological, psychological, environmental, and social factors affects how humans perceive, process, and

respond to information. The influence of each of these factors varies, corresponding to an additional set of variables, including time, age, attention, and memory limitations. Understanding the totality of human cognition is beyond the scope of this article; however, it is valuable to note that despite the impressive ability of humans to intake and analyze data, the human mind remains a fallible tool, impacted by cognitive biases, challenges associated with processing information, and the ever-present emotional influences that skew rationality and lead to impulsive decisions.

"Cognitive biases are mental errors caused by our simplified information processing strategies."[1] Simply stated, cognitive biases are mental shortcuts or patterns that lead to errors in reasoning or judgment. A common example of a cognitive bias is confirmation bias, which involves seeking information that supports a pre-existing idea or belief. For example, a stark instance of confirmation bias that negatively affected national security decision making occurred before the 1941 Japanese attack on Pearl Harbor. Decision makers in the United States believed Japan was more likely to attack targets in the Southwest Pacific to secure natural resources.[2] As a result, the United States downplayed evidence that Japan was planning a surprise attack on Hawaii as the information did not conform to expectations. Historical vignettes like this illustrate the importance of thinking critically and questioning established assumptions. Failure to do so in the context of defense and national security could yield deadly consequences.

Mental models or biases are dangerous for a variety of reasons: they can distort the understanding of a situation by altering how individuals process information, undermine objective decision making, prompt faulty assessments and thus increase risks, and, perhaps most applicable to national security decision making, compound errors through the unintentional rejection of relevant data or through the misjudgment of an actor's ability to influence a situation. There are many approaches to mitigating the impacts of cognitive biases, such as using critical thinking frameworks, employing decision-making tools, and implementing technology solutions. Most importantly, awareness, recognition, and contending with cognitive biases are crucial to effective decision making, particularly in the high-stakes realm of national security.

Information Processing

Humans process data through a combination of sensory, cognitive, perceptual, attention, and other mental frameworks that directly shape cognition and decision making.[3] Understanding how humans process information serves to identify the strengths and limitations of cognition, which contributes to more effective and positive decision-making outcomes. Every second, sensory inputs bombard the human mind with environmental stimuli. Fundamentally, the brain categorizes these stimuli into relevant and irrelevant data or, simply, information required for safety and survival and that which is not necessary. Unnecessary information is discarded. The mind then encodes and stores important information in short-term or long-term memory for recognition or retrieval.[4] This information is then used for processing and decision making. Through this interconnected cycle, humans receive, optimize, and process information based on the unique circumstances encountered.

Though highly sophisticated, human information processing is not without drawbacks. First, humans have a limited working memory capacity, which can result in information overload when contending with complexity.[5] Second, compared to the processing speed of information technology systems, human cognition is relatively sluggish, which can slow the overall decision-making process. Finally, human cognitive performance declines with fatigue, which can impair decision making.

The role and impact of emotions in decision making are multifaceted. Emotions have the propensity to shape human choices, either positively or detrimentally. Optimism and confidence grounded in objectivity and realism can encourage creative thought and the exploration of alternative approaches to a problem. At the same time, impulsivity and irrationality can prompt a decision maker to myopically focus on a singular outcome that does not seek an optimal resolution. Since they are often made rapidly, emotional decisions may not conform to long-term goals.[6] This condition of emotional decision making illustrates the importance of understanding the psychology of one's decision making to make more rational and informed choices.

Artificial Intelligence as an Aid

The recent rapid advances in AI technology will likely offer significant potential to aid national security decision making. Fully overcoming the limitations of human cognition is not a feasible prospect; however, implementing measures to mitigate some of the negative impact is reasonable and necessary, particularly in the fast-paced arena of national security, where an incorrect or off-base decision can have cascading effects. Given this importance, it is imperative to employ structured frameworks to overcome the impact of cognitive biases, to consider and attempt to regulate one's emotional state before proposing a decision that could yield significant consequences, and to understand the limitations of human information processing. AI can complement these practices by enhancing data analysis, by modeling realistic scenarios that gauge responses to security challenges, and by moderating the influence of cognitive biases and human emotions through the provision of data-driven and objective analysis.

The requirements to balance competing interests, mitigate risks, and contend with continuously developing and evolving crises are just some characteristics of national security

decision making. For each of these concerns, decision makers encounter an overwhelming volume of data from many sources, including intelligence and diplomatic reports, social media, imagery, and advice from subordinates and colleagues. Ideally, the information provided to a decision maker results from a structured, orderly process involving multiple layers of quality assurance and review to ensure timely and responsive delivery. However, the dynamics of the global security environment and the need to contend with information from multiple sources generate interpretation and analytical challenges for the decision maker. AI is an ideal means to provide structured analysis to enable data-intensive national security decision making. AI's capability to synthesize multiple data points and identify patterns in large data sets is an effective means of data analysis to determine threat indications. Additionally, AI's rapid or real-time data processing capability can specify the primary catalyst of an issue, making deliberations more efficient for decision makers.

AI is most notable for its computational and data analytics capabilities. However, it also offers unique modeling and simulation functions that can help national security decision makers overcome ambiguity and complexity to make informed and effective decisions. Using historical data, AI could quickly create vignettes based on user input to determine the most favorable response to a given scenario. For instance, an AI algorithm trained on game theory could explore interactions between peer adversaries competing just below the threshold of armed conflict, or in a situation where responses are not always scripted or anticipated. In cases where pre-planned responses exist, AI could test the viability and the feasibility of interactions and adapt them to new circumstances and facts on the ground while simultaneously determining their success potential. Moreover, given the complexity of the global security environment, conflicts involving only two actors are rare; decision makers must consider multiple economic, diplomatic, and military interdependencies among numerous actors. An AI-powered modeling and simulation capability could aid in exploring the implications of these various factors and their ramifications for each actor. These capabilities represent just a sampling of the potential modeling and simulation prospects of AI.[7] Other potential modeling and simulation uses could include support to military operations through the evaluation and testing of operational plans, the development of real-time visualizations to depict and represent ongoing events and crises, and depictions that explore actions in multiple domains.

Perhaps AI's most integral function is its potential to mitigate the deleterious impact of cognitive biases and thus improve human decision making. The human mind is prone to unintentional errors and subjectivity and tends to favor preconceived ideas that support an individual's beliefs. Overcoming these issues, particularly in a time-constrained decision-making cycle, is not just challenging but close to impossible. The Prussian military philosopher Carl von Clausewitz spoke of the *coup d'œil*, or the "inward eye" that enables a battlefield commander to see "a truth that the mind would ordinarily miss or would perceive only after long study and reflection."[8] It is difficult to challenge Clausewitz's assertion that successful military commanders possess an intrinsic genius that allows them to make quick yet informed decisions, which could potentially alter the outcome of a battle. However, our understanding of human cognition has advanced considerably since his time and has not fully reinforced the natural coup d'œil; instead, it has revealed the contradictory mechanisms that subconsciously skew human perception and understanding of the environment. A deeper understanding of human thought necessitates implementing measures to overcome the problems posed by cognitive biases and mental models.

AI can aid in tempering these issues by invoking increased impartiality and the rigor necessary to counteract the impact of such biases. Through a data-driven approach, AI can offer objective, emotionally disconnected recommendations that correspond to recognized norms and practices. When appropriately trained, AI could employ structured analytical techniques such as red-teaming, analysis of competing hypotheses, alternative futures analysis, and other approaches to provide a decision maker with unbiased decision recommendations, validated by stringent data analysis and analytical methodologies.[9] It is important to note a potentially significant fault with AI, however: the risk that training data used to develop the AI algorithm could contain information already flawed by bias, inaccuracies, or falsehoods. Despite AI's data analysis advantages, decision makers should, therefore, be measured and cautious about incorporating such data until a means is in place to extricate any pre-existing bias.

Conclusion

The advances in artificial intelligence offer a unique capability to manage the challenges inherent to national security decision making. With its ability to handle vast amounts of data, AI is a tool that can integrate information from multiple sources into digestible and easily comprehensible visualizations at a rate that far surpasses human analysts. AI modeling and simulation offer a rapid means to assess and forecast the impacts of national security decisions, which could identify possible unintended outcomes. Perhaps most importantly, AI can serve as a vital tool to mitigate the consequences of cognitive biases. AI can process data systematically and free from the biases introduced by human cognition. This technology offers a means to moderate the impact of emotionally charged decision making by providing objectively synthesized information, free from human emotional influence.

Given the advantages of leveraging AI in national security decision making, we must address the inevitable question: Does the automated analysis of current or potential events and crises render human judgment unnecessary? Though human cognition cannot compete with the data processing power of AI systems, the need for human judgment in national security decision making remains fundamentally unaltered.[10] AI is unlikely to develop or exhibit the creativity or ingenuity intrinsic to the human mind, especially when contending with highly complex and delicate national security issues. At the same time, however, humans cannot contend with the influx of multiple data flows and will exhibit cognitive fatigue over time. Individually, AI and humans are both fallible; however, integrating decision making between man and machine allows for the distillation of data into easily discernible components while preserving the originality and vision that would enable human decision makers to think more effectively and thus to produce significantly more accurate national security decisions.

Endnotes

1. Richards J. Heuer, Jr., *Psychology of Intelligence Analysis* (Center for the Study of Intelligence, 1999), 111, https://www.cia.gov/resources/csi/static/Pyschology-of-Intelligence-Analysis.pdf.

2. Lori S. Tagg, "Intelligence, Japanese Attack on Pearl Harbor," U.S. Army website, January 4, 2017, https://www.army.mil/article/180285/intelligence_japanese_attack_on_pearl_harbor.

3. Sabine Prezenski, André Brechmann, Susann Wolff, and Nele Russwinkel, "A Cognitive Modeling Approach to Strategy Formation in Dynamic Decision Making," *Frontiers in Psychology* 8 (2017):1335, https://www.frontiersin.org/journals/psychology/articles/10.3389/fpsyg.2017.01335/full.

4. Ibid.

5. George A. Miller, "The Magical Number Seven, Plus or Minus Two: Some Limits on Our Capacity for Processing Information," *Psychological Review* 63, no. 2 (1956):81-97, https://doi.org/10.1037/h0043158.

6. Sk Mustain, "Understanding Human Behavior: The Psychology of Decision Making," Medium, September 20, 2023, https://medium.com/@skmustain/understanding-human-behavior-the-psychology-of-decision-making-4ed6c884146a.

7. Jack Hidary, "Beyond ChatGPT: AI Simulation is the Next Frontier of Advanced Computing," Innovation, Forbes, January 12, 2024, https://www.forbes.com/councils/forbestechcouncil/2024/01/12/beyond-chatgpt-ai-simulation-is-the-next-frontier-of-advanced-computing/.

8. Carl von Clausewitz, *On War*, trans. Michael Eliot Howard and Peter Paret (Princeton University Press, 1989).

9. *A Tradecraft Primer: Structure Analytic Techniques for Improving Intelligence Analysis* (Center for the Study of Intelligence, 2009), https://www.cia.gov/resources/csi/static/Tradecraft-Primer-apr09.pdf.

10. Damien van Puyvelde, Stephen Coulthart, and M. Shahriar Hossain, "Beyond the Buzzword: Big Data and National Security Decision-Making," *International Affairs (Royal Institute of International Affairs 1944—)* 93, no. 6 (2017): 1397-1416, https://www.jstor.org/stable/48570026.

LTC Noah Cooper is a career Army military intelligence officer with nearly 20 years of experience. He currently serves as an instructor at the Joint Forces Staff College, Joint and Combined Warfighting School. He received a master of arts degree from Johns Hopkins University and from King's College London.

MI Is Out Front in Army Transformation

by Major General John D. Thomas, Jr.

Photo Couresy of SPC Timothy J. Belt.

Editor's Note: In continuation of the historical retrospective that began with our 50th Anniversary Commemorative Compilation, every quarter, the Military Intelligence Professional Bulletin will highlight an article from the past that is still relevant today. This article first appeared in the October–December 2000 issue.

This special issue of the ***Military Intelligence Professional Bulletin (MIPB)*** focuses on transformation. The Chief of Staff of the Army identified transformation as a crucial aspect of his vision. This Army transformation by design will make the Army a full spectrum, strategically relevant force. The Military Intelligence Corps plays a key role in Army Transformation. The basis for many of the initiatives that will move the Army to the objective force is an assumption of improved situational awareness, which includes an accurate and timely understanding of opponents, neutrals, weather, and terrain. Achievement of this increased level of situational awareness rests, in large measure, on our ability to deliver refined intelligence products across the force. This is an exciting time to be intelligence professionals and promises to move our Corps into an even closer membership in the combined arms team.

We often think of transformation as focusing on equipment. Although equipment is important, it is the human dimension—our soldiers and civilians—that will transform the Army. Transformation is a new way of doing our business, not simply a "tweaking" of our Cold War organizations, but rather a fundamental examination of what the MI Corps must accomplish as part of the combined arms team. In this issue of ***MIPB***, we will discuss many aspects of transformation, but I would first like to set the stage.

Enabling and Integrated Intelligence

The MI Corps has primarily focused on providing "enabling" intelligence, which dealt mainly with the disposition and intention of opponent formations. This intelligence is essential for conducting the military decisionmaking process and critical to a commander disposing and committing his formations. It is primarily a planning-focused activity. Once direct combat operation began within the "Red zone," there was little direct intelligence contribution. Weapons system capabilities often provided the basis for mission effectiveness and stand off.

With changes in the operational environment, especially the proliferation of sophisticated weapons systems and the requirement to deploy forces quickly over long distances, we must change the mission effectiveness equation. Intelligence, surveillance, and reconnaissance (ISR) must become part of the overmatch ratio. ISR together with mobility, lethality, and survivability must be what guarantees overmatch during the close fight on the 21st century battlefield. In addition to "enabling" intelligence, we must provide "integrated" intelligence—that intelligence which is closely linked to the tactical operator engaged in the "Red zone" fight. These intelligence capabilities must be a part of the ongoing combat operation, not just support planning of the operation. Some examples of this approach are—

- Integrated human intelligence (HUMINT) soldiers in the Reconnaissance, Surveillance, and Target Acquisition (RSTA) Squadrons of the Initial Brigade Combat Teams (IBCTs).
- Provision of enemy situational awareness information directly to combat platforms by the Force XXI Battle Command Brigade and Below (FBCB2) system.
- Integration of unmanned aerial vehicles (UAVs) with manned Army Aviation helicopters.

Force Structure

The force structure of the MI Corps must support our mission. We need increased analysis, HUMINT, and imagery capabilities within our tactical organization. Additionally, we need to improve our ability to focus and integrate the myriad ISR capabilities available to a

Photo Couresy of SPC Timothy J. Belt.

commander. These assets include a wide range of capabilities operated across the battlefield by both MI organizations and other battlefield functional areas such as Army Aviation, Special Operations Forces, Field Artillery, Chemical Corps, Engineers, and many others. This integration role has long been the function of the intelligence officer but in many cases, neither the personnel nor the equipment were available to accomplish the mission. The varied nature of the future battlefield makes this integration mandatory.

The Reserve Component's MI force structure—for the U.S. Army Reserve (USAR) and the U.S. Army National Guard (ARNG)—must also transform. Crucial initiatives include the organization of additional, fully capable, divisional MI battalions in the ARNG and more effective support organizations in the USAR. The superb performance of ARNG and USAR soldiers in recent operations and contingencies underscores both the value of these professionals and the importance of proper structure and integration.

U.S. Army photo.

Equipment and Personnel

There **is** an equipment aspect to transformation. First, our equipment must get to the fight. All equipment must be C-130-transportable. We must integrate functions of various pieces of equipment to reduce tactical operations center (TOC) footprint and deployability issues. MI must develop and field sensors specifically aimed at the urban environment. Our automation systems—the All-Source Analysis System (ASAS) and the Army Battle Command System (ABCS)—must be able to share a common picture with all echelons and the joint and national intelligence community. They must also provide tools across the operational spectrum from stability and support operations, through small-scale contingencies, to high-intensity operations.

The key to successful transformation remains our soldiers and civilians. We must continue to develop their basic intelligence skills of analysis, collection, and integration. None of these initiatives in any way reduces the requirement for first-class individual intelligence skills capable of operating in the digital environment of the information age. Our military occupational specialty (MOS) structure needs critical examination to ensure it provides the commander with the expertise and flexibility to operate in the 21st century and also assures rewarding career opportunities for our soldiers. Strong leadership by our officers, noncommissioned officers, and civilians will be required during this period of unprecedented change.

Conclusion

Our organizations, equipment, doctrine, and training will change, but the result will be the provision of improved intelligence as part of the combined-arms team. It is important that we all understand the mission and environment of today's Army and move out to continue our tradition as the best intelligence service in the world.

ALWAYS OUT FRONT!

Major General John D. Thomas, Jr., enlisted in the U.S. Army in 1968. He received his commission following graduation as a Distinguished Graduate from the Field Artillery Officer Candidate School and his initial positions were in the 7th and 2d Infantry Divisions and command of an AIT (advanced individual training) company. His past intelligence and electronic warfare assignments included Field Station Augsburg; the Combined Forces Command and U.S. Forces–Korea; the Department of the Army Staff; Deputy Chief for Intelligence, Special Technical Operations Division, J3, Joint Staff; and Associate Deputy Director for Operations (Military Support) at the National Security Agency (NSA) and Deputy Chief, Central Security Service (CSS). MG Thomas has served in many command positions including C Company (Guardrail), 15th MI Battalion (Aerial Exploitation (AE)), 504th MI Brigade; 3d MI Battalion (AE), 501st MI Brigade; 11th MI Brigade (Training); U.S. Army Intelligence and Security Command (INSCOM); and the U.S. Army Intelligence Center and Fort Huachuca. He became the fifth Chief of the MI Corps in June 1998. He is a graduate of the Armed Forces Staff College and the National War College . MG Thomas is a Master Army Aviator rated in both fixed-wing and rotary aircraft and is a fixed-wing instructor pilot. He earned a Bachelor of Arts degree in History from Wilkes College in Wilkes-Barre, Pennsylvania, and a Master of Arts degree in International Relations from the University of Southern California.

34th Infantry Division Soldier cools the expandable van temporary sensitive compartmented information facility environmental control unit using a commercial off-the-shelf water gun. (U.S. Army Photo by SPC Tyler Becker)

NEAR-TERM COMMAND POST SURVIVABILITY: LESSONS LEARNED FOR THE INTELLIGENCE COMMUNITY

BY CAPTAIN AUSTIN LIND

Introduction

Division G-2's must evolve to maintain survivability during large scale combat operations. Command post (CP) survivability is a critical aspect of military operations during large-scale combat; however, the traditional CP configuration, with electronic emitters, dozens of generators and vehicles, and extensive support requirements, is easily targeted and destroyed by an ever-expanding array of threat sensors and shooters. The 2023 *Military Review* article, "The Graveyard of Command Posts," addresses the vulnerability of traditional CPs.[1] Near-term solutions for more survivable CPs require an assessment of tactics, techniques, and procedures (TTPs) focused on survivability using existing equipment. To increase survivability, division intelligence elements must operate in the rear and increase the mobility of forward elements. At the same time, the intelligence warfighting function must consider security requirements when planning distributed operations.

Division intelligence staff require access to sensitive compartmented information (SCI) to conduct operations and inform the commander's decision making. SCI is classified information concerning or derived from intelligence sources, methods, or analytical processes, which must be managed within formal access control systems established by the Director of National Intelligence.[2] SCI may only be processed in a secure, enclosed area designed for processing and handling SCI, known as a sensitive compartmented information facility (SCIF).

34th Infantry Division's temporary sensitive compartmented information facility while conducting dispersed operations in the U.S. Central Command area of responsibility. (U.S. Army Photo by SPC Tyler Becker)

While deployed to the U.S. Central Command area of responsibility, the 34th Infantry Division fielded the Integrated Tactical Network (ITN) as part of the Army 2030 and Transformation in Contact initiatives. Concurrently, the 34th Infantry Division was tasked with conducting distributed CP operations to provide feedback to the Army on CP survivability. The goal was for the division to train on the new ITN equipment, conduct a CP survivability assessment using the ITN equipment, and support mission requirements for Operation Spartan Shield while distributed. To accommodate this requirement, the 34th Infantry Division G-2 used a distributed mobile temporary SCIF, or T-SCIF, capable of all-source intelligence operations.

Lessons Learned for the Intelligence Community

The 34th Infantry Division G-2 incorporated five principles of near-term CP survivability drawn from the March 2023 U.S. Combined Arms Center white paper, *Near-Term Command Post Survivability*,[3] into the planning process, which culminated in a successful command post exercise in August 2024. (The article addresses integrating the five principles in a later section.) The G-2's experience with distributed SCIF operations and the ITN equipment offers valuable insights and lessons into near-term CP survivability and ways ahead for the intelligence warfighting function when conducting distributed operations.

The special security officer is integral to distributed command post intelligence operations. The special security officer (SSO) is responsible for overseeing the physical and technical security measures that protect SCI. In a distributed environment where intelligence activities are conducted across multiple locations, the SSO must ensure security measures are applied consistently and effectively across all locations. This may involve working with other SSOs, special security representatives (SSRs), and security managers. Accreditation documentation for SCIFs must be completed by an SSO who should be an E-7 or above and appointed by the senior intelligence officer.[4] SSRs are physically located at distributed sites, where they assist with implementing the SCI Security Program and managing SCIF operations under the direction of the SSO. SSRs can be E-5s and above and are appointed by the senior intelligence officer.[5] The SSO and SSRs must have in-depth knowledge of both Army Regulation 380-28, *Army Sensitive Compartmented Information Security Program*, and Intelligence Community Directive 705, *Sensitive Compartmented Information Facilities*, before conducting distributed operations.[6]

SCIFs must be mobile in large-scale combat environments. A fixed SCIF does not offer the mobility necessary for survival in large-scale combat operations. A T-SCIF is the ideal type of facility for distributed intelligence operations.

> ***T-SCIFs are used . . . for a limited time where physical security construction standards associated with permanent facilities are not possible. They may include hardened structures (buildings and bunkers for example, truck-mounted or towed military shelters, tents, prefabricated modular trailers or buildings, and areas used on aircraft and surface and subsurface vessels).***[7]

Flexibility, adaptability, and mobility are necessary for CP survivability. The 34th Infantry Division G-2 found that using an M1087A1 Expandable Van in conjunction with military intelligence (MI) systems provided the best mobility and met the most operational requirements for large-scale combat operations. An expandable van offers a large workspace that can accommodate up to 10 Soldiers at one time alongside the necessary MI systems. This provided the division G-2 with a tactical mobile CP that enabled all the intelligence functions to operate within a single controlled space.

Utilizing an expandable van as a mobile T-SCIF also offers several security advantages because this type of mobile T-SCIF conforms better to SCIF regulations than an existing permanent building in a combat operations environment. Intelligence

Community Directive 705 states that any proposed T-SCIF structure previously occupied by a non-U.S. element must undergo a technical surveillance countermeasures (TSCM) inspection to prevent or detect the interception of sensitive or classified information. Therefore, any permanent type hardened structure in a deployment area would require a TSCM inspection.[8] However, division headquarters do not have the organic capability to conduct a sweep for surveillance devices, and coordinating a TSCM inspection is time-consuming and not feasible during large-scale combat operations. The Accrediting Official can avoid the risk posed by surveillance threats during large-scale combat if units use this mobile T-SCIF concept. Other security benefits include acoustic protection for a classified discussion area and an easily controlled single point of access to prevent surreptitious or forced entry. The mobile T-SCIF offers demonstrable benefits; however, division G-2s are not organically equipped with expandable vans. This is a capability gap that the Army should consider. Division intelligence must be allocated expandable vans or similar vehicles or find an alternative means of making a mobile T-SCIF when planning for large-scale combat operations.

Establishing a T-SCIF takes extensive planning and preparation and requires multiple steps. Establishing a T-SCIF is a complex undertaking vital for maintaining secure communications and intelligence operations, particularly in rapidly evolving environments. While established procedures exist, practical experience reveals critical nuances in successful T-SCIF deployment and sustained operation. This section covers key areas such as site selection, security protocols, personnel management, and accreditation. This analysis provides valuable insights for personnel responsible for establishing and maintaining secure intelligence capabilities in dynamic operational environments.

Site Selection. The location should be secure, free of counter-surveillance threats, and have adequate space for intelligence equipment and personnel. The SSO, SSRs, and military intelligence systems maintainers should utilize pre-deployment site surveys whenever possible to ensure the site is protected against surreptitious or forced entry.

Design and Construction. T-SCIFs have strict construction and security requirements, including establishing layers of physical security, access control, and manning requirements.

Equipment and Manning. Conduct pre-combat checks and inspections on vehicles and equipment, including workstations and MI systems. Mobile T-SCIFs contain sensitive equipment but are not equipped with an intrusion detection system. Therefore, they require adequate manning by SCI-indoctrinated personnel to accommodate 24-hour operations in a large-scale combat environment.

Personnel Security. All personnel must meet clearance requirements. The SSO or SSR should post a security clearance access roster at the single, controlled entrance for access control and verification of personnel.

Training. All T-SCIF personnel must train in proper handling of SCI information and sensitive equipment; they must also be grounded in T-SCIF procedures, including rehearsals of the standard operating procedures and emergency action plan.

Accreditation. The accreditation process involves a thorough review of the facility's physical and technical security measures, as well as its personnel, policies, and procedures. While the Accrediting Official determines what documentation is necessary for accreditation, it is the SSO who creates those documents with assistance as needed from SSRs.

Post Accreditation. Once the Accrediting Official approves the T-SCIF, the SSO or SSRs handle providing updates relating to the current locations and status of T-SCIFs under their control as directed by the combatant command SSO.[9]

Intelligence systems maintainers are instrumental in enabling distributed CP intelligence operations. Network access requests, communications security requests, and network testing of MI systems are complex, often unpredictable processes and should be factored into planning well before a division conducts distributed operations. MI systems maintainers are essential to these processes.

Establish competencies in convoy operations and plan for the wear and tear of intelligence equipment. While the mobile nature of the T-SCIF offered undeniable advantages, it also presented some unanticipated challenges. For example, when conducting dispersed operations, the expandable van's environmental control unit (ECU) could not compensate for both the outside temperature and the communication equipment's interior heat generation. To combat this, the 34th Infantry Division G-2 shaded the ECU with camouflage netting and used a water sprayer to cool the unit to prevent it from overheating.

Intelligence equipment in permanent structures, like those used during counterinsurgency operations, rarely moved and thus did not require regular recalibration. However, because of the jarring and vibration resulting from displacing the 34th Infantry Division G-2 T-SCIF, the equipment often required recalibration. Going forward, the Army may need to re-examine the design of intelligence equipment for better durability in mobile operations.

Establish clear classification guidance for the Integrated Tactical Network. The ITN is comprised of radios operating on the tactical scalable mobile ad-hoc networking waveform, which allows them to work in secret and sensitive but unclassified-encrypted (SBU–E) enclaves. These radios provide line-of-sight voice, data, and near real time friendly force position, location, and identification (PLI). Any equipment providing near real time PLI in the U.S. Central Command (CENTCOM) area of responsibility should be classified at the secret level,

The 34th Infantry Division expandable van temporary sensitive compartmented information facility environmental control unit. (U.S. Army Photo by SPC Tyler Becker)

depending on the mission; however, CENTCOM's classification guidance did not address SBU–E equipment, and there was no clear guidance on individual PLI data. CENTCOM is working with both the Joint Staff and Army Program Executive Office to address this emerging technology, but end-user organizations must continue to push for updated guidance.

Integrating Near-Term Survivability Principles[10]

The evolving threat landscape demands a re-evaluation of traditional CP security measures. Modern adversaries possess increasingly sophisticated capabilities to detect, target, and disrupt command and control nodes. Consequently, near-term survivability principles—encompassing dispersion, sub-surface cover and concealment considerations, signal management, and nodal movement—are paramount. This section explores the practical application of these principles, drawing on recent intelligence operations observations and offering recommendations for bolstering CP resilience in a contested environment.

Rearward functional echelonment. Most intelligence capabilities will remain in the rear. Divisions must assess the allocation of MI forces among distributed CPs in the large-scale combat environment.

Dispersion. The distributed CP concept requires dispersion of the division staff elements. Nodes must be broken down into sub-nodes, or "micro CPs," each with two mobile T-SCIFs providing top secret capability not only for intelligence personnel, but also for other division staff elements such as the G-31 (Training, Readiness, and Exercise Division) space and cyberspace electromagnetic activities personnel. Two mobile T-SCIFs provide redundancy to support intelligence operations in the event of a micro CP loss. The dispersed operations conducted by the 34th Infantry Division G-2 had two vehicles within its pod, mitigating the possibility of visual detection and targeting by indirect fire.

Sub-surface cover and concealment. We previously addressed the security risk of using permanent-type hardened structures in a large-scale combat environment. This includes sub-surface structures. While these structures can certainly provide cover and concealment for a T-SCIF, they nevertheless pose a surveillance security risk for SCIF operations and limit the CP's mobility. Additional planning is necessary to ensure the site is suitable for T-SCIF emplacement and MI system connectivity. Using hardened or sub-surface structures will require expanded TTPs to ensure intelligence elements have the flexibility, adaptability, and mobility necessary for CP survival.

Signal management. MI systems have a pronounced, identifiable signature, making them easier to target. Additionally, while ITN radios do not have distinct signatures when operating en masse, using them enhances the electromagnetic signature. The 34th Infantry Division G-2 attempted to gather baseline readings of electromagnetic activity and bandwidth usage for dispersed MI systems; however, the request did not have a high enough priority to receive collection. Use of MI systems in distributed operations nevertheless requires additional analysis to determine how they can "swim" within the electromagnetic spectrum, especially in austere environments.

Nodal movement. The 34th Infantry Division G-2 designed its mobile T-SCIF to pack up and jump to a new location within 24 hours, mitigating the risk of accurate, targetable detection by threats. By using two distributed mobile T-SCIFs, the division G-2 could alternate survivability bounds to ensure that at least one forward intelligence element is always operational.

Operation Spartan Chain

During Operation Spartan Chain, the 34th Infantry Division's mission command deployment within the larger Operation Spartan Shield contingency operation, the G-2 established a T-SCIF with connectivity to secret and top secret enclaves

Interior space of 34th Infantry Division's expandable van temporary sensitive compartmented information facility, displaying an Intelligence Fusion Server, Geospatial Intelligence plotter, and workstations. (U.S. Army Photo by SPC Tyler Becker)

within two hours. The G-2 can minimize set-up time further with the refinement of standard operating procedures and processes. The available space inside the expandable van allowed for one Geospatial Intelligence (GEOINT) Workstation, one GEOINT plotter, one Intelligence Fusion Server, and 10 classified network workstations with access to multiple web applications (e.g., AIDP, MAVEN, Chatsurfer). This allowed 10 intelligence Soldiers to operate inside the expandable van's T-SCIF at one time, representing all intelligence functions.

Recommendations Going Forward

To ensure robust intelligence support across a distributed command structure, a deliberate approach to node organization and communication is essential. These recommendations outline critical steps for division G-2s to optimize intelligence functions at each node, enhance cross-functional collaboration, and mitigate vulnerabilities inherent in dispersed operations.

Intelligence liaison officers at each node. Division G-2s should have a liaison officer with the command group and other distributed nodes. Working in a distributed environment isolates division staff sections from each other; however, staff collaboration within nodes is vital. For example, the field artillery intelligence officer needs to have a presence in the intelligence node to ensure an effective targeting process. Placing intelligence liaisons across nodes would ensure that updates to the common intelligence picture occur across all distributed CPs.

Cross-functional collaboration. When considering distributed nodes, division G-2s must consider how they allocate personnel by intelligence function to create the best situational understanding at each G-2 pod. Additionally, to synchronize with division efforts and facilitate cross-functional collaboration with the wider division staff, the placement of G-2 pods and systems within the division "starfish" must be a consideration in relation to the large-scale combat operational environment.

Approved collaboration peripherals. Collaboration peripherals are the tools that enable communication in distributed environments. SCIF collaboration peripherals must meet Department of Defense and Defense Intelligence Agency requirements as well as Intelligence Community Directive 705 specifications. The Accrediting Official must then approve their use. Division intelligence elements must ensure that adequate organic, approved collaboration peripherals are available at all distributed nodes.

Minimized electromagnetic footprint. MI systems, such as the TROJAN intelligence network system, have pronounced, identifiable signatures that make them easier to target. The intelligence warfighting function must allocate resources to determine how its systems can swim undetected within the electromagnetic spectrum. Until this is possible, division G-2s should consider holding distributed T-SCIFs in the rear for survivability.

Conclusion

Lessons and best practices from the 34th Infantry Division G-2's experience with distributed SCIF operations and ITN equipment highlight the importance of several key factors for ensuring CP survivability during large-scale combat operations. Involvement of the SSO and SSRs is crucial when planning, emplacing, and managing distributed SCIFs. Utilizing mobile T-SCIFs, particularly in vehicles such as expandable vans, offer a more flexible and adaptable solution than fixed or hardened SCIFs, while also conforming better to security regulations. Establishing a T-SCIF requires extensive planning and preparation, including site selection, design and construction, equipment and manning, personnel security, and training.

Additionally, T-SCIF operations require significant accreditation documentation. Staff should include military intelligence systems maintainers, who play a vital role in facilitating network access requests, communications security requests, and network testing of MI systems. In addition to these MI functions, dispersed operations compel the development of competencies in convoy operations and consideration of the wear and tear on intelligence equipment. Currently, there is not clear classification guidance for the ITN; this must be remedied to ensure effective communication and security.

The integration of near-term survivability principles, such as rearward functional echelonment, dispersion, signal management, and nodal movement, is crucial to ensuring CP survivability. The 34th Infantry Division G-2's experience with Operation Spartan Chain demonstrated the feasibility of establishing a T-SCIF and connectivity within a short timeframe. By applying these lessons and best practices, the intelligence warfighting function can operate more effectively and securely in a distributed environment during large-scale combat operations.

Endnotes

1. Milford Beagle, Jason Slider, and Matthew Arrol, "The Graveyard of Command Posts: What Chornobaivka Should Teach Us about Command and Control in Large-Scale Combat Operations," *Military Review* 103, no. 3 (2023): 10-24, https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/May-June-2023/Graveyard-of-Command-Posts/.

2. Office of the Director of National Intelligence (DNI), Intelligence Community Directive (ICD) No. 703, *Protection of Classified National Intelligence, Including Sensitive Compartmented Information* (2013), 2, https://www.odni.gov/files/documents/ICD/ICD-703.pdf.

3. Training and Doctrine Command (TRADOC) Proponent Office–Echelons Above Brigade (EAB), *White Paper: Near-Term Command Post Survivability*, Version 13 (Combined Arms Center, TRADOC, 2023).

4. Department of the Army, Army Regulation (AR) 380-28, *Army Sensitive Compartmented Information Security Program* (Government Publishing Office, 2018), 4.

5. Ibid., 5, 18.

6. Department of the Army, AR 380-28 *Army Sensitive Compartmented Information Security Program*; and Office of the DNI, ICD No. 705, *Sensitive Compartmented Information Facilities* (2010), https://www.dni.gov/files/documents/ICD/ICD-705-SCIFs.pdf.

7. Department of the Army, AR 380-28, *Sensitive Compartmented Information Security*, 18.

8. National Counterintelligence and Security Center, *Technical Specifications for Construction and Management of Sensitive Compartmented Information Facilities*, Version 1.5 (DNI, 2020), 47. https://www.dni.gov/files/Governance/IC-Tech-Specs-for-Const-and-Mgmt-of-SCIFs-v15.pdf.

9. Department of the Army, AR 380-28, *Sensitive Compartmented Information Security*, 18.

10. TRADOC Proponent Office–EAB, *Near-Term Command Post*.

CPT Austin Lind is the 34th Infantry Division Special Security Officer. He recently deployed to the U.S. Central Command area of responsibility in support of Operation Spartan Shield. He holds a degree in architecture and is currently studying for a master's of business administration at the University of Minnesota's Carson School of Management.

A human intelligence collector competes during the Inaugural Army Interrogation Olympics at Fort Bragg, NC, on 9 August 2022. (U.S. Army photo by SSG Jeremiah Meaney)

IMPROVING THE ARMY'S HUMAN INTELLIGENCE COLLECTOR

BY STAFF SERGEANT JOSHUA BADGER

Thoughts and opinions expressed in this article are those of the author. They do not reflect an official assessment of or the official policy or position of the U.S. Army Intelligence Center of Excellence or the Department of the Army.

Introduction

Over the past 15 years, the 35M military occupational specialty (MOS), Human Intelligence (HUMINT) Collector, has focused on three functions: intelligence interrogation, military source operations (now known as defense human activities), and debriefings. In 2024, a critical task site selection board updated the HUMINT collector critical task list to focus on interrogations and screenings, tasks most often associated with large-scale combat operations. This represents a significant shift from the HUMINT collector operations conducted over the past decade, and going forward, HUMINT collectors will primarily support the large-scale combat operations of maneuver commanders. To balance this shift in priorities, source operations will be severely curtailed for most HUMINT collectors. This presents an opportunity for 35M Soldiers to master the skills of interrogation and debriefing without the requirement to be top-level experts in a wide variety of other functions. This objective can be achieved by improving the assignment process, crafting new career development models, and reevaluating mission focus areas.

Opportunities and Challenges

The decision to refocus HUMINT collectors toward interrogation substantiates the need to specialize. This is most apparent within the U.S. Army Forces Command and the Army National Guard and Army Reserve, where over 80 percent of HUMINT collectors are assigned. Within the intelligence community and the Department of Defense, most top practitioners in this specialty dedicate themselves entirely to a singular focus, whether source handlers in the various government agencies, debriefers within the Defense Debriefing Service, or interrogators within the Joint Special Operations Command Intelligence Brigade and the High Value Detainee Interrogations Group.

Over the past 20 years, Army HUMINT collectors focused broadly on source operations, interrogations, and debriefings, leaving them less qualified and with less experience in any single area than their intelligence community and Department of Defense counterparts. However, with the focus now on large-scale combat operations, most Army HUMINT collectors can specialize in one area rather than be stretched amongst all the functions, thus becoming truly valuable assets to the Army and the greater intelligence community.

Retention among initial and mid-term HUMINT collectors historically has presented a challenge for the Army. Though the rate fluctuates, it is typically under 30 percent, and most HUMINT collectors cite the lack of opportunities to perform their assigned jobs as their primary reason for leaving Army service. Because it costs the Army over $150,000 to train a HUMINT collector that attends the Defense Language Institute, this disappointing retention rate represents a considerable investment loss. Making better use of trained HUMINT collectors and providing them with operational opportunities in their first assignment can address this significant concern and improve the retention rate.

A Way Forward

The following paragraphs contain recommendations for strengthening the HUMINT collector MOS, resulting in an Army HUMINT workforce that will better support the maneuver commander.

Duty Assignments. Refining the 35M MOS must begin with Advanced Individual Training (AIT). Course performance must be tied to a Soldier's potential first duty station to provide meaningful opportunities for practice and refinement of their specialty; this will require coordination with Human Resources Command and the Office of the Chief of Military Intelligence. Soldiers exhibiting higher-level potential should be assigned to units likely to have an active HUMINT collection mission, such as a Special Forces Group support battalion, U.S. Army Intelligence and Security Command, or a combatant command. The halted Quickstart program, which identified top performers during AIT and selected them for special follow-on assignments, could be reinstated to support this goal. A class order of merit list could be the basis for selection. A similar concept currently in use is the Advanced HUMINT Management Bridge, which typically provides Soldiers attending the MOS reclassification course follow-on opportunities through deployment or additional training. Sending high-performing 35M graduates to the Defense Strategic Debriefing Course is another option. This will further sharpen the foundational skills they acquired at AIT and certify them with the N7 (Strategic Debriefer) additional skill identifier, enabling them to conduct debriefing operations in specific areas of responsibility. Implementing any of these during 35M AIT would yield tremendous results for the force.

Force Reduction. Given continuing budgetary constraints, implementing these proposed solutions requires reducing the number of HUMINT collectors. Army structure changes address this issue but have the potential to further refine the 35M force structure through additional downsizing. An assumption under this model is that every 35M would become more valuable because the loss of manpower would be balanced against the increased skills they bring to the fight. If there are fewer HUMINT collectors, they must be better prepared.

Foreign Language Training. The current HUMINT collector language training model does not meet standards to operate effectively in large-scale combat operations. A complete discussion of those standards is beyond the scope of this article; for this discussion, we will note simply that the Army must revisit the requirement that HUMINT collectors must achieve, at minimum, Level 2 (advanced proficiency) in reading and listening and Level 1+ (high intermediate) in speaking on the Defense Language Proficiency Test. In addition, there will not be enough civilian interpreters to meet mission requirements in a large-scale combat environment.

Reading. The reading standard should be lowered or eliminated. This is especially relevant to document and media exploitation (DOMEX), which refers to the process of translating enemy documents. Historically, this has been a time- and resource-intensive process: if there was not a translator on site proficient enough in the target language to translate enemy documents, physical or digital copies had to be sent to the rear to be translated by linguists. Technological advances have made DOMEX a task that can be performed instantly by virtually any Soldier using a handheld electronic translator. Most Soldiers now use encrypted devices in place of hard-copy documents, which eliminates much of the need for on-the-spot DOMEX. Reducing or eliminating the reading requirements would allow HUMINT collectors more opportunities to master their speaking skills.

Speaking. The real value of the 35M lies in their speaking proficiency, and the current standard of Level 1+ (high intermediate proficiency) is simply insufficient to conduct operations in the target language at a valuable level. A Level 2+ (advanced-plus proficiency) and/or a successful Two-Score Oral Proficiency Interview (TSOPI) should be the minimum acceptable standard for the HUMINT collector. At that level, the practitioner will possess the skills necessary both to speak and to listen effectively while conducting operations.

Listening. The current listening standard of Level 2 (advanced proficiency) for the HUMINT collector is arguably irrelevant, as it is more applicable to linguists in the 35P (Signals Intelligence Voice Interceptor) MOS, who don't speak conversationally with detainees, but instead listen passively with no speaking required—an entirely different skill set than the listening employed while conversing. The listening requirement for HUMINT collectors is adequately met through TSOPI, which assesses both speaking *and* listening skills.

One day, technology will likely overtake the need for specialized foreign language training—but until then, trained HUMINT collectors are the solution. Downgrading the reading and listening requirements to the 0+ level (or eliminating them) while upgrading the speaking proficiency requirement to a Level 2+ (and/or implementing the TSOPI as Army Special Operations Forces currently use it) will result in more capable collectors.

Career Development. The 35M MOS offers Soldiers numerous opportunities to attend advanced courses that develop the practitioner into a more well-rounded collector. Within the career field, the focus should be on a progressive journeyman-to-master model. To produce a 35M force capable of leading HUMINT operations, U.S. Army Forces Command's annual training guidance should include the following requirements:

- **Defense Strategic Debriefing Course.** HUMINT collectors practice skills and gain experience in debriefing. HUMINT collection teams (HCTs) should have a minimum of one course-trained and certified debriefer.

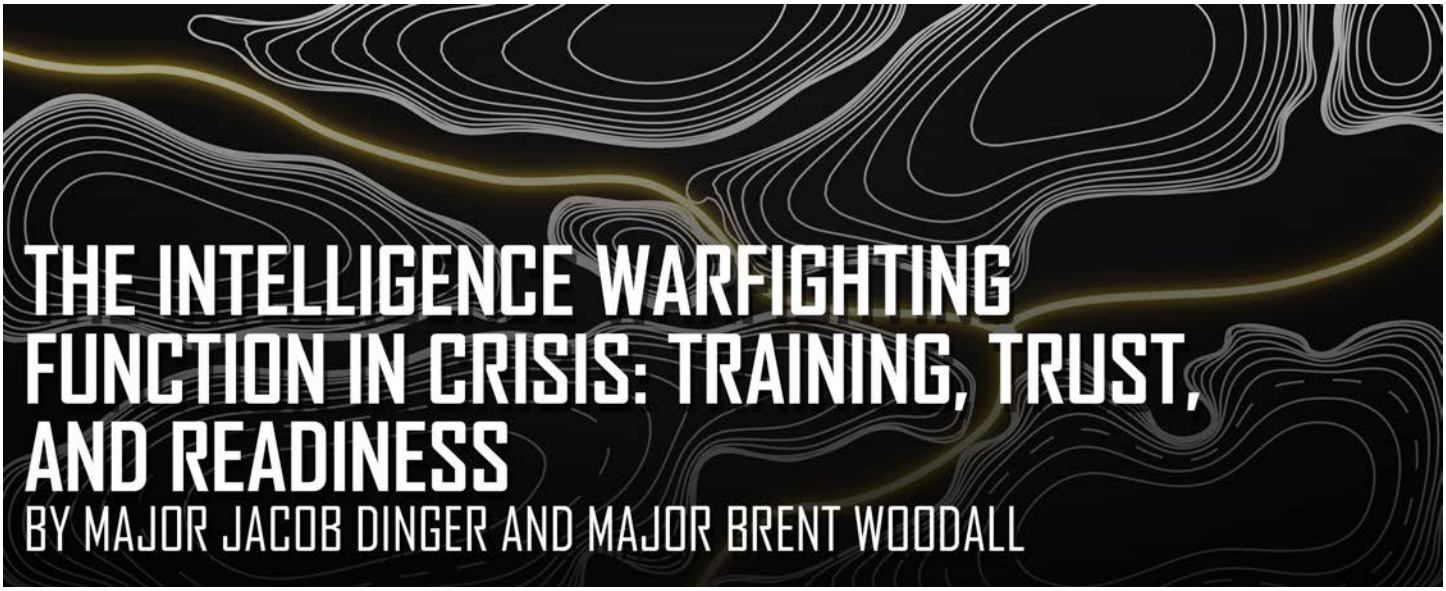
- **Advanced Operations Course-HUMINT.** Equips HUMINT leaders with skills to plan, integrate, and manage operations supporting commanders' decision making. This course teaches members of the HUMINT community how to lead and perform at the junior noncommissioned officer level in a deployed environment.
- **Joint Counterintelligence and HUMINT Analysis and Targeting Course.** Teaches how to leverage analytical processes to support targeting at the tactical, operational, and strategic levels. This course, along with the Advanced Operations Course, is ideal for HUMINT collectors at senior specialist or sergeant levels.
- **Joint Senior Interrogator Course.** A "train-the-trainer" course that increases the operational effectiveness of interrogation capabilities and enables students to transfer knowledge to their home station. The target audience is HUMINT collectors at the staff sergeant level. Every HCT should include at least one graduate to oversee interrogation operations.

Each of these courses enhances the versatility of Army HUMINT collectors and increases the ability of HCTs' to support maneuver commanders in developing a comprehensive picture of the operational environment.

Conclusion

The 35M MOS is at a crossroads. Recent updates from the critical task site selection board have created a unique opportunity for the MOS to shift from a generalist model to one of specialization and focused excellence. By utilizing technological advances, HUMINT collectors can become a force multiplier to consequential missions across the Army intelligence enterprise. Implementing the outlined recommendations, in addition to addressing retention concerns, will result in more common and effective use of HUMINT collectors. Better trained, more focused HUMINT collectors offer commanders greater flexibility in operations with fewer resources. By refining assignment processes, career development models, and mission focus, the Army can create a sustainable and competent force of HUMINT professionals who, in turn, become masters in their field and significantly contribute to HUMINT operations within the intelligence community and the Department of Defense.

SSG Joshua Badger currently serves in the S-3 of the Headquarters and Headquarters Company, U.S. Army Intelligence Center of Excellence, Ft. Huachuca, AZ. His previous assignments include service with the 504th Expeditionary Military Intelligence Brigade, Special Operations Command Central, and U.S. Army Special Operations Command. SSG Badger has deployed to Afghanistan and Qatar, conducting tactical human intelligence (HUMINT) operations, organizational level debriefings, and serving as the Theater Special Operations Command J-2X Forward noncommissioned officer in charge. SSG Badger has also completed multiple HUMINT Training-Joint Center of Excellence courses.



THE INTELLIGENCE WARFIGHTING FUNCTION IN CRISIS: TRAINING, TRUST, AND READINESS

BY MAJOR JACOB DINGER AND MAJOR BRENT WOODALL

A Call to Action

The dry Mojave wind clawed at Brent's face as he stepped away from the chaotic scene at the tactical operations center. It was only day six at the National Training Center (NTC), and the Stryker brigade combat team was coming apart. Brent, a seasoned observer coach/trainer, had seen bad rotations before, but this was different. This wasn't just friction in a complex training environment. This was a collapse. He ducked behind a HMMWV, pulled out his phone, and dialed a familiar number.

Miles away in the southern Arizona desert, a phone rang inside the instructors' bullpen office at the Military Intelligence Captains Career Course. Jake, who had taught most of the junior intelligence officers in this rotation, answered the call. Brent didn't waste time. He recounted what he'd just seen: intelligence sections completely out of synch with brigade operations, no coherent enemy picture, collection plans that ignored priority intelligence requirements, and commanders making decisions in an information vacuum.

"They knew the enemy was maneuvering," Brent said, voice tight. "They had the right tools, but they were improvising intelligence processes mid-fight, like they were learning their jobs in contact."

Jake was quiet for a moment. Then: "That's not a training gap we can solve with doctrine. If commanders aren't listening and S-2s can't command influence with their analysis, we've moved beyond technical failure. That's a trust issue. A failure to prove intelligence relevance at the point of decision."

Brent nodded without speaking as Jake's words settled in. The implications were obvious. Without deliberate, structured training and rehearsals of the basic warfighting functions before deployment, intelligence sections were being asked to perform in combat what they'd never actually practiced outside of a classroom.

As Brent gazed out over the all-too-familiar scattering of blinking lights in the NTC desert, he knew the upcoming after action review wasn't just about products or collection plans. It was a call to action: for junior intelligence officers to own their warfighting function, for commanders to reinvest in their S-2s, and for senior leaders to mentor and enforce standards that prevent collapse before contact—because in the next war, there won't be a phone call. There won't be a reset. There will only be the first fight, whether we are ready for it or not, and those blinking lights may be burning Strykers.

The Intelligence Readiness Gap

This vignette highlights a gap between the foundational instruction provided in professional military education and the continuous application and reinforcement required for operational intelligence execution. While professional military education effectively establishes a strong and necessary doctrinal foundation, sustained proficiency requires deliberate training at echelon. Learning loss resulting from doctrinal fundamentals not being reinforced, compounded by force structure changes, poor communication, and insufficient collective training, undermines the operational effectiveness of battalion and brigade intelligence officers.

This capability gap has profound operational consequences. Intelligence officers unable to effectively integrate with command decision-making processes hinder operational agility, contribute to missed opportunities in shaping the battlefield, and erode the foundational trust necessary for intelligence to inform maneuver at echelon. To bridge this gap, S-2s must assert proactive ownership over their professional development, improve communication with their field-grade officers, and receive sustained mentorship and oversight from senior intelligence leaders.[1]

Perishable Skills and Structural Challenges

Doctrinal instruction provides officers with the foundational knowledge needed to execute the intelligence warfighting function tasks, but without sustained and deliberate training, proficiency erodes rapidly. Intelligence fundamentals are a perishable skill set, requiring iterative reinforcement to maintain operational effectiveness. However, as operational deployments have decreased, administrative and security-related responsibilities increasingly consume intelligence sections, diverting focus from core analytic and collection tasks.

Routine garrison requirements such as security programs, arms room oversight, and personnel management often dominate intelligence officers' time, reducing opportunities for

collective training and practical application. While intelligence doctrine assigns these responsibilities, they must not come at the expense of the intelligence section's primary mission of enabling commanders to understand and shape the operational environment through timely, accurate intelligence.[2]

Compounding this issue, changes in force structure further challenge the sustainment of intelligence proficiency.[3] The restructuring of intelligence and electronic warfare battalions at the division level has reduced opportunities for collective intelligence training and integration at the brigade and below levels without additional coordination. Previously, the Military Intelligence Training Strategy enabled cross-training between brigade and battalion intelligence sections, fostering a baseline of competency across formations. Without the support of dedicated intelligence units, battalion S-2 sections must now self-sustain their training efforts but often lack the resources, expertise, or prioritization necessary to do so effectively.

"Intelligence fundamentals are a perishable skill set, requiring iterative reinforcement to maintain operational effectiveness."

Without intervention, these structural and doctrinal gaps will continue to degrade the ability of intelligence officers to deliver timely, relevant intelligence to their commanders, ultimately reducing the Army's capacity for effective decision making at echelon.[4]

Intelligence Training Misalignment and Proactive Solutions

A fundamental misalignment exists between intelligence training and unit-level exercises. A pervasive misconception suggests that brigade- and battalion-level training events should serve as opportunities for intelligence sections to refine their individual skills. However, these exercises are not designed for intelligence-specific skills development but are instead for intelligence integration into collective training objectives.[5] Intelligence sections are meant to serve as enablers, providing commanders with the necessary intelligence to drive maneuver decision making.

Due, in part, to this misalignment, intelligence officers often enter major training exercises underprepared, attempting to refine their fundamental analytical, collection, and dissemination skills while simultaneously supporting the broader mission.[6] This reactive approach leads to suboptimal intelligence outputs, diminishing the commander's trust in the S-2 section's ability to provide timely, relevant, and actionable intelligence.

To correct this deficiency, intelligence officers must secure dedicated training opportunities outside of large-scale unit exercises to develop their technical competencies in a controlled environment.[7] Before integrating into unit training, S-2 sections must conduct iterative internal training that focuses on intelligence-specific tasks, such as intelligence preparation of the operational environment (IPOE), intelligence estimate production, targeting synchronization, and collection management.[8] This requires proactive engagement with command leadership to advocate for the time, resources, and prioritization necessary to sustain intelligence readiness.

Without deliberate pre-exercise preparation, intelligence sections will continue to struggle with both technical proficiency and operational credibility.[9] Intelligence officers must take the initiative to align their section's training with both doctrinal requirements and unit objectives, ensuring that intelligence remains a force multiplier rather than an afterthought in operational planning and execution.

Developing and Sustaining Tactical Intelligence Proficiency

Intelligence officers must take immediate ownership of their section's training and development upon arrival at their unit. The priority is a comprehensive assessment of the section's competency in executing its core warfighting function tasks, as outlined in Field Manual 2-0, *Intelligence*. These tasks are: support to force generation, support to situational understanding (specifically IPOE), intelligence support to targeting, and information collection.[10] Beyond doctrinal understanding, the intelligence section must demonstrate its ability to characterize the operational environment to commanders effectively, anticipating their information requirements and providing them with the situational awareness necessary for decision superiority.

To sustain readiness, intelligence officers must integrate intelligence-specific training into broader unit training objectives, ensuring that the section can support operational planning rather than functioning in isolation. This requires a progressive, structured training plan that starts with building fundamental skills, such as IPOE, threat tactics, and targeting integration, and continues with advanced application in live training environments.

Recognizing that external intelligence support elements like the military intelligence company are no longer available,

Military Intelligence Captains Career Course Class 25-003 students conduct an information collection rehearsal for their instructor at Fort Huachuca, AZ. (U.S. Army photo by CPT Joel Hammond)

battalion S-2s must take proactive measures to cultivate self-sustaining intelligence training. This includes leveraging reachback resources, such as doctrinal templates, intelligence estimate shells, and case study analyses, to ensure standardization and professional development. Over the past few years, the Military Intelligence Captains Career Course has refined its curriculum to ensure it remains accessible beyond graduation. This enables battalion S-2s to leverage prebuilt training materials, standardized rubrics, and doctrinal templates to assess and develop their personnel without the need to create operation orders and annexes from scratch. These resources facilitate continuity in training and enhance the ability of intelligence officers to sustain operational readiness at the battalion level.

Strengthening the Communication Link Between S-2s and Commanders

Success in intelligence operations links directly to how well intelligence officers communicate training priorities to leadership. Subordinates will always focus on what their leaders emphasize, making it critical for field-grade officers, especially battalion executive officers and commanders, to prioritize intelligence training explicitly. Without clear prioritization, competing demands will inevitably overshadow intelligence development, leaving S-2 sections underprepared to support operations.

Prioritization alone is insufficient. Battalion S-2s must take an active role in engaging their executive officers and commanders to ensure understanding, resourcing, and execution of training requirements. Without deliberate communication, intelligence training risks being underfunded, deprioritized, or ignored altogether. Headquarters and headquarters company commanders often struggle to articulate the staff's training efforts to higher headquarters while protecting allocated training time from competing demands. Frequently, the intelligence section is a target for additional duties when it does not effectively communicate its training priorities. New S-2s should proactively build a relationship with their headquarters and headquarters company commander, using the commander's experience to navigate the training calendar for securing dedicated time for intelligence development. This level of coordination alone places the S-2 ahead of most staff officers in their battalion.

To drive effective training integration, intelligence officers must link their section's training plan to the unit's mission-essential tasks and operational objectives.[11] This alignment ensures that intelligence efforts directly support the commander's ability to make informed decisions. Commanders, in turn, must clearly articulate their expectations for intelligence proficiency, ensuring that S-2 sections are focusing on warfighting readiness rather than administrative or non-mission-essential tasks.

Proactive dialogue with commanders and executive officers is essential. Intelligence officers must not hesitate to advocate for the necessary training time, resources, and doctrinal alignment necessary for success. Well-prepared intelligence sections are force multipliers; ensuring their readiness is not just the responsibility of the S-2, but of the unit's entire leadership.

Maximizing Mentorship and Counseling for Intelligence Leaders

The brigade combat team S-2 is not a battalion intelligence officer's direct supervisor, but they are an invaluable resource for professional development and training advocacy. Intelligence officers should actively engage with their brigade S-2 early in their tenure, leveraging the brigade S-2's expertise, network, and influence to secure training resources and refine intelligence warfighting function priorities. Brigade S-2s play a crucial role in ensuring the intelligence warfighting function effectively integrates across the formation. They must proactively communicate to their fellow field-grade officers the value of intelligence at echelon, ensuring its value is understood and leveraged appropriately. Competence, reliability, and demonstrated operational relevance build credibility with the staff—having an advocate who can vouch for the intelligence section's contribution is essential to ensuring its place in decision making.

A battalion S-2 should approach their initial counseling with their commander prepared to discuss intelligence priorities, training gaps, and expectations for support. This ensures a shared understanding of how intelligence integrates into the unit's mission and sets the conditions for success. This discussion should define commander expectations, intelligence priorities, and acceptable risk levels. Intelligence officers must communicate their capabilities and shortfalls early to ensure alignment with mission needs.

Failing to establish the intelligence warfighting function's credibility early will result in the sidelining of the intelligence section and relegating them to administrative tasks rather than shaping operational decisions. S-2s must emphasize their role in threat analysis and warfighting tasks. If the S-2 does not assert their value, they will quickly find themselves relegated to arms room inspections and weather slides. This is the moment to reinforce that intelligence is a critical enabler, not an afterthought. This is *your* job; do not assume your predecessor established this credibility for you. Even if they did, you owe your commander proof that you can ensure the intelligence section remains relevant and indispensable.

Effective mentorship is critical for navigating the complexities of the military intelligence officer corps. Officers without a mentor should proactively seek one, either within their brigade or through structured programs like the Define and Design Your Success Mentorship Program at Fort Huachuca.[12] This underutilized program offers valuable frameworks for professional growth and intelligence leadership development. Whether you are branch detailed or pure military intelligence, at the tactical level or with the Intelligence and Security Command (operational intelligence), or a combination of these, others have navigated and excelled in the same challenges you now face. If there is one underutilized asset in the intelligence profession, it is mentorship. A trusted mentor will help you navigate the complexities of your role, offering insights that extend beyond the broad recommendations provided here. The challenges may not be as simple or as complex as they seem, but the right guidance can make them manageable.

Successful intelligence officers take ownership of their development by seeking mentorship, asking informed questions, and leveraging the experience of seasoned professionals. Regular engagement with field-grade officers and more experienced peers is essential to ensuring readiness for combat operations and aligning intelligence efforts with commander expectations.

Closing Thoughts: Winning the First Fight

In his 2024 article for the Modern War Institute, Major General Curt Taylor, Commanding General of 1st Armored Division and Fort Bliss and former Commanding General of the National Training Center and Fort Irwin, noted, "The National Training Center's mandate since our founding forty-two years ago is to prepare the Army's combined arms formations to win the first battle of the next war."[13] These words encapsulate the enduring necessity of readiness—ensuring that from day one, intelligence professionals are not just present but pivotal in the fight. Intelligence officers must take ownership of their training, build credibility with their commanders, and integrate seamlessly into operational planning.

History has shown that the first fight is often the most consequential, and those who fail to adapt early pay the highest price. Intelligence sections that are unprepared, disjointed, or sidelined will not have time to recover in combat. Success is determined long before the first round is fired, through training, mentorship, and proactive engagement with commanders.

The Army cannot afford for its intelligence warfighting function to be an afterthought. The responsibility lies with every intelligence officer to ensure that when the next war comes, the commander is making decisions based on accurate, timely intelligence because in the first fight, there are no second chances.

Endnotes

1. Elizabeth K. Schloemann, "Keeping Army Intelligence Training Relevant in a Rapidly Evolving World," (master's thesis, United States Marine Corps University, 2023), https://apps.dtic.mil/sti/trecms/pdf/AD1178193.pdf.

2. Department of the Army, Field Manual (FM) 3-0, *Operations* (Government Publishing Office [GPO], 2025), 26.

3 Department of the Army, Office of the Deputy Chief of Staff, Force Management, *Army Structure (ARSTRUC) Memorandum 2025-2029* (Department of the Army, 2024).

4. Cortis B. Burgess, "News from the CTC: Intelligence After Action Review Trends at the National Training Center," Center for Army Lessons Learned, October 21, 2020, https://cgsc.contentdm.oclc.org/digital/collection/p15040coll4/id/214/rec/1.

5. Schloemann, "Keeping Army Intelligence Training Relevant," 38.

6. Burgess, "Intelligence After Action Review Trends."

7. Ibid.

8. Schloemann, "Keeping Army Intelligence Training Relevant."

9. Burgess, "Intelligence After Action Review Trends."

10. Department of the Army, FM 2-0, *Intelligence* (GPO, 2023), B-1—B-24.

11. Schloemann, "Keeping Army Intelligence Training Relevant."

12. "D2YS Mentorship Program," Units/Tenants, U.S. Army Intelligence Center of Excellence (USAICoE), U.S. Army Fort Huachuca website, last modified May 24, 2024, https://home.army.mil/huachuca/units-tenants/usaicoe/D2YS-mentorship.

13. Curt Taylor, "Preparing to Win the First Fight of the Next War," Modern War Institute at West Point, February 23, 2024, https://mwi.westpoint.edu/preparing-to-win-the-first-fight-of-the-next-war/.

MAJ Jacob Dinger is currently a student at the School of Advanced Military Studies. He previously served as an instructor at the Military Intelligence Captains Career Course and has held leadership roles as a company commander and battalion S-2 for the 296th Brigade Support Battalion, 1-2 Stryker Brigade Combat Team, 7th Infantry Division at Joint Base Lewis-McChord, WA. Commissioned as an infantry officer through the University of Southern Mississippi, he later transitioned to military intelligence. His operational experience includes a deployment to Iraq in support of Operation Inherent Resolve as a weapons platoon leader. His military education includes the Infantry Officer Basic Course, the Military Intelligence Captains Career Course, and the Command and General Staff College.

MAJ Brent Woodall is currently assigned to 3rd Infantry Division, G-2 Operations. He previously served as an observer coach/trainer at the National Training Center, Fort Irwin, CA, and as a battalion S-2 in the 725th Brigade Support Battalion and 1st Battalion, 501st Infantry Regiment (Airborne) at Joint Base Elmendorf-Richardson, AK. He commissioned as a military intelligence officer through Texas A&M University, and his operational experience includes a deployment to Iraq in support of Operation Inherent Resolve as a battalion assistant S-2 and military intelligence company executive officer. He holds a juris doctor from South Texas College of Law. His military education includes the Military Intelligence Basic Officer Leader Course, the Military Intelligence Captains Career Course, and the Command and General Staff College.

An M109A2 Paladin crew assigned to 1st Battalion, 5th Artillery Regiment, 1st Armored Brigade Combat Team, 1st Infantry Division cleans the gun's tube following a Table XVIII live fire event in Torun, Poland, April 2019. (Photo by MAJ Christopher Collins)

THE BRIGADE COMBAT TEAM S-2: KEY CONSIDERATIONS FOR SUCCESS

BY LIEUTENANT COLONEL CHRISTOPHER M. COLLINS

Introduction

I initially drafted this article in 2019 while serving in Poland with the 1st Armored Brigade Combat Team (ABCT), 1st Infantry Division. At that time, a good friend was transitioning to a brigade combat team (BCT) S-2 position and asked me to share any insights and best practices from my experience as an S-2. I shared with him observations that focused on four critical areas for a BCT S-2:

- ✦ Intelligence systems, personnel, and architecture.
- ✦ Intelligence and fires warfighting functions integration.
- ✦ Information collection and the cavalry squadron.
- ✦ Role as a coach, teacher, and mentor.

Intelligence Systems, Personnel, and Architecture

Serving in a BCT provides a unique experience for military intelligence (MI) officers due to the complexity of the equipment used, the military occupational specialty (MOS) diversity, and the communication architecture. In 2018 and 2019, 1st ABCT was equipped with Portable Multifunction Workstations, Geospatial Intelligence Workstations, Intelligence Fusion Servers, the Tactical Intelligence Ground Station, the Intelligence Processing Center, the Prophet System, and the Trojan System. It was manned by human intelligence, signals intelligence (SIGINT), geospatial intelligence, all-source intelligence, and intelligence systems integration and maintenance warrant officers, noncommissioned officers, and Soldiers. Each of these disciplines has its own training challenges, and they each have critical missions to accomplish. For me, the challenge early on was understanding unfamiliar systems that were unique to 1st ABCT.

The first of these systems was the Intelligence Fusion Server, which was fielded in a stand-alone version but also functions as a component of the Intelligence Processing Center.[1] The Intelligence Fusion Server connects laptop-style Portable Multifunction Workstations to a secure network and provides analysts with tools to conduct processing, exploitation, and dissemination of intelligence information.[2] One challenge for the BCT is ensuring that the Intelligence Fusion Server can function properly by connecting to a higher echelon's server and communicating with the BCT's workstations. Having an aggressive and innovative team of MOS 35T (MI systems maintainer/integrator) noncommissioned officers and Soldiers helps ensure the Intelligence Fusion Server is working as designed for the BCT. Additionally, field service representatives are available to assist with troubleshooting the system.

The second system I was unfamiliar with was the Prophet system. The 1st ABCT had three Prophet systems mounted on mine-resistant ambush protected all-terrain vehicles. The Prophet is a ground-based tactical SIGINT and electromagnetic support sensor system.[3] Crewmembers who operate the sensor are SIGINT voice interceptors and SIGINT analysts. Our unit's SIGINT analysis technician helped me with navigating the complexities of the brigade's SIGINT mission and equipment. This warrant officer provided the expertise and leadership needed to train our Soldiers during National Training Center (NTC) rotation 18-10, and he also enabled the brigade to complete a critical equipment readiness test while supporting Operation Atlantic Resolve.

One of the communication networks the BCT S-2 uses to receive and distribute information is the Mission Command Network, which consists of two components: the upper tactical internet (upper TI) and the lower tactical internet (lower TI).

I was familiar with Command Post of the Future and Force XXI Battle Command Brigade and Below from earlier assignments, but at 1st ABCT, the terms upper TI and lower TI were used extensively. The use of lower TI systems, such as the Joint Battle Command Platform and high-frequency radios, was very effective and became the primary communication method due to their low bandwidth capability.[4] Ultimately, the S-2 receives, analyzes, and disseminates information to enable the destruction of the enemy; therefore, they must be familiar with both components of the Army's mission command network.

Intelligence and Fires Integration

A second lesson learned for me was the important relationship between the intelligence and fires warfighting functions. Specifically, I learned three things that an S-2 must do to facilitate the targeting process:

- ✦ Know and understand the enemy's capabilities.
- ✦ Determine how the enemy will employ those capabilities in a fight.
- ✦ Conduct information collection to locate and later confirm that fires has destroyed the enemy's capabilities during conflict.

These actions are a standard part of intelligence preparation of the operational environment, but they require more analysis and integration with fires to enable the targeting process.

Any new BCT S-2 must study and understand their adversaries. This requires extensive observation of their equipment, doctrine, and tactics. I discerned quickly that the opposing force (OPFOR) 1st ABCT faced during NTC rotation 18-10 was much different from what I had encountered in my 2007 NTC rotation. This OPFOR fought in formations like the Division Tactical Group and Brigade Tactical Group. They utilized systems such as the 1L220 Zoopark-2 counter-artillery radar system and the 2S19 Msta-S 152mm self-propelled howitzer, and employed either an integrated attack or a dispersed attack.[5] Existing understanding of the systems and tactics used by the OPFOR can be lost after years of serving in a broadening assignment, so one must prepare and study well in advance of subsequent training rotations.

A comprehensive understanding of the enemy's capabilities includes knowing the maximum range of their weapon systems. For example, the OPFOR's indirect fire system, the 2S19, has a maximum range of 29 kilometers;[6] a crucial fact to know when assessing where the enemy is likely to position their howitzer batteries on the battlefield. Answering how the enemy fights will help determine what weapon systems are likely to be present during the counter-reconnaissance phase of an operation and in the exploitation force. Information collection will aid in confirming or denying the initial analysis of the enemy's course of action.

Information Collection with the Cavalry Squadron

The 1st ABCT commander emphasized the importance of using the 1st Squadron, 4th Cavalry Regiment as the primary platform for information collection during large-scale combat operations. The 1st Squadron, 4th Cavalry Regiment is an all-weather sensor unit whose mission is to conduct reconnaissance and security operations in support of the brigade. The unit has three troops and one tank company in its task organization. The troops are equipped with organic optic capabilities that allow them to see up to 8 kilometers from their positions when conducting a screen in unrestricted terrain (see figure). The BCT S-2 section, however, relied more on overhead sensors to meet information collection requirements, rather than using the cavalry squadron, which we endeavored to remedy through brigade-to-battalion staff training.

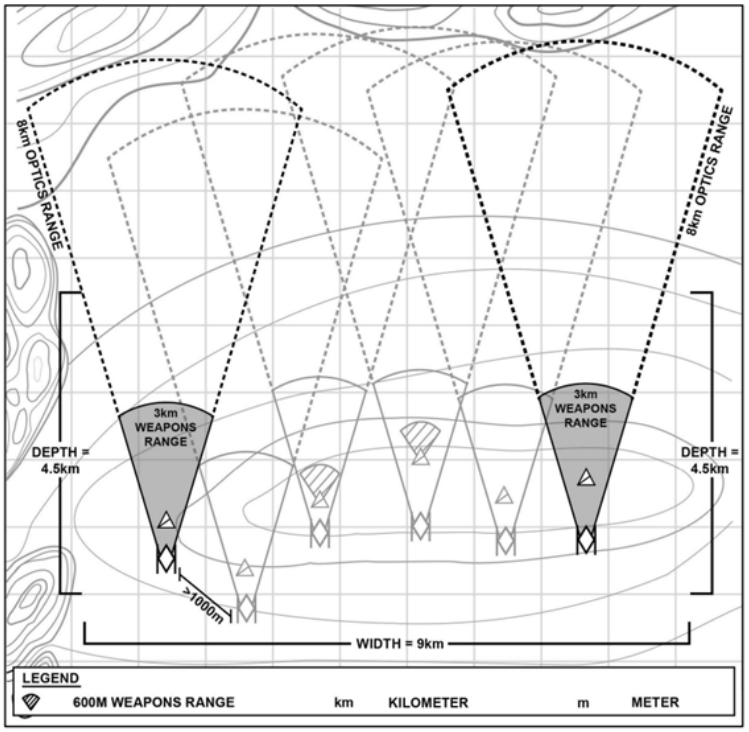


Figure. Armored brigade combat team scout platoon in unrestrictive terrain[7]

The leaders of the 1st Squadron, 4th Cavalry Regiment were receptive to conducting training to increase awareness of the brigade's organic collection capabilities. During a brigade-to-battalion staff training event, the executive officer provided a capability briefing to several intelligence professionals covering the squadron's mission, equipment, and task organization as well as lessons learned from NTC rotation 18-10. Other intelligence professionals provided capability briefs to the operations officer and other staff officers on the Prophet and Shadow systems, human intelligence, and geospatial intelligence. This training event was a first step toward improving information collection processes between the cavalry squadron and members of the brigade staff and MI company.

The S-2 and S-3 for the 2nd Squadron, 278th Armored Cavalry Regiment (Tennessee Army National Guard) conducts a wargame in preparation for a combined arms live fire exercise at Bemowo Piskie Training Area, Poland, March 2019. (Photo by MAJ Christopher Collins)

Coach, Teacher, and Mentor

The fourth and final lesson learned relates to the BCT S-2's role as a coach, teacher, and mentor. I had several opportunities to experience this, the first being when 1st ABCT provided observer controller/trainer support to the 2nd Squadron, 278th Armored Cavalry Regiment's combined arms live fire exercise at Bemowo Piskie Training Area, Poland. This opportunity allowed me to work directly with a subordinate S-2 section and apply lessons learned from my experience as a battalion and brigade S-2. The undertaking was extremely rewarding, and I learned a lot in the process.

Later, I had the opportunity to work with "Hamilton's Own," 1st Battalion, 5th Field Artillery Regiment, 1st Infantry Division Artillery during their Table XVIII live fire event in Torun, Poland. This experience allowed me to observe how the battalion maneuvered their M109A2 Paladin 155mm turreted self-propelled howitzers during live fire, and it helped me understand the challenges faced by their S-2 section. At that time, I was augmenting the 1st Infantry Division Artillery, which had training and oversight responsibility over the division's field artillery battalions. This was a learning point for me as well, and it was gratifying to learn from the division's artillery commander and his staff during the live fire exercise.

The 1st ABCT Best Intelligence Team competition at Zagan, Poland, presented a third opportunity to coach, teach, and mentor. This event, named Operation Rescorla in honor of the late, retired Colonel Rick Rescorla, brought together 65 officers, warrant officers, noncommissioned officers, and Soldiers from across the BCT. It included MI, aviation, engineering, and fires personnel. The competition consisted of a land navigation course, a round-robin event for weapon disassembly and assembly, first aid, a knowledge test, radio operation, a physical challenge, and vehicle maintenance. The final event was a graded intelligence brief during which each team had two hours to analyze a scenario. This event recognized the best intelligence team of the day, and it improved intelligence teamwork across the BCT.

For recent graduates of Command and General Staff College or MI officers leaving a broadening assignment, these lessons learned will help prepare you to serve as a BCT S-2. Understanding the MI systems, personnel, and architecture will help you speak the correct language. Integrating with fires personnel and using organic capabilities will help you focus on how to find and kill the enemy. Embracing your role as a coach, teacher, and mentor will enable you to develop others and advance your professional career. Seek those opportunities whenever possible. The BCT S-2 role is challenging, yet rewarding, and it will provide valuable insights into your development as an MI leader.

Endnotes

1. U.S. Army Intelligence Center of Excellence (USAICoE), Military Intelligence Publication (MI Pub) 2-01.2, *Establishing the Intelligence Architecture* (USAICoE, 2014), 1-4. The Distributed Common Ground Station-Army intelligence fusion server enables intelligence staff to manage and replicate multidisciplinary intelligence databases. It includes a suite of core applications for analyzing and storing intelligence, as well as disseminating intelligence products to all echelons.

2. Department of the Army, Training Circular (TC) 2-19.403, *Military Intelligence Training Strategy for the Brigade Combat Team Tier 3* (Government Publishing Office [GPO], 2020), 1-7.

3. "Tactical Spectrum Warfare: Prophet Enhanced," PM Electronic Warfare & Cyber, Program Executive Office Intelligence, Electronic Warfare & Sensors, last modified August 7, 2025, https://peoiews.army.mil/pm-ewc/.

MAJ Christpoher Collins awards the Army Achievement Medal to a geospatial intellignece imagery analyst on the team winning the Best Intelligence Team competition in Zagan, Poland, June 2019. (U.S. Army photo)

Soldiers from the S-2 for the 1st Battalion, 5th Field Artillery Regiment, 1st Armored Brigade Combat Team, 1st Infantry Division pack their equipment at the conclusion of the Table XVIII live fire event in Torun, Poland, April 2019. (Photo by MAJ Christopher Collins)

4. USAICoE, MI Pub 2-01.2, *Establishing the Intelligence Architecture*, B-3. Lower tactical internet has a low bandwidth capability that supports limited data exchange.

5. Department of the Army, TC 7-100.2, *Opposing Force Tactics* (GPO, 2011), 3-10.

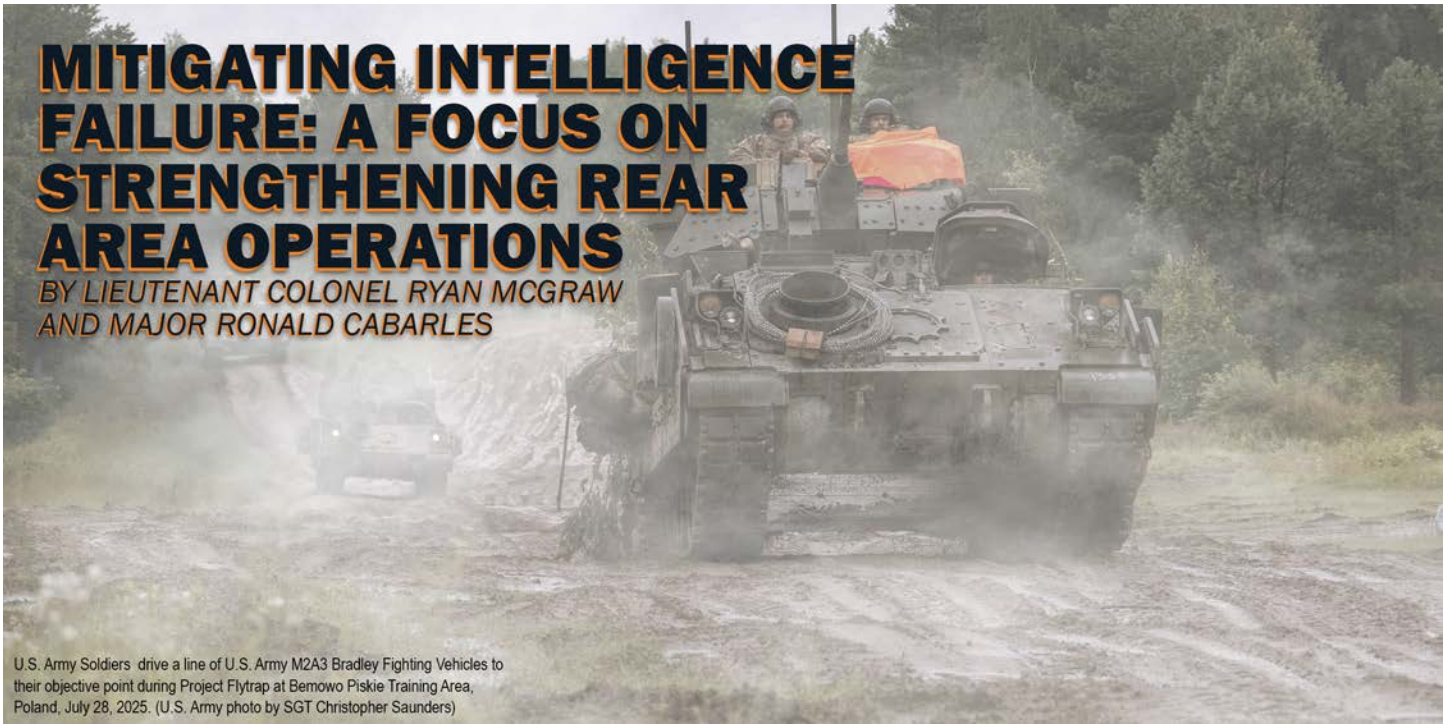
6. Neil Ritchie, "Russian Ground Forces Receive Upgraded 2S19M1 Msta Howitzers," Land Platforms, Defence Today, August 31, 2022, https://www.defencetoday.com/land/land-platforms/russian-ground-forces-receive-upgraded-2s19m1-msta-howitzers/.

7. Figure A-1, Department of the Army, Army Technical Publication 3-20.97, *Cavalry Troop* (GPO, 2024), 112.

LTC Christopher Collins is an assistant professor at the Command and General Staff College, Fort Leavenworth, KS. He previously served as the commander of the Kansas City Recruiting Battalion and has deployed to Iraq, Afghanistan, Japan, and Poland. He has served as an engineer brigade S-2 and an armored brigade combat team S-2. His broadening assignment was with the 138th Military Intelligence Company at Robins Air Force Base, GA, where he served as an Army crew member on the Joint Surveillance Target Attack Radar System. LTC Collins has a master of science of strategic intelligence degree from the National Intelligence University and is a graduate of the Command and General Staff College.

MITIGATING INTELLIGENCE FAILURE: A FOCUS ON STRENGTHENING REAR AREA OPERATIONS

BY LIEUTENANT COLONEL RYAN MCGRAW AND MAJOR RONALD CABARLES



U.S. Army Soldiers drive a line of U.S. Army M2A3 Bradley Fighting Vehicles to their objective point during Project Flytrap at Bemowo Piskie Training Area, Poland, July 28, 2025. (U.S. Army photo by SGT Christopher Saunders)

Introduction

Intelligence failure haunts every zone of the battlefield. When intelligence failure occurs, targets evade destruction; decision points fade into the shadows of ambiguity; and enemy forces scheme, maneuver, and kill in the darkness. Every intelligence officer recognizes the potentially dire consequences of intelligence failure and aggressively seeks to prevent it. Institutionally, the Army recognized the risks associated with intelligence failure and arrayed its intelligence doctrine, training, and organizations in a manner to avoid or reduce the possibility of failure. The processes and procedures for units conducting intelligence operations in the rear area must, therefore, be congruent with the magnitude of intelligence failure in this critical battle zone area.

Even in ideal conditions, the sustainment framework can be extremely fragile. For example, sea states, port facility issues, or any of several other circumstantial events can easily disrupt archipelagic sustainment, even absent an enemy threat. Factor in an aggressive and determined enemy—perhaps one that has prioritized sustainment disruption as a key targeting objective—and the conditions for intelligence failure are well established. When intelligence failure occurs in the rear area, it is most likely to affect the sustainment framework or targets associated with fires and aviation, which are often the primary means of engagement employed by a corps-level formation. Thus, intelligence failure in the rear area can prevent sustainment, hamper fires, or remove aviation assets from a commander's employable toolset. The standard intelligence processes I Corps previously followed were insufficient to address the significance of potential consequences should intelligence fail in the rear area.

The Problem

From late 2023 through December 2024, I Corps conducted its train-up to Warfighter 25-02. During pre-execution exercises, the G-2 emphasized improving intelligence support to the rear area, with particular emphasis on—

- Finding corps-level intelligence process efficiencies.
- Unifying commanders' understanding.
- Adjusting the burden placed on small intelligence sections.
- Increasing rear area representation in the targeting process.

Corps-level intelligence process efficiencies. I Corps had numerous units operating independently in the rear area, which impacted the intelligence battle rhythm and processes. Organically, I Corps has an expeditionary sustainment command, an engineer brigade, a fires brigade, a combat aviation brigade, a signal brigade, a military police brigade, and a military intelligence brigade. These units all operate or are headquartered in the corps rear area. The corps operational framework calls for a reserve brigade combat team, plus at least one maneuver enhancement brigade with additional battalion- and brigade-level attachments, to operate in the rear area.

Given that multiple brigade-level intelligence sections operated independently, it was common and completely understandable for multiple unique assessments of the rear area to propagate through several different battle rhythm events. Because each of those briefs increased the intelligence synchronization time significantly, and because time was our most valued resource, I Corps G-2 must gain something more than a redundant assessment.

This overlap in rear area intelligence also led to a potentially overwhelming number of unique collection requests for every air tasking order cycle, placing a significant burden on the I Corps collection management team. These were often redundant, but due diligence still required the collection management team to adjudicate each request. This unnecessarily burdened an already small section with additional work.

Commanders' understanding. Similarly, if there are multiple brigade commanders in the rear area with each unit's intelligence officers and sections operating relatively independently, there will likely be multiple interpretations of the rear area enemy situation. There are battle rhythm events that synchronize rear area operations, but these are exponentially more effective if the participating commanders arrive with the same understanding of the enemy situation. Without unity of understanding, the likelihood of disunity in effort and operations is high or at least higher than it should be.

Small intelligence sections' workload. Though small, brigade-level sections still have minimum doctrinal requirements:

- ✦ Commander's situational awareness: Advise the functional command commander on the larger battlefield.
- ✦ Support to force protection: Provide information and intelligence on emerging threats to the mission and threats to the force.

I Corps included functional analysis as a standard task for its subordinate commands and separate brigades. Organically, the Corps G-2 is composed entirely of intelligence Soldiers lacking the inherent knowledge possessed by these subordinate units. For example, the combat engineer brigade is best positioned to identify the threat's critical capabilities and vulnerabilities and conduct intelligence preparation of the battlefield during counter-mobility operations. The functional brigades' S-2s and subordinate commands' G-2s can leverage those experts to augment their analysis of the opposing force. Functional analysis briefs extraordinarily well and pays dividends; however, functional analysis will not inherently be a priority as each rear area formation rightfully prioritizes the commander's situational awareness and its force protection.

Rear area representation in the targeting process. Like functional analysis, there is a burgeoning potential for rear area formations to develop nominations for targeting. These formations experience enemy operations differently than units in the deep and close areas, and they have a unique perspective on which systems are disrupting rear area activities. This insight can and should be represented throughout the targeting process.

Formations must reduce the likelihood of intelligence failure by addressing intelligence synchronization and reducing workload on intelligence sections. Intelligence section leaders should make a significant effort to ensure unity in the understanding of brigade-level commanders. Without commanders' understanding, conditions are ripe for intelligence failure, which leads to operational failure. Operational failure in the rear area has a cascading effect on all operations.

The Solution

Before Warfighter 25-02, the I Corps G-2 appointed a senior intelligence officer to the rear area to reduce the likelihood of intelligence failure. This individual and their team streamlined the rear area tenant unit intelligence activities. I Corps resourced the G-2X (human intelligence and counterintelligence operations cell) to the rear area command post, and liaison officers for the expeditionary-military intelligence brigade were also located in the rear area.

Key to the smooth functioning of this process was buy-in from the tenant rear area brigades as well as their regular participation in the rear area threat and targeting synchronization (RATTS) meeting. The RATTS meeting was designed to feed the I Corps intelligence synchronization working group, sustainment working group, protection working group, and targeting working group. Unfortunately, the timing could not support all those groups. The result was hours of intelligence decay between the RATTS, the sustainment working group, and the protection working group. Open lines of communication were leveraged to mitigate this issue.

Due to an already grueling battle rhythm, the RATTS was very direct and simple. Conducted virtually, the meeting consisted of an overview by the senior intelligence officer, followed by a roundtable in which each unit informally answered the question: What is killing you and how? Answers were fed into the various working groups, sorted by threat awareness (sent to the sustainment working group) and targeting or operations (sent to the targeting and protection working groups). Specific units reported on niche analytic topics such as civilian impacts from the civil affairs unit and enemy targeting trend analysis by the counter-fire artillery brigade.

I Corps first implemented the RATTS process before Warfighter 25-02 during a preparatory command post exercise. The rear area intelligence workload was spread across multiple organizations and focused through the RATTS. One significant challenge was integrating U.S. Army Reserve formations into the process. Reserve scheduling limitations prevented these formations from participating fully in the preparatory command post exercise. In future contingency operations, it should be expected that many rear area units will primarily be reserve formations. Therefore, every effort must be made to develop habitual relationships with supporting reserve formations and include them in training and exercises.

During the exercise, the RATTS was conducted daily, and a Maven Smart System common intelligence picture dedicated to the rear area was produced. It was far from perfect, and we made several key observations for improvement and optimization.

Lack of a formalized rear area targeting and collection discussion. The fires officer, dedicated to the rear area by the Deputy Commanding General-Protection, was marginally isolated from the RATTS. Despite the haggard coordination, the rear area targeteer did produce sound analysis linking enemy systems to rear area disruptions. Residual collection and bonus opportunities covering the rear area were considered when collection was planned. This process worked, but the rear area senior intelligence officer could have certainly added more formality and rigor to reduce the strain on the collection management and dissemination team and the aviation brigade team. In future operations, the I Corps rear area senior intelligence officer will include the fires officer in the RATTS and incorporate targeting recommendations into the I Corps targeting process.

Note: I Corps does not as a standard practice have a Deputy Commanding General-Protection; however, during this warfighter the Corps benefitted from a U.S. Army Reserve brigadier general filling this role.

Task organization of rear area sensors. During the training leading up to Warfighter 25-01, I Corps experimented with task organizing sensors in the rear area. I Corps tested a multitude of relationships, achieving the best results by splitting responsibility between the maneuver enhancement brigade and the expeditionary-military intelligence brigade.

Rear area senior intelligence officer. The I Corps G-2 selected the 593rd Corps Sustainment Command G-2 to be the rear area senior intelligence officer. This was the obvious choice because the rear area brigades have majors as their S-2s, while the corps sustainment command has a lieutenant colonel as its G-2. In retrospect, the officer selected should align more closely with the protection effort and have ready access to the fires and maneuver enterprises. This would also allow the corps sustainment command G-2 to focus more fully on intelligence support to sustainment and functional analysis of enemy forces sustainment.

Full integration of all rear area elements. Initially, some rear area elements were excluded unintentionally, most notably the civil affairs battalion. However, in addition to providing an overview of civil actions affecting operations, they were able to drill down and track specific threat tactics, techniques, and procedures, as well as capabilities of the special purpose forces.

During execution, the G-2's experiment to improve intelligence support to the rear area accomplished its goal. The intelligence process at echelon was optimized for greater unity of understanding and reduced workload on rear area intelligence sections. By the opposing force commander's own admission, the aggressive and synchronized actions of the rear area security elements limited the freedom of movement of his special purpose forces. Doctrinally, the special purpose forces provides intelligence to the opposing force commander along with an option for disruption. By reducing the special purpose forces' freedom of movement, enemy targeting was degraded, as was their ability to affect the I Corps long-range fires, aviation operations, and sustainment activities.

Recommendation

Corps and divisions should seek means to streamline their intelligence processes, and aligning the rear area problem set under a single leader is an effective way to gain efficiencies. The utility of a rear area senior intelligence officer, however, is mainly dependent on how the rear area is addressed: a singular commander fighting the rear area in the same way they fight a division battlespace maximizes the value of the rear area senior intelligence officer. A second significant challenge for headquarters is staffing a rear area intelligence section. Optimally, using a lieutenant colonel without an already assigned senior intelligence officer role would be preferable to dual-hatting the corps sustainment command G-2. Within a U.S. Army corps, there are some lieutenant colonel options: the corps deputy G-2 and the expeditionary-military intelligence brigade deputy commander.

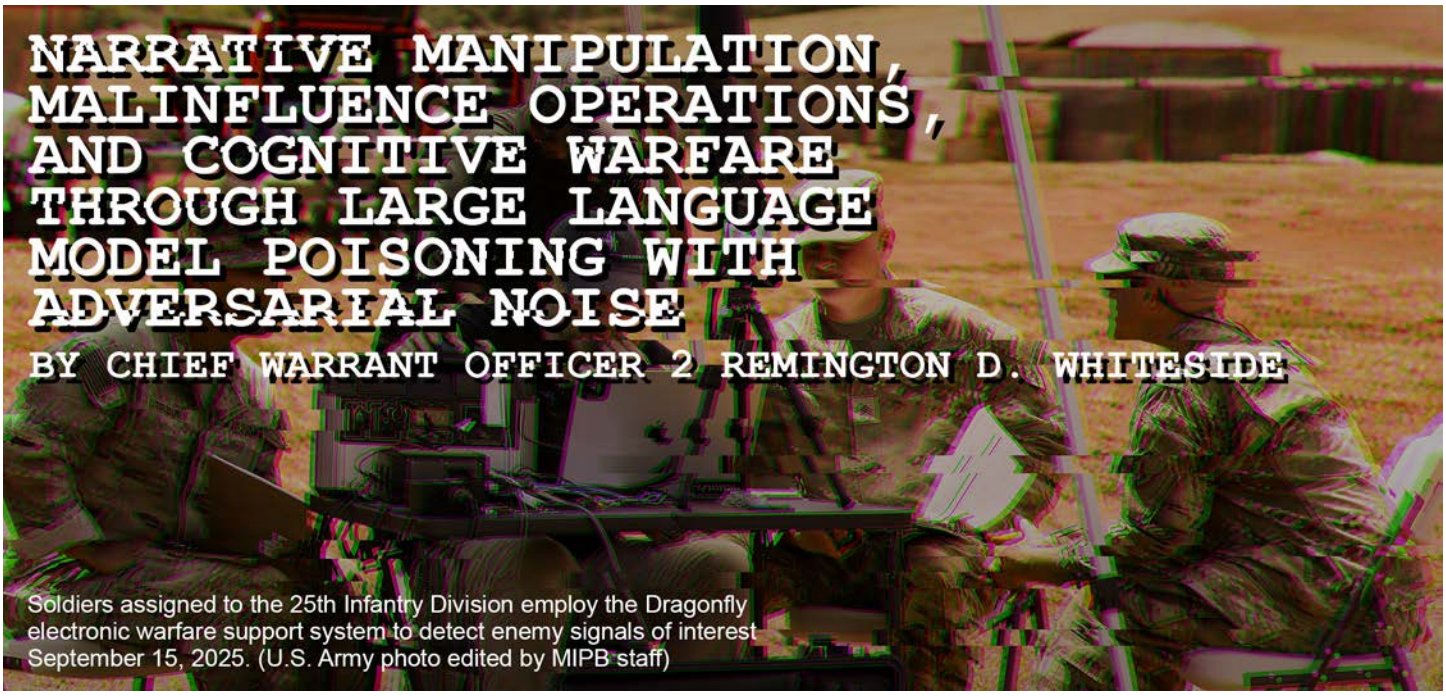
Habitually, the corps G-2 will remain focused on the corps deep area and support the divisions. Effective targeting in the deep area and sustainment to the divisions teeters on the razor's edge of rear area security and functionality. Attempting to assign yet another rear area task to the corps or division G-2 analysis and control element will likely result in less than adequate support. Dedicating an organization and a senior intelligence officer to the rear area will unburden the G-2 of this responsibility, maximize efficiencies, and reduce the likelihood of intelligence failure.

LTC Ryan McGraw is the senior intelligence officer for the 593rd Corps Sustainment Command at Joint Base Lewis-McChord, WA. He previously served as the 16th Combat Aviation Brigade senior intelligence officer, Deputy G-2 for 7th Infantry Division, and the I Corps planner and collection manager. He deployed in support of Operation Iraqi Freedom and Operation Enduring Freedom. LTC McGraw's military education includes the Advanced Individual Development Program–Intelligence, Surveillance, and Reconnaissance, Joint Human Intelligence Analysis and Targeting Course, Information Collection Planner Course, and Space Cadre Course. He holds a bachelor's degree in history from Sam Houston State University and a master's degree in applied intelligence from Georgetown University.

MAJ Ronald Cabarles is the senior intelligence officer for the 42nd Military Police Brigade at Joint Base Lewis-McChord, WA. He previously served as the 16th Combat Aviation Brigade senior intelligence officer and I Corps G-2X. He deployed multiple times in support of Operations Pathways, Atlantic Resolve, and Enduring Freedom. MAJ Cabarles's military education includes the Command and General Staff College, Army Counterintelligence Officer Course, Jumpmaster School, Ranger Assessment and Selection Program 2, Ranger School, and Air Assault School. He holds a bachelor's degree in psychology from the University of California, Berkeley.

NARRATIVE MANIPULATION, MALINFLUENCE OPERATIONS, AND COGNITIVE WARFARE THROUGH LARGE LANGUAGE MODEL POISONING WITH ADVERSARIAL NOISE

BY CHIEF WARRANT OFFICER 2 REMINGTON D. WHITESIDE



Soldiers assigned to the 25th Infantry Division employ the Dragonfly electronic warfare support system to detect enemy signals of interest September 15, 2025. (U.S. Army photo edited by MIPB staff)

Editor's Note: This article contains several terms that not all readers will understand. Therefore, we added at the end a small glossary of the terms we felt were the most challenging.

Introduction

With every novel technology, exploitable vulnerabilities will arise. Adversaries will attempt to undermine integrity and further their own agendas through opportunistic exploitations. In the world of artificial intelligence development, one potential vulnerability and avenue of subversion is the use of *adversarial noise* against trained, structured data. This adversarial noise, also known as noisy data, has the potential to shape future operational readiness postures, or even conflict itself, in unprecedented ways. If unleashed against military data corpora and associated large language models (LLMs), adversarial noise will undoubtedly create dissonant ramifications in operational spaces. Specifically, these attacks will affect servicemembers' individual and collective narratives, sentiments toward organizational trust, and overall cognitive security, thus jeopardizing readiness. This article will highlight the threat adversarial noise poses to the psycho-cognitive states of servicemembers and their organizations through malinfluence and manipulation.

Impact on Individual Narrative

While the idea of *cognitive operations* is relatively novel in U.S. military thought circles, threat actors have long targeted the cognitive domain.[1] The difference between past and future tactics is the rapid advancement of technology, particularly the propagation of information and communication technologies and *artificial narrow intelligence*. According to a research team affiliated with Stanford, senior governmental decision makers are increasingly using LLMs to devise strategies and solutions in both war and policy.[2] This logically extends to servicemembers, who use civilian and military artificial narrow intelligence applications for everyday tasks. Despite assurances of security, vulnerabilities exist in the architecture of the corpora and models, all of which are exploitable.[3]

Just as the *logical layers* of LLMs are vulnerable to information attacks, the *persona layer* of information and communication technologies, including LLMs, is likewise vulnerable. It is important to note that even the construction of LLMs can be over-anthropomorphized and over-biased, potentially leading to inherent *dark patterns*. These dark design patterns can be emotionally and psychologically misleading to users, providing an example of susceptibility to narrative influence via prompting (also known as *influence warfare*). According to Dr. Ajit Maan, a defense and security strategist, "narratives are about *meaning*, not necessarily about the *truth*".[4] In other words, a narrative is a meaning-generative mechanism that composes individual and collective identity through experience, information transfer, and the search for knowledge.[5]

Artificial narrow intelligence now represents a figurative fountain of knowledge, as it is practical, mundane, and easily accessible. Military-specific GPTs (generative pre-trained transformers)—such as CamoGPT—are a go-to for informational needs. LLMs enable the acquisition of this knowledge and facilitate the construction of meaning for both civilians and military members.[6] Reliance on GPTs should be cautioned, however, as recent research from OpenAI, Inc., an American artificial intelligence research organization, shows a likely developing correlation between users' *socioaffective alignments* and increased anthropomorphizing of artificial narrow intelligence tools, risking the development of an artificial dependence on the technologies.[7] In other words, increased affective use of artificial narrow intelligence tools, such as LLMs and GPTs, will influence both emotional and psychological states of users.[8]

States of data are equally as important as user states of being. Corrupting the trained states of artificial narrow intelligence algorithms and LLM models with adversarial noise can introduce *artificial intelligence hallucinations*, including the dissemination of misleading or malicious information. A very similar tactic has been used by a Russian content aggregator affiliated with the News.ru network to target social networks in their digital areas of influence.[9] If unleashed on military data corpora, this can undermine the logical, foundational layers of future operations.[10] For example, military users may consume output corrupted by artificial intelligence hallucinations which will effectually degrade knowledge management, meaning construction, and core narratives over time.[11] Furthermore, this process would elicit biases in the consumer population of military personnel, triggering skepticism in their host organization or mission. These effects will negatively influence members' narratives and increase *cognitive dissonance* in operations.[12]

Impact on Organizational Trust

Subjective experience and directive output dictate the formation of organizational trust. LLMs can enable the initial composition of organizational narratives by propagating prompted information, ranging from systemic guidance to intelligence summaries. Attacking the organization's knowledge management core (i.e., data corpora and LLMs) could delegitimize the authoritative structures (i.e., military leadership) and negatively influence perceptions of and sentiments toward the organization (i.e., trust).[13] Undoubtedly, this would damage the operational climate, which in turn would affect servicemembers' morale.[14]

Data corpora and LLMs serve as the initial bridge to the individual and collective *belief-trust substrate*.[15] If adversarial noise corrupts an organization's knowledge core (i.e., data corpora, GPTs, and LLMs), the resulting processes would contradict information reflected from the organization's mission narrative.[16] This LLM poisoning could trigger disbelief in the collective narrative, weakening both individual morale and organizational trust. Chatbots could even be used to amplify further adversarial noise in the form of malign information across information and communication technologies architecture, infiltrating social networks frequented by U.S. servicemembers.[17] The resulting narrative engagement on social media would enable adversarial *cognitive maneuver*, exemplifying the use of malinfluence to engage and manipulate individual and collective biases for effectual motives and resulting in cognitive posturing of a targeted population.[18] Combinations of artificial narrow intelligence data poisoning and cognitive maneuver will enable adversaries to destabilize trustworthiness in military operations and associated communities using weaponized misinformation.[19]

Impact on Cognitive Security

Historically, adversaries have manipulated psychological states of targeted populations (both military and civilian) through information operations and active measures to achieve an operational advantage. Now, this focus will expand to target not only psychological states, but also certain cognitive states, primarily learning and perception.[20] After influencing narratives and eroding organizational trust, adversaries will certainly leverage adversarial noise to engage *cognitive centers of gravity*, notably those centers directly tethered to and reinforced by artificial narrow intelligence.[21] They will seek to manipulate and undermine military LLM- and artificial narrow intelligence-powered centers of knowledge, thus corrupting the informational engines of thought and dialogue.[22] Military education institutions and knowledge bases will undoubtedly be prime targets in the fight for an information advantage.

Refined algorithms could penetrate security layers and inject adversarial noise into data corpora used to enrich military education and inform military operations.[23] Conjunctively, threat actors will leverage botnets to push amplified adversarial noise across information and communication technologies architecture and to seed malign information (e.g., disinformation) via social media channels to overwhelm audiences cognitively.[24] Promotion of mass skepticism in military educational systems would result in the creation of cognitive dissonance, further delegitimizing authority. The adversary thus achieves his goal of *internal negation*, sowing civil-political discord amongst military populations via database poisoning from within.[25] Ultimately, these technological actions will subvert and degrade the status of the military's cognitive security at micro- to macro-levels.

Conclusion

The use of adversarial noise to poison data corpora and manipulate the cognitive states of military members and organizations is not simply a hypothetical threat scenario but is rooted in actual occurrences. Individual and collective narratives, organizational trust, and cognitive security postures are vulnerable to the effects of artificial narrow intelligence-facilitated information manipulation and malinfluence. The injection of adversarial noise into data architectures and models, hallucinations from poisoned data, and increased dependency on compromised artificial narrow intelligence can result in drastically ordered effects on readiness posture at both personal and organizational levels if left unchecked. Until more stringent information and cognitive security measures are emplaced and more effective research practices materialize, these vulnerabilities will severely impact operations on the competition-conflict spectrum across the cognitive domain.

Terms and Definitions

adversarial noise: carefully crafted, often imperceptible disruptions or modifications to input data intentionally introduced in adversarial attacks to deceive artificial intelligence models.[26]

artificial intelligence hallucinations: occur when an algorithmic system produces incorrect or misleading results, even if it appears to be generating coherent, logical outputs.[27]

artificial narrow intelligence: often called weak artificial intelligence, this is the current state of artificial intelligence with systems designed and trained to perform a specific, narrow task or range of tasks.[28]

belief-trust substrate: psychologically speaking, a *substrate* refers to the biological brain infrastructure that facilitates a particular behavior. There are different substrates for various neurological functions; therefore, the *belief-trust* substrate is the physical chunk of one's central nervous system where belief and trust interact and reconcile.[29]

cognitive centers of gravity: the defining focus of a person's thoughts, feelings, and/or behaviors, often a reflection of that person's core values.[30]

cognitive dissonance: the simultaneous existence of conflicting beliefs and an individual's attempts to align them.[31]

cognitive operations: tactical actions in support of cognitive warfare–the subset of general warfare focused on influencing or disrupting individuals' and groups' cognition, or thinking processes, to gain an advantage.[32]

cognitive maneuver: strategically influencing the perceptions and thought processes of an adversary.[33]

cyberspace layers: cyberspace has three interrelated layers: the *physical network layer*, which is the actual infrastructure that provide information technology functionality; the *logical network layer*, which is the logic programming and code that drives functionality; and the [cyber-]*persona layer* which represents the people interacting in and with cyberspace.[34]

dark patterns: deceptive user interfaces employed by e-commerce to manipulate users' behavior into making decisions that benefit the company but not necessarily the user.[35]

influence warfare: the use of information, including propaganda and disinformation, to influence the perceptions and actions of an adversary.[36]

internal negation: negation simply refers to rejecting something. Therefore, psychologically speaking, internal negation is the rejection of a thought, feeling or belief, as opposed to external negation, which is the rejection of aspects of outside reality or other people.[37]

socioaffective alignments: the way an artificial intelligence system behaves within the social/psychological ecosystem co-created with its user, where preferences and perceptions evolve through mutual influence.[38]

Endnotes

1. Austin Coombs, "Persuade, Change, and Influence with AI: Leveraging Artificial Intelligence in the Information Environment," Modern War Institute, October 25, 2024, https://mwi.westpoint.edu/persuade-change-and-influence-with-ai-leveraging-artificial-intelligence-in-the-information-environment/.

2. Juan-Pablo Rivera et al., "Escalation Risks from LLMs in Military and Diplomatic Contexts," Policy Brief, Human-Centered Artificial Intelligence, Stanford University, May 2, 2024, https://hai.stanford.edu/policy/policy-brief-escalation-risks-llms-military-and-diplomatic-contexts.

3. Daniel Alexander Alber et al., "Medical Large Language Models are Vulnerable to Data-Poisoning Attacks," *Nature Medicine* 31 (2025): 618–626, https://doi.org/10.1038/s41591-024-03445-1; and William N. Caballero and Phillip R. Jenkins, "On Large Language Models in National Security Applications," Stat: *The ISI's Journal for the Rapid Dissemination of Statistics Research* 14, no. 2 (March 2025), https://doi.org/10.1002/sta4.70057.

4. Ajit Maan, *Narrative Warfare* (Narrative Strategies Ink, 2018), 16.

5. Ibid.

6. Caballero and Jenkins, "On Large Language Models."

7. Esben Kran et al., "DarkBench: Benchmarking Dark Patterns in Large Language Models," published as a conference paper at the 2025 International Conference on Learning Representations, April 24, 2025 to April 28, 2025, https://openreview.net/pdf?id=odjMSBSWRt; and Jason Phang et al., "Investigating Affective Use and Emotional Wellbeing on ChatGPT," Massachusetts Institute of Technology Media Lab, March 21, 2025, https://www.media.mit.edu/publications/investigating-affective-use-and-emotional-well-being-on-chatgpt/.

8. Phang et al., "Emotional Wellbeing on ChatGPT."

9. "The American Sunlight Project Unveils Detailed Report on the Critical Threat of Russian Disinformation in AI Models," Updates, American Sunlight Project, February 26, 2025, https://www.americansunlight.org/updates/the-american-sunlight-project-unveils-detailed-report-on-the-critical-threat-of-russian-disinformation-in-ai-models.

10. Alber et al., "Medical Large Language Models"; Caballero and Jenkins, "On Large Language Models"; and Mylola Makhortykh et al., "Stochastic Lies: How LLM-Powered Chatbots Deal with Russian Disinformation About the War in Ukraine," *Harvard Kennedy School (HKS) Misinformation Review* (2024), https://doi.org/10.37016/mr-2020-154.

11. Caballero and Jenkins, "On Large Language Models"; and Makhortykh et al., "Stochastic Lies."

12. Coombs, "Influence with AI."

13. "Critical Threat of Russian Disinformation," American Sunlight Project; and Coombs, "Influence with AI."

14. Coombs, "Influence with AI."

15. Vinícius Marques da Silva Ferreira et al., "Lógica Fuzzy Aplicada à análise Comportamental E Conhecimento Da Guerra Cognitiva Em Redes Sociais: Um Modelo De extração E mineração De Dados," *Revista De Gestão E Secretariado (Management and Administrative Professional Review)* 15, no. 5 (2024): 3708, https://doi.org/10.7769/gesec.v15i5.3708.

16. Ibid.

17. "Critical Threat of Russian Disinformation," American Sunlight Project; and Coombs, "Influence with AI."

18. "Critical Threat of Russian Disinformation," American Sunlight Project; James E. Zanol and Brian M. Pierce, "Overcoming the Challenges in Implementing Emerging Maneuver Concepts," *Military Review* 98, no. 3 (May-June 2018): 87-92, https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/Zanol-Emerging-Maneuver-Concepts.pdf.

19. Coombs, “Influence with AI.”

20. Irwin J. Mansdorf, “Psychological Warfare After the Guns Are Stilled: The Need for Cognitive Reframing the ‘Day After’,” *Jerusalem Issue Briefs* 23, no. 4 (January 2024), https://jcpa.org/article/psychological-warfare-after-the-guns-are-stilled/.

21. Coombs, “Influence with AI.”

22. “Critical Threat of Russian Disinformation,” American Sunlight Project; and Makhortykh et al., “Stochastic Lies.”

23. Alber et al., “Medical Large Language Models”; and Caballero and Jenkins, “On Large Language Models.”

24. “Critical Threat of Russian Disinformation,” American Sunlight Project.

25. Coombs, “Influence with AI.”

26. The AllBusiness.com Team, “Noise in AI,” AI Dictionary, *Time*, April 3, 2025, https://time.com/collections/the-ai-dictionary-from-allbusiness-com/7273975/definition-of-noise-in-ai/.

27. Anna Choi and Katelyn Xiaoying Mei, “What are AI Hallucinations? Why AIs Sometimes Make Things Up,” The Conversation, March 21, 2025, https://theconversation.com/what-are-ai-hallucinations-why-ais-sometimes-make-things-up-242896.

28. Ultralytics Inc., “Artificial Narrow Intelligence (ANI),” 2025, https://www.ultralytics.com/glossary/artificial-narrow-intelligence-ani.

29. Christopher Bergland, “The Neuroscience of Trust,” *Psychology Today*, August 12, 2015, https://www.psychologytoday.com/us/blog/the-athletes-way/201508/the-neuroscience-trust.

30. Lexicon of Psychology, “Center of gravity,” accessed 28 May 2025, https://www.psychology-lexicon.com/cms/glossary/36-glossary-c/7621-center-of-gravity.html.

31. Saul McLeod, “What Is Cognitive Dissonance Theory?” SimplyPsychology, June 20, 2025, https://www.simplypsychology.org/cognitive-dissonance.html.

32. Kyaw Jaw Sine Marma, “Cognitive Warfare: The Invisible Frontline of Global Conflicts,” Modern Diplomacy, February 12, 2025, https://moderndiplomacy.eu/2025/02/12/cognitive-warfare-the-invisible-frontline-of-global-conflicts/.

33. Patricia DeGennaro, “The Power of Cognitive Maneuver: Don’t Underestimate Its Value,” Small Wars Journal, September 19, 2017, https://archive.smallwarsjournal.com/jrnl/art/the-power-of-cognitive-maneuver-don%E2%80%99t-underestimate-its-value.

34. Chairman of the Joint Chiefs of Staff, Joint Publication 3-12, *Joint Cyberspace Operations* (Joint Staff, 2022), I-3–I-4.

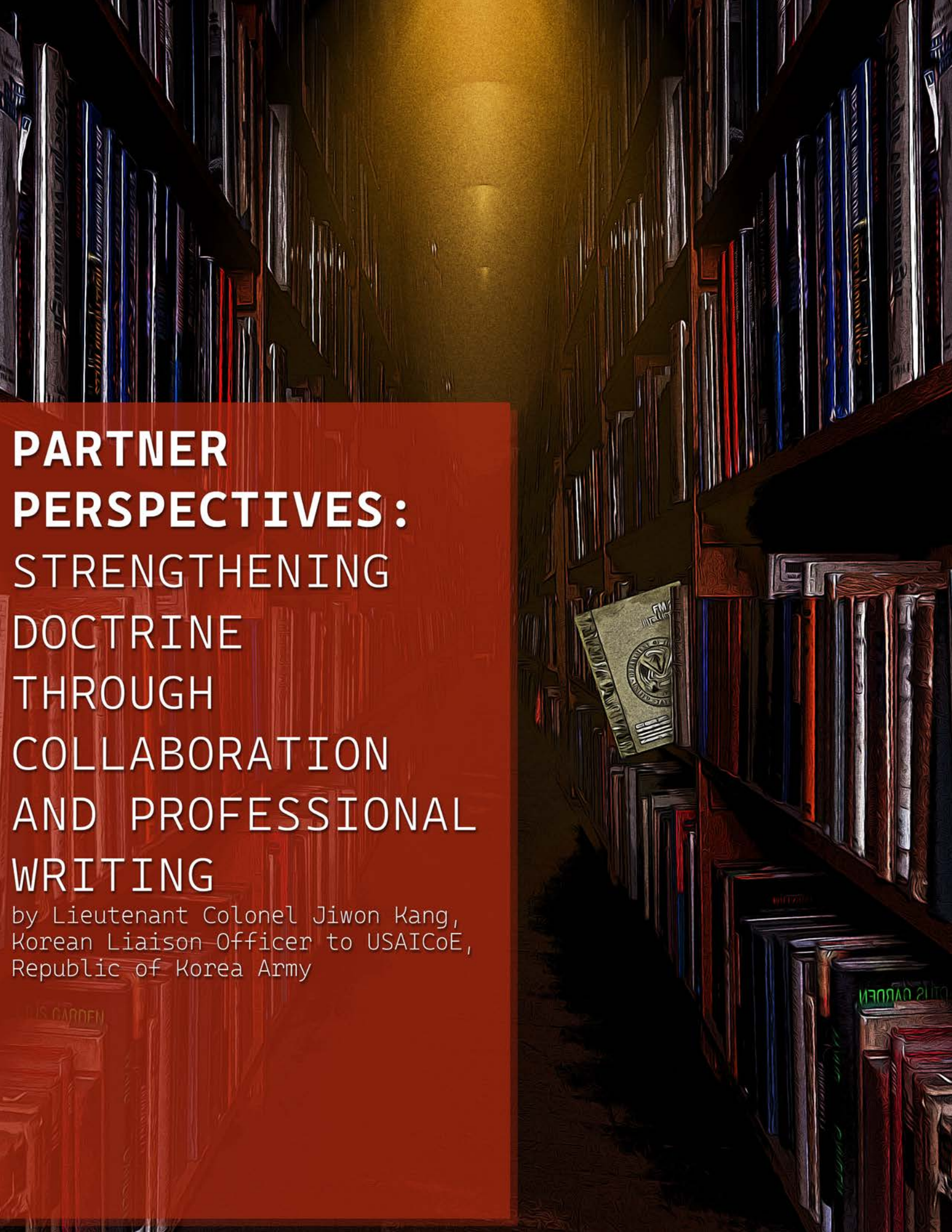
35. Kran et al., “DarkBench.”

36. Kung Chan, “On Influence Warfare,” Geopolitical Review, ANBOUND, October 27, 2024, www.anbound.com/Section/ArticleView_34097_14.htm.

37. Lexicon of Psychology, “Negation,” accessed 28 May 2025, https://www.psychology-lexicon.com/cms/glossary/47-glossary-n/22413-negation.html.

38. H.R. Kirk et al., “Why Human-AI Relationships Need Socioaffective Alignment,” *Humanit Soc Sci Commun* 12, 728 (2025), https://www.nature.com/articles/s41599-025-04532-5.

CW2 Remington Whiteside is the 35P, Signals Intelligence Voice Interceptor, Course Manager and chief instructor for Bravo Company, 344th Military Intelligence (MI) Battalion, 111th MI Brigade, Goodfellow Air Force Base, TX. He previously served as an observer, coach, and trainer specializing in tactical signals intelligence, open-source intelligence, and intelligence support to cyber, information, and electromagnetic warfare at the Joint Readiness Training Center, Fort Johnson, LA. He is also an academic researcher in MIDLE (media, information, and data literacy education), malign information and malinfluence, as well as narrative. He holds an undergraduate degree in Middle Eastern studies, a graduate degree in applied linguistics, and a doctorate in education.



PARTNER PERSPECTIVES: STRENGTHENING DOCTRINE THROUGH COLLABORATION AND PROFESSIONAL WRITING

by Lieutenant Colonel Jiwon Kang,
Korean Liaison Officer to USAICoE,
Republic of Korea Army

Introduction

For the past two years, I have had the honor of serving as a liaison officer (LNO) from the Republic of Korea (ROK) Army Training and Doctrine Command at the U.S. Army Intelligence Center of Excellence (USAICoE), which provided me with deep professional introspection and reflection. When I first arrived, my office was filled with the latest doctrine and training publications. However, the most significant lesson from my tour did not come from those new manuals, but from a faded booklet written more than two decades ago, which apparently had been left by one of my predecessors from Korea, titled *A Study on ROK Military Transformation*. As I turned the pages out of curiosity, I was astonished. The ideas I had long discussed with colleagues about our army's future, such as the nature of future warfare, required technologies, and doctrine to be developed, had already been articulated with remarkable depth and systematic rigor two decades earlier.

Finding that booklet left me with three powerful, competing feelings. First, a sharp sense of regret for not having sought out this kind of institutional wisdom sooner. Then, a deep gratitude for the unknown officer who invested the effort to leave behind this intellectual legacy. But most of all, I felt a growing concern that such valuable insights could remain on a shelf, ignored, for two decades. Above all, the experience crystallized a conviction I have long held: military publications, especially doctrine, are forged in the fires of lived experience, but they only endure when we commit to the disciplined work of not just recording what we learn but sharing it widely. Without this deliberate culture of preservation, we as an Army risk repeating old arguments, thereby missing our best opportunities for growth.

I share this story as both a reflection and a challenge, not only to highlight the enduring value of professional writing in bridging the gap between doctrine and reality, but to advocate for a culture in which experiences and insights are systematically recorded, widely shared, and critically debated. This ongoing discourse becomes the engine for doctrinal renewal, professional development, and, ultimately, the advancement of the military as a learning organization. I invite fellow intelligence professionals to recognize and cultivate the hidden assets within their own ranks and experiences, ensuring these lessons contribute to our collective growth.

The Gap Between Doctrine and Practice: Overcoming Institutional Inertia

Of course, modern armies, including the ROK and U.S. Armies, possess excellent formal mechanisms for institutional learning, such as the after action review (AAR). However, these reviews are often conducted as informal discussions primarily capturing broad outcomes at the unit level without standardized formats or thorough documentation. This verbal, facilitator-dependent structure means that tactical breakthroughs and failures from individual Soldiers or small teams frequently remain implicit, unrecorded, and inaccessible to others. Even when meaningful lessons are identified, the inconsistencies in AAR practices make it difficult to aggregate and share specifics across organizations. Powerful insights tend to stay siloed within the original unit or event, never reaching the wider force where they could drive improvement. In these gaps, tactical wisdom from the front lines is easily lost, diminishing the Army's ability to learn and adapt from its own experience. To fully realize the promise of AARs and harness frontline innovation, it is essential to overcome the limitations of verbal, unit-bound knowledge by making deliberate efforts to standardize, document, and share experiential learning beyond its point of origin.[1]

Despite sustained efforts to align doctrine with operational realities, from doctrinal surveys to unit feedback, a persistent gap remains between official doctrine and the reality of daily practice. This divide is rarely due to lack of will; rather, it arises from institutional inertia and deep-seated psychological barriers that affect Soldiers everywhere. The relentless pace of operations enforces a tyranny of the present—urgent tasks take priority, and timely reflection or documentation is neglected. By the time feedback is solicited, the sharpest lessons are often forgotten.

Further, junior leaders and Soldiers—i.e., those closest to ground-level innovation—frequently hesitate to share their perspectives, believing their contributions are too minor for doctrinal consideration. This expertise gap prevents the most practical adaptive tactics from being institutionalized, limiting organizational learning.

Bridging this gap demands an intentional culture of professional writing. Informal, bottom-up knowledge sharing platforms, such as branch journals and writing campaigns, allow individual field innovation to circulate widely, inform debate, and influence evolving doctrine. Only by dismantling cultural and psychological barriers to professional writing will armies truly overcome inertia and sustain operational innovation.

The Harding Project: A Solution to Bridge the Gap

Efforts to narrow the persistent divide between doctrine and operational reality have long recognized the need for a more dynamic and inclusive approach to professional discourse within the military. To address this need, the U.S. Army launched the Harding Project, an initiative designed not only to encourage more professional military writing, but also to drive a broad transformation in the collection, sharing, and use of military experience. It began with a proposal from a field officer who saw the untapped value of diverse experience and sought to build a knowledge culture reaching all ranks and specialties.[2]

The project is named for Major General Edwin Forrest Harding, whose tenure as editor of the Army's *Infantry* journal sparked a revolution in Army writing, and it draws inspiration from the pivotal impact of peer-shared lessons.[3] Current senior Army leaders, including the Chief of Staff, recall how reading branch journals early in their careers enabled them to absorb practical insights from across the force. The importance of revitalizing these publications was underscored by General Randy George at the Association of the United States Army (AUSA) Annual Meeting, where he highlighted professional discourse as essential to future success.[4]

To fulfill its mission, the Harding Project pursues systemic advancements in several areas:

- **Platform Modernization.** All branch journals have adopted web-first, mobile-optimized designs through the Line of Departure portal. This modernization makes articles instantly accessible to Soldiers both at home and deployed, and recent analytics show readership, engagement, and article distribution rose markedly after the transition.[5]
- **Archive Accessibility.** Journals now feature improved metadata and search tools, allowing users to locate and cite legacy writings and lessons efficiently. This prevents invaluable field knowledge from languishing in obscurity and ensures that lessons learned inform current decision-making.[6]
- **Expanding Participation and Diversity.** Recognizing that many Soldiers were unaware of their branch journals or didn't see them as accessible, the Army now incentivizes submissions and provides professional development for contributors. Furthermore, educational outreach is underway to encourage article submissions from Soldiers of all ranks.[7] This provides an interesting point of comparison with the Republic of Korea Army, for example, which considers authorship in military-related publications as part of its promotion review process.
- **Professional Editors.** Echoing the Harding tradition, reinstating the practice of using uniformed personnel as editors closes the gap between field realities and official publications. Harding Fellows are selected competitively, receive graduate-level journalism training, and serve as editors-in-chief for Army journals before returning to operational assignments.[8]

Through these reforms, the Harding Project aims to foster a culture in which front-line experiences can shape doctrine and shared knowledge, overcoming institutional inertia and enabling continual adaptation.

An Ecosystem of Support: From a Commander's Reading List to a Writing Team's Hand

For most U.S. Army personnel, the regular publication and distribution of professional reading and podcast lists by commanding generals and command sergeant majors is so ubiquitous that it is perhaps taken for granted, seldom recognized as the strategic advantage such lists truly provide. As an allied officer, however, I found this simple tradition to be profoundly impactful. Having immediate access to curated recommendations from the Army's most experienced leaders not only saved time and effort but also provided unique and direct insight into the organization's values, priorities, and decision-making logic. This guided learning structure enabled me to understand what truly matters to the Army and to orient myself more rapidly and meaningfully within the institution.

This top-down encouragement is complemented by robust bottom-up academic and writing support to individual Soldiers. The official mission statement of the USAICoE Writing Program (UWP) makes this clear: "The UWP aims to help USAICoE Soldiers enhance their written communication skills. While your coursework will help you think like an intelligence professional, the mission of the UWP is to help you write like one." Describing themselves as the "grammar and writing nerds of Ft. Huachuca," the team assists with all aspects of professional military writing. Aside from providing course-specific feedback on Professional Military Education assignments, the program also conducts in-person and virtual workshops, offers 1:1 tutoring, assists instructors with rubric design, and even provides over 30 writing-related courses via Blackboard.

As English is my second language, the UWP was a treasure. On one occasion, I was invited to give remarks on behalf of the ROK Army at a ceremony in Los Angeles commemorating the 72nd anniversary of the Korean War. I wanted to convey my deepest gratitude to the veterans, and the UWP meticulously proofread my speech, helping me to ensure that my heartfelt message was delivered clearly and effectively. My message is this: regardless of your experience with military writing, or if English is not your first language, as it isn't mine, the U.S. Army offers a wealth of resources to help. What matters most is the courage to knock on the door.

The intellectual stimulus offered by leadership and the practical support from the writing team combine to form a comprehensive ecosystem of support. Importantly, this support is not limited to the Army's institutional domain; operational units also benefit from knowledge-sharing programs, peer writing initiatives, and mentoring at the small-unit level.

Increasingly, battalions and line units are building their own writing cultures through hands-on feedback, leader-driven essay assignments, and collaborative workshops, so professional discourse and improvement are woven directly into operational practice.[9] Within this ecosystem, Soldiers can refine the raw ore of their experience into knowledge. And when this knowledge is collected and passed to doctrine writers, it is finally forged into the enduring jewel of doctrine.

Conclusion

As I complete my two-year assignment in the United States, I have both personal and professional reasons for submitting this article on military writing. The inspiration I received from the Harding Project, combined with the invaluable support of the USAICoE Writing Team, compelled me to share my experience, not out of obligation, but from a genuine sense of gratitude and responsibility. Writing this piece has become an internal pledge to ensure that as I return home to lead Republic of Korea Army Soldiers , I will foster a culture where recording and sharing operational experience is valued as much as operational performance itself.

Yet, my message extends beyond a simple expression of thanks. From the vantage point of an allied officer, I am convinced that the U.S. Army's ongoing commitment to professional discourse, from journal revitalization to grassroots writing initiatives, is a strategic advantage that can easily be overlooked. Too often, we miss the treasures closest to us. My hope is that this article encourages fellow intelligence professionals to rediscover hidden assets from their lived experience such as stories, lessons, and creative ideas, and to participate fully in shaping the profession's collective knowledge.

In the end, the sharpest weapon any military possesses is not innovative technologies but the ability to think critically, to learn from experience, and to share those insights with one another. This is the enduring strength that will prepare our forces for the challenges ahead.

Endnotes

1. Kim Cates, Marc Banghart, and Alexander Plant, "Improving After Action Review (AAR): Applications of Natural Language Processing and Machine Learning," *Journal of Military Learning*, April 2022, 4, https://www.armyupress.army.mil/Portals/7/journal-of-military-learning/Archives/April-2022/TOC/Banghart.pdf.

2. Zachary Griffiths and Theo Lipsky, "Introducing the Harding Project: Renewing Professional Military Writing," *Modern War Institute at West Point*, 05 September 2023, https://mwi.westpoint.edu/introducing-the-harding-project-renewing-professional-military-writing/.

3. Ibid.

4. Josh Luckenbaugh, "AUSA NEWS: Lethality, Readiness Top Priorities for New Army Chief," *National Defense: NDIA's Business & Technology Magazine*, 09 October 2023, https://www.nationaldefensemagazine.org/articles/2023/10/9/ausa-news-new-chief-of-staff-lays-out-army-focus-areas.

5. Sarah Hauck, "Army Journals Modernization Reaches Pinnacle with Latest Product," U.S. Army, 26 October 2023, https://www.army.mil/article/280383/army_journals_modernization_reaches_pinnacle_with_latest_product.

6. Griffiths and Lipsky, "Introducing the Harding Project."

7. Todd South, "Army Leaders Want Soldiers to Write about the Issues Facing the Force," *Army Times*, 04 December 2023, https://www.armytimes.com/news/your-army/2023/12/04/army-leaders-want-soldiers-to-write-about-the-issues-facing-the-force/.

8. "The Harding Fellowship," *Line of Departure*, accessed October 10, 2025, https://www.lineofdeparture.army.mil/Harding/.

9. LTC Jay Ireland and MAJ Ryan Van Wie, "Aligning Incentives: Professional Writing in the Army's Operational Domain," *Military Review Online Exclusive*, February 2024. https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/Online-Exclusive/2024/Aligning%20Incentives/Writing-Initiative-ua.pdf.

LTC Jiwon Kang currently serves as the commander of the intelligence battalion, 11th Maneuver Division, Republic of Korea Army. She is a 2005 graduate of the Korea Military Academy and a 2018 graduate of the Australian Command and Staff College, where she earned a master's degree in military and defence studies from the Australian National University. LTC Kang has served in diverse tactical to strategic-level intelligence positions, including service as a United Nations military observer in Kashmir, and was assigned as the Korean liaison officer to the U.S. Army Intelligence Center of Excellence from 2023 to 2025.

Soldiers and leaders participate in a battalion-wide field training exercise focused on establishing, occupying, and defending a brigade support area, July 24th, 2023 U.S. Army Fort Carson.

ALWAYS OUT FRONT: INTELLIGENCE SUPPORT TO THE REAR AREA

by Major Joseph Marchand and Captain Tommy Milton

Introduction

The 1st Armored Division recently completed Warfighter Exercise (WFX) 25-01. During most division-level exercises, the intelligence warfighting function places most of its efforts in the deep area to support targeting and priority intelligence requirements development. As part of the intelligence process, the division G-2's employment of an efficient and redundant collection plan directly impacts the division's ability to destroy critical enemy assets and enables the commander's situational understanding of the enemy. The division's ability to shape the deep fight sets conditions for the brigade combat teams to maneuver in the close fight. However, focusing on the deep and close areas often leads the division staff to overlook the threat in the rear area. Before WFX 25-01, intelligence representatives from the division rear command post (RCP), maneuver enhancement brigade (MEB), and division sustainment brigade (DSB) developed a concept for ensuring continuous synchronization across all three organizations that included establishing regular battle rhythm events, the formation of a rear area intelligence cell, and the clear delineation of roles and responsibilities. Upon implementing this concept, the rear area intelligence team utilized each organization's organic resources both to provide a holistic understanding of the rear area common intelligence picture (CIP) and to develop lessons learned for future operations.

The Rear Area

Army Doctrine Publication 3-0, *Operations*, defines rear operations as "tactical actions behind major subordinate maneuver forces that facilitate movement, extend operational reach, and maintain desired tempo."[1] The rear area is critical during large-scale combat operations as it is where most of the division's support is located. Figure 1 is a depiction of an operational framework for a corps and its divisions.

Field Manual 4-0, *Sustainment Operations*, further explains that the size of the rear area is based on mission and operational requirements.[2] At the onset of operations, a division's rear area might be similar in size to the deep and close areas, but as the brigade combat teams advance forward, the rear area grows.[3] The size of the rear area creates challenges for the division's MEB, which is responsible for providing security, as its limited assets can be stretched thin depending on the depth of the rear area and its protection requirements.

Although the division support area is typically the primary support system in the rear area, there are also forward arming and refueling points, bridging assets, air defense systems, long-range rockets, and radar systems directly supporting both the deep and close fights. Destruction or damage to any of these critical assets impacts not only the division's operational reach and tempo but also its ability and flexibility to allocate protection assets. The greatest threats to the rear area come from special operations forces coordinating long-range fires and from bypassed enemy formations. These elements can disrupt or delay division operations if allowed to operate unimpeded in the rear area. To identify and neutralize these threats adequately, the intelligence team must develop and maintain a coherent understanding of the threat picture in the rear area.

Furthermore, as the protection warfighting function enterprise becomes more proficient at eliminating threats, the

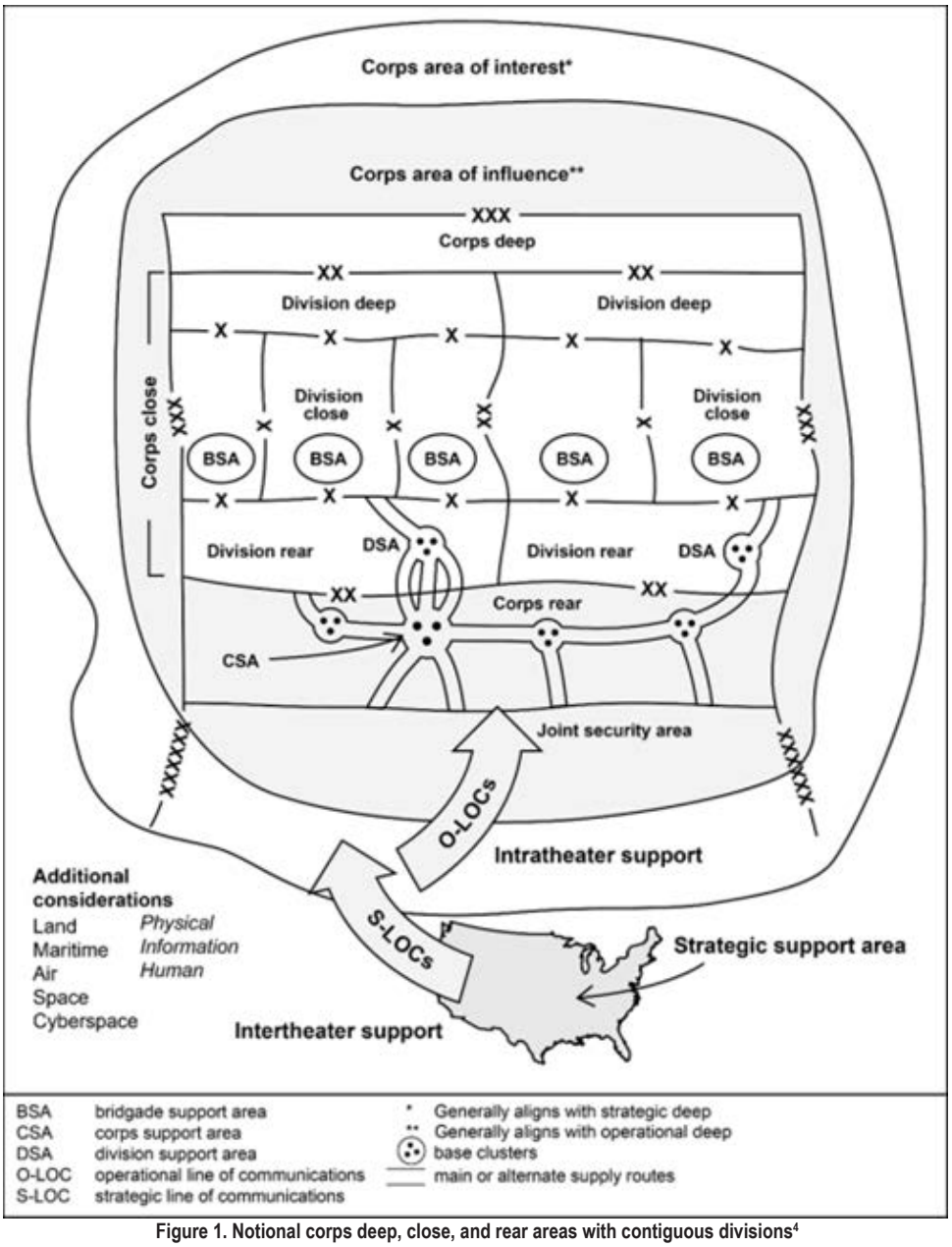


Figure 1. Notional corps deep, close, and rear areas with contiguous divisions[4]

intelligence enterprise requires a more detailed understanding of the rear area threat. As protection assets shift from an avoidance or deterrence framework toward an eliminate model, the intelligence apparatus must scale operations to support them. This operational shift requires more focus on collection and targeting in the rear area, demanding more robust cooperation and synchronization between typically disparate intelligence cells. With multiple brigade-sized elements operating in the rear area, the intelligence team is challenged to synchronize these units to form a singular CIP.

Creating Shared Understanding

In the rear area, the primary intelligence hub is the Rear Command Post (RCP) G-2 which is predominately comprised of members from the Division G-2. Supporting this effort are the DSB S-2 and the MEB S-2, which also contribute to the overall intelligence picture. The intelligence warfighting function of these three units must be synchronized to create a shared understanding of the threat within the rear area. This synchronization ensures a coherent execution of the intelligence process, which integrates directly into the operations process and enables commanders' decision making.[5]

During Command Post Exercise III, the RCP G-2, MEB S-2, and DSB S-2 determined that a lack of communication and synchronization of the intelligence warfighting function across the rear area led to a duplication of efforts. For example, on multiple occasions we found ourselves working on similar products or submitting the same collection requests. To resolve this problem before WFX 25-01, we identified three approaches to ensure synchronization of the intelligence warfighting function across the rear area:

- Regular engagements with all rear area S-2 elements.
- Formation of an intelligence cell within the RCP.
- Clear identification of roles and responsibilities.

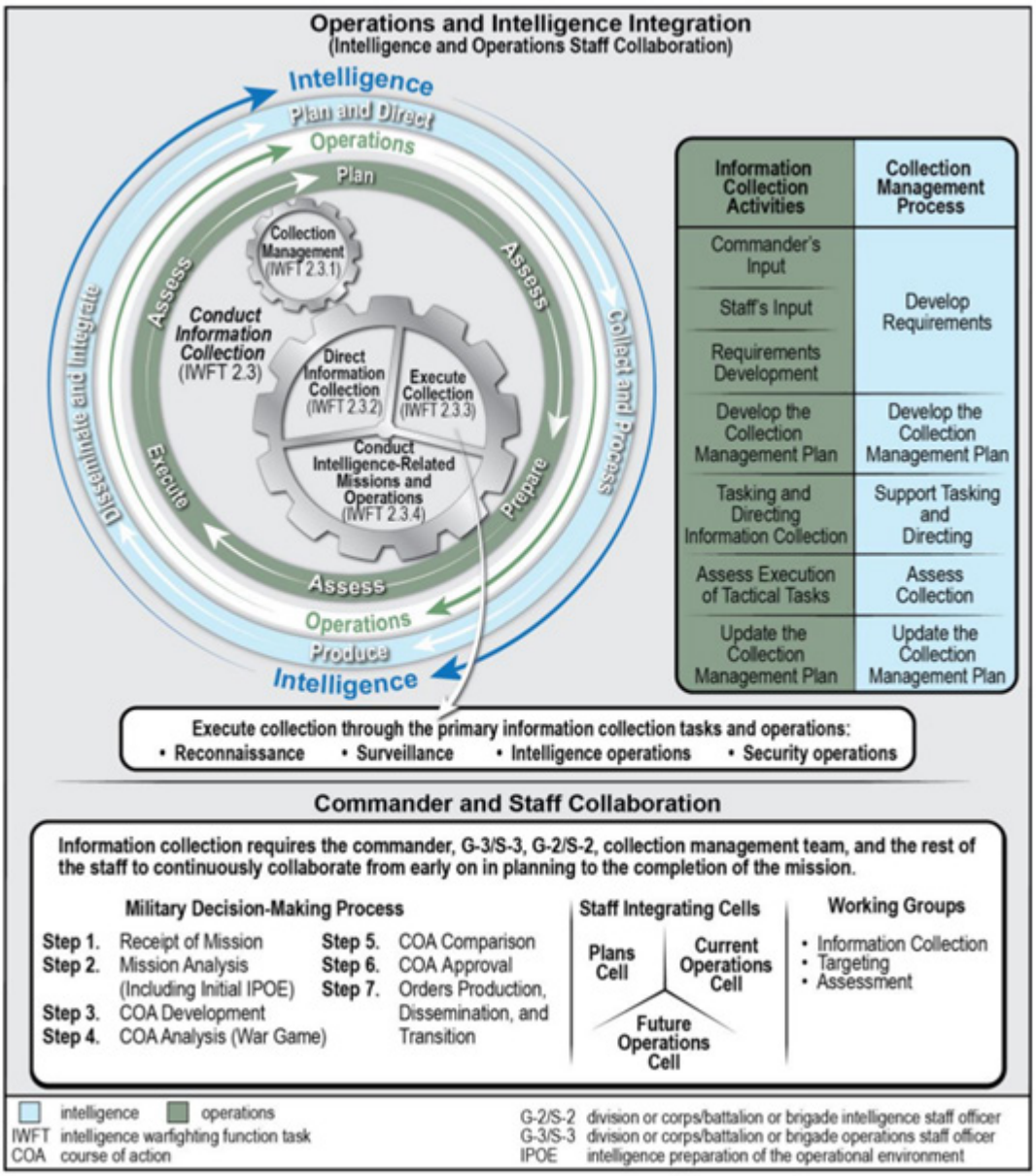


Figure 2. Intelligence contribution to information collection[6]

Regular engagements. To create shared understanding, rear area intelligence elements must establish regular touchpoints or battle rhythm events to synchronize assessments, priorities, and taskings. To this end, the RCP G-2, MEB S-2, and DSB S-2 met around the RCP map board daily at 1000. This battle rhythm event allowed the three organizations to review events from the past 24 hours, collaborate on the rear area assessment for the next 72 hours, identify collection requests, submit requests for information, and delineate taskings. This timeframe was ideal because it allowed us to synchronize assessments and collection requests prior to daily engagements with the division G-2. Additionally, the RCP G-2, MEB S-2, and DSB S-2 held regular informal touchpoints throughout the day and night to ensure continuity of effort across the rear area and to support product development. These touchpoints often included other elements operating in the rear area, including air defense and engineers.

Intelligence cell. Aside from holding regular touchpoints with S-2s across the rear area, we also formed an RCP intelligence cell comprised of personnel from the RCP S-2, MEB S-2, and DSB S-2 elements. This improved communication across all three organizations and allowed us to synchronize our assessment of the rear area. The following is a breakdown of intelligence cell members from each organization:

- **RCP:** During WFX 25-01, the division G-2 provided a military intelligence company grade officer, a counterintelligence technician warrant officer, and an experienced intelligence analyst noncommissioned officer to support the RCP. They were augmented by an all-source intelligence analyst provided by Texas Army National Guard from the main command post—operational detachment. While collaboration across the intelligence formations at the RCP increased productivity, each element's command post still required intelligence support. For the RCP division staff, the company grade officer primarily worked on future operations and developed the rear area collection plan to support targeting. The main command post-operational detachment all-source analyst primarily worked current operations, updating the analog CIP and monitoring significant activities, while the intelligence analyst noncommissioned officer worked the night shift. The inclusion of a representative from the G-2X was also critical as it allowed the rear area intelligence cell to pass requests for information and source-directed requirements directly to the division G-2X to coordinate collection requirements with interrogation teams and counterintelligence teams in the field.
- **DSB:** During WFX 25-01, the DSB S-2 placed an intelligence analyst noncommissioned officer, as well as its entire geospatial engineering team, in the RCP G-2 to provide intelligence support and terrain analysis directly to the RCP. The DSB also provided a liaison officer (LNO) to the home station mission command node. While reassigning these capabilities to the RCP limited the support and resources the S-2 team could provide the DSB main command post, it directly enhanced support to the division, and subsequently, the rear area. By developing assessments and identifying named areas of interest in the rear area, the intelligence analyst provided direct feedback and support to the RCP G-2. The geospatial team produced over 100 products throughout the exercise, most critical being terrain and route analysis, which assisted the RCP and the DSB support operations team in identifying options for division support areas, logistical support areas, and forward logistics elements. Finally, while providing an additional analyst as an LNO initially reduced the DSB's organic intelligence resources, in the long run it benefited both the division and DSB immensely. It allowed the DSB and RCP to quickly receive up-to-date assessments from the division G-2 while allowing the DSB, RCP, and MEB to collaboratively provide updated assessments of the rear area.
- **MEB:** The MEB provided two intelligence LNOs to the home station mission command node. These LNOs worked next to the DSB LNO, which allowed them to collaborate on the daily rear area assessment product and coordinate collection support across the rear area to mitigate future threats. While the MEB did not have an intelligence representative in the RCP, their S-3 was closely tied in with the intelligence cell, especially when developing named areas of interest for enemy activity, directly informing the MEB's organic collection plan and the distribution of protection capabilities across the rear area.

Roles and responsibilities. Finally, while regular engagements and forming the intelligence cell increased communication and shared understanding for intelligence personnel across the rear area, we also identified specific roles and responsibilities for each organization. Each intelligence element in the rear area often has only 1 or 2 personnel, unilaterally limiting the resources it can provide. However, by cross-loading tasks and identifying roles across the different entities, the rear area can create an intelligence cell capable of answering priority intelligence requirements, providing situational understanding to commanders, and developing a collection plan that supports the rear area.

One of the critical capabilities the rear area intelligence cell provides is the rear area threat assessment. The division intelligence apparatus and other command posts are primarily concerned with understanding the enemy in the deep and

close areas. The home station mission command node and the division main command post relied heavily on the rear area assessment provided by the DSB, RCP, and MEB to understand the threat to friendly assets in the rear area. The reliance on these elements allowed the rest of the division to stay focused on the deep and close areas without having to devote additional resources or time to the division's rear area.

- **RCP G-2 roles and responsibilities.** The RCP G-2's responsibilities focused on supporting the RCP staff and providing situational understanding of the threat in the rear area to the Deputy Commanding General–Support. Based on these requirements, the RCP must stay integrated with the other intelligence elements in the rear area to ensure a coherent understanding of the threat. For division battle rhythm events, the RCP G-2 primarily attended the protection working group and protection decision board. One tool the RCP G-2 utilized to better understand the threat in the rear area was the development of the enemy high-payoff target list. This tool was vital as it forced S-2 elements in the rear area to understand the enemy commander's decision points and intent. Based on these two criteria, the G-2 team could identify what friendly assets the enemy commander believed they needed to target to enable mission success. This directly informed the division's prioritized protection list and the allocation of protection assets across the division.
- **DSB S-2 roles and responsibilities.** The DSB S-2 responsibilities focused on providing threat and terrain analysis to main supply routes, alternate supply routes, and current and future sustainment areas including division support areas, logistical support areas, and forward logistics elements through the geospatial team. The two critical products that the 1st Armored Division DSB produced daily included the threat route analysis and the rear area assessment, in coordination with the RCP and MEB teams. The threat route analysis directly informed the division transportation office and its designation of route statuses across the area of operations. The DSB S-2 also participated in the G-2/S-2 synchronization and collection working groups, which allowed us to share our assessments and synchronize collection requests with other units operating in the rear area.
- **MEB roles and responsibilities.** Within the division rear area, an MEB is typically designated with area of operations responsibilities. These rear area control responsibilities include area security, terrain management, information collection, integration and synchronization, civil affairs operations, civil-military operations, psychological operations, movement control, mobility support, clearance of fires, personnel recovery, airspace control, and minimum-essential stability tasks.[7] Aside from its organic capabilities, the MEB can control collection assets. During WFX 25-01, the division provided two Terrestrial Layer Systems in a general support role. The placement and utilization of these assets were critical to identifying enemy special forces locations across the rear area, which informed the MEB commander where to place his resources.

Lessons Learned

Collectively, we learned much from Command Post Exercise III and used those lessons to adjust our approach and enable success for WFX 25-01. We recognized that there should have been better integration with other units in the rear area. Although the RCP, DSB, and MEB S-2 elements established regular touchpoints to share information, most of the engagements with other units operating in the rear area were ad hoc, including those with the combat aviation brigade, division artillery, air defense, and engineer elements. Formally integrating these elements would provide a more holistic understanding of the threat in the rear area and better synchronize assessments across the division. Additionally, including junior intelligence Soldiers in these formal and informal touchpoints would support their development, expose them to unfamiliar resources and information, and help them understand the importance of sharing information across the intelligence warfighting function.

Conclusion

While the division's ability to shape the deep fight sets conditions for brigade combat teams to maneuver in the close fight, the rear area is often overlooked from an enemy perspective. The disparate nature of the rear area creates a challenge for the intelligence enterprise to synchronize assessments and resources to create a single coherent CIP for commanders. During WFX 25-01, intelligence elements in the 1st Armored Division rear area developed a concept of employment that greatly enhanced the understanding of the rear area threat both for the intelligence community and among the staff. This concept included establishing rear area intelligence battle rhythm events, the formation of a rear area intelligence cell, and the clear delineation of roles and responsibilities. Upon implementing this concept, the rear area intelligence team was able to utilize each organization's organic resources to provide a holistic understanding of the rear area CIP and develop lessons learned for future operations. While there is more that can be built upon by future units, the 1st Armored Division intelligence team established a concept that allowed us to create shared understanding across the division intelligence enterprise while enhancing situational awareness for commanders at multiple echelons and command posts.

Endnotes

1. Department of the Army, Army Doctrine Publication 3-0, *Operations* (Government Publishing Office [GPO], 2025), 31.

2. Department of the Army, FM 4-0, *Sustainment Operations* (GPO, 2024), 114.

3. Department of the Army, FM 3-81, *Maneuver Enhancement Brigade* (GPO, 2021), 1-9.

4. Figure 3-5 from Department of the Army, Field Manual (FM) 3-0, *Operations* (GPO, 2025), 77.

5. Department of the Army, FM 2-0, *Intelligence* (GPO, 2023), 3-15.

6. Figure 3-4 from Department of the Army, FM 2-0, *Intelligence*, 3-16.

7. Department of the Army, FM 4-0, *Sustainment Operations*, 114.

MAJ Joseph Marchand is the S-2 for the 1st Armored Division Sustainment Brigade. He has deployed twice to Afghanistan serving as a battalion assistant S-2 and a squadron S-2. He holds a bachelor of science degree in economics from Duquesne University and a master of arts degree in international relations from the University of Oklahoma. MAJ Marchand is a graduate of the U.S. Army Command and General Staff College.

CPT Tommy Milton is an operations officer for the 1st Armored Division G-2 who serves as the G-2's representative to the division tactical command post and rear command post. Prior to serving in 1st Armored Division, CPT Milton served as a combat medic and an infantry officer with a deployment to Afghanistan. He holds a bachelor of science degree in comparative politics from the United States Military Academy.

FRIDAY: UNLOCKING THE POWER OF OPEN-SOURCE INTELLIGENCE FOR A DATA-DRIVEN ARMY

by Colonel Christopher Tomlinson, Chief Warrant Officer 3 Felix Rodriguez Faica, Angela White, and Kathryn Ruhl

Introduction

The modern intelligence landscape is characterized by unprecedented opportunities and challenges. The sheer volume of publicly available information (PAI) and open-source intelligence (OSINT) offers invaluable insights into emerging threats and complex operational environments where collection assets are limited. Effectively harnessing PAI and OSINT at speed and scale requires overcoming significant hurdles, particularly when integrating unclassified information into classified intelligence workflows. To take full advantage of OSINT and enable near-real-time intelligence analysis, the U.S. Army must prioritize both technical interoperability and policy reform to streamline the flow of open-source data into classified analysis.

The FRIDAY project, developed by Southern European Task Force—Africa's (SETAF-AF) Africa Data Science Center (ADSC), enables the seamless and secure movement of OSINT data from the unclassified Non-Secure Internet Protocol Router Network (NIPRNET) to the classified Secret Internet Protocol Router Network (SIPRNET), where analysts can use the data to enhance object-based intelligence production within existing enterprise systems like the Army Intelligence Data Platform (AIDP). Produced through a collaboration between military personnel and civilian data scientists, FRIDAY utilizes a novel data processing capability to overcome interoperability limitations in current intelligence programs of record, enabling a holistic and data-driven approach to intelligence analysis. FRIDAY addresses the critical need for rapid and timely conversion of open-source data into actionable intelligence on classified systems. SETAF-AF is thus empowered to capitalize fully on the wealth of information available in the open-source environment, which ultimately strengthens the overall security posture within its area of responsibility.

Currently, turning raw OSINT data into actionable intelligence objects within AIDP involves a series of multiple handoffs between different teams and systems. This fragmented approach risks creating bottlenecks, increases the potential for errors, and limits the speed and agility of the intelligence cycle. FRIDAY tackles the fragmented multi-domain challenge head-on through a streamlined process using existing government off-the-shelf (GOTS) and commercial off-the-shelf (COTS) systems that are readily accessible to the Army intelligence community. Instead of relying on cumbersome and error-prone manual creation and re-creation, FRIDAY automatically and securely moves OSINT reports from NIPRNET to SIPRNET, eliminating a significant workflow bottleneck for analysts. This not only frees up bandwidth for analysts but also ensures that analysts operating within classified environments have ready access to valuable OSINT insights. Additionally, the FRIDAY project addresses the critical need for secure information sharing between different classification domains using existing enterprise tools with defense and intelligence community standard authentication methods and group- and role-based access controls.

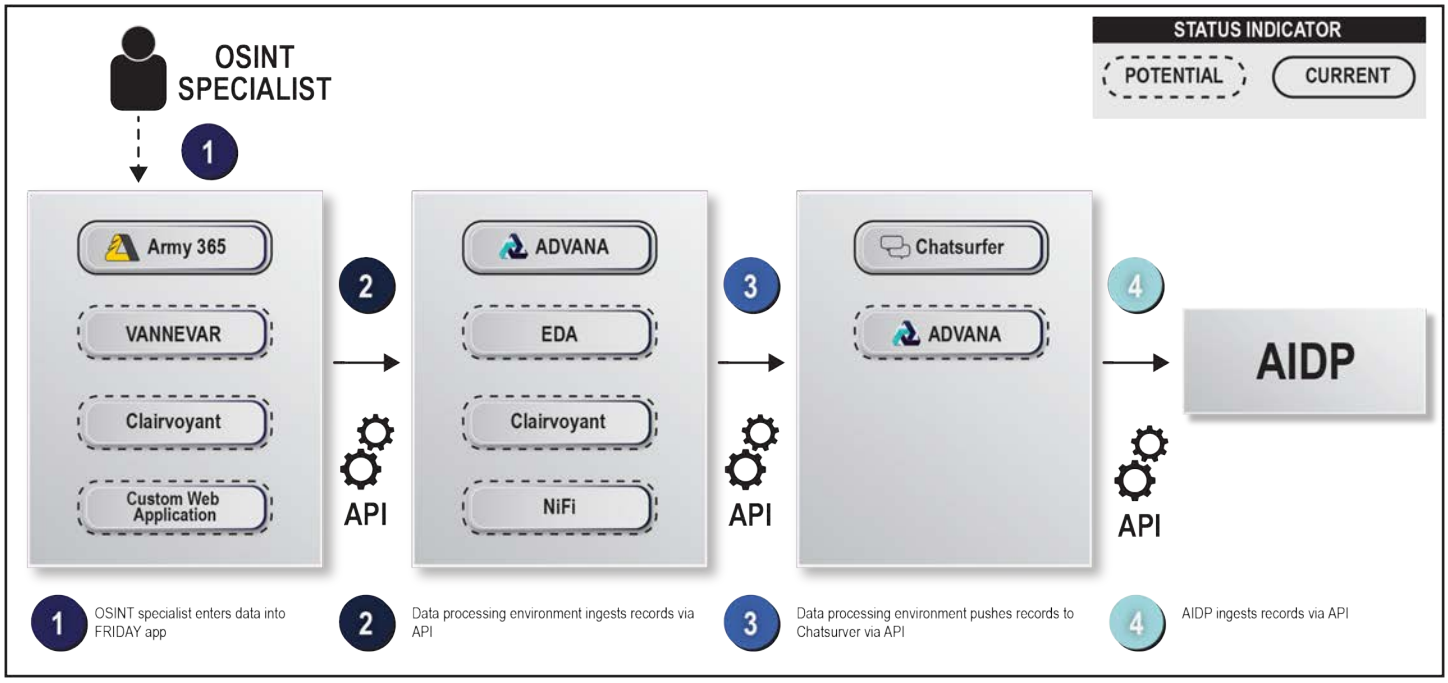


Figure. FRIDAY workflow

As shown in the figure above, FRIDAY is not just a tool but a pipeline that features a user interface for data entry, an environment for data processing, a cross-domain solution, and, at the final step, integration with AIDP. Recognizing that OSINT input often comes in inconsistent formats, FRIDAY implements a crucial step: data normalization. As the OSINT collector enters OSINT reports, FRIDAY standardizes their format. Ensuring data consistency and ontology compatibility regardless of the original source or structure makes the data resistant to "anomalous usage patterns found in intel traffic."[1] Data normalization is a requirement for seamless integration with enterprise tools like AIDP to allow OSINT data to corroborate other sources for intelligence purposes.

Once FRIDAY processes and transfers OSINT data to the SIPRNET environment, it undergoes a crucial transformation into "ontology objects" within AIDP. These objects represent key entities, events, and units extracted from the OSINT reports, and they enrich the existing intelligence picture with valuable insights gleaned from the open-source realm. This object-based approach goes beyond simply adding more data; it connects the dots between seemingly disparate pieces of information. By linking OSINT-derived objects with classified data already present in AIDP, analysts achieve a more comprehensive understanding of the operational environment.

During design and development of the pipeline, ADSC conducted tradeoff analyses and testing with multiple technologies to prototype a solution. Advana, Chat Surfer, and Microsoft Power Platform are already acquired GOTS and COTS systems, allowing ADSC to bring the tool from design to user-acceptance testing in under four months with zero added cost to the organization. While the current implementation (outlined in solid black in the figure referenced by the status indicator) balances robustness and feasibility given the availability of the tools, further iteration and analysis are required to attain long-term viability and scalability.

Ultimately, the goal is to establish near real-time connectivity between open-source information and classified analysis. To unlock FRIDAY's full potential, the U.S. Army must break down the barriers to true interoperability, which present in two categories: technical and procedural. Technical interoperability requires compatible schema definitions, practical ontologies, data governance and security best practices, and avoiding vendor lock-in. Procedural interoperability is sometimes more difficult to achieve. It requires different organizations with idiosyncratic, people-driven processes to design systems using common or compatible technical specifications and to embrace VAULTIS data standards,[2] often entailing daunting cultural shifts on top of technical project setup. Further, organizations must designate stewards to take responsibility for data initiatives beyond initial operating capability and into the maintenance phase.

Compatibility issues in integrating data science and engineering (DS&E) tools with, for example, legacy systems present data formatting discrepancies and security challenges that hinder the smooth exchange of information between new and existing systems. Addressing these interoperability hurdles requires a strategic approach that identifies technical and procedural limitations and deliberately weighs the costs of long-term solutions against the risks and opportunities of short-term workarounds.

While the benefits of integrating DS&E into intelligence workflows are undeniable, we must continue to highlight additional challenges to fully realize its transformative potential. One hurdle is overcoming cultural resistance to new

technologies and approaches. Many intelligence professionals steeped in traditional methods may be hesitant to embrace DS&E, perceiving it as disruptive or overly complex. Therefore, fostering a deeper understanding of DS&E capabilities among both analysts and leadership is crucial.[3] This requires demonstrating the tangible value of DS&E through concrete examples and success stories, highlighting its ability to enhance, not replace, existing expertise.

Conclusion

Finally, building a sustainable pipeline of skilled data science professionals is paramount for long-term success. This requires a multifaceted approach that encompasses targeted training programs for existing intelligence personnel, recruitment efforts aimed at attracting top data science talent, and the establishment of career paths that recognize and reward expertise in both intelligence and DS&E. By investing in workforce development, the intelligence community can ensure it has the skilled personnel necessary to leverage the power of data science effectively for years to come.

Initiatives like FRIDAY demonstrate the transformative potential of DS&E in modernizing intelligence operations, particularly in leveraging the power of OSINT. By examining the factors that inhibit innovation within the enterprise, and encouraging data-driven solutions, the U.S. Army can maintain its strategic advantage in the face of evolving threats and complex operational environments. Continued investment in DS&E infrastructure, training, and research will be critical for ensuring timely, insightful, and actionable intelligence reaches decision-makers at all levels.

Endnotes

1. J. Palmer, "Textually retrieved event analysis toolset," *MILCOM 2005—2005 IEEE Military Communications Conference Vol. 3*, Atlantic City, NJ, 2005, 1679-1685. https://ieeexplore.ieee.org/document/1605916.

2. "VAULTIS" is an acronym for "visible, accessible, understandable, linked, trustworthy, interoperable, and secure." For more information on VAULTIS standards, see Rebecca Sammons, "Laying the Foundation for AI Adoption in the Department of Defense with the VAULTIS Framework," Government Technology Insider, 23 April 2024, https://governmenttechnologyinsider.com/laying-the-foundation-for-ai-adoption-in-the-department-of-defense-with-the-vaultis-framework/.

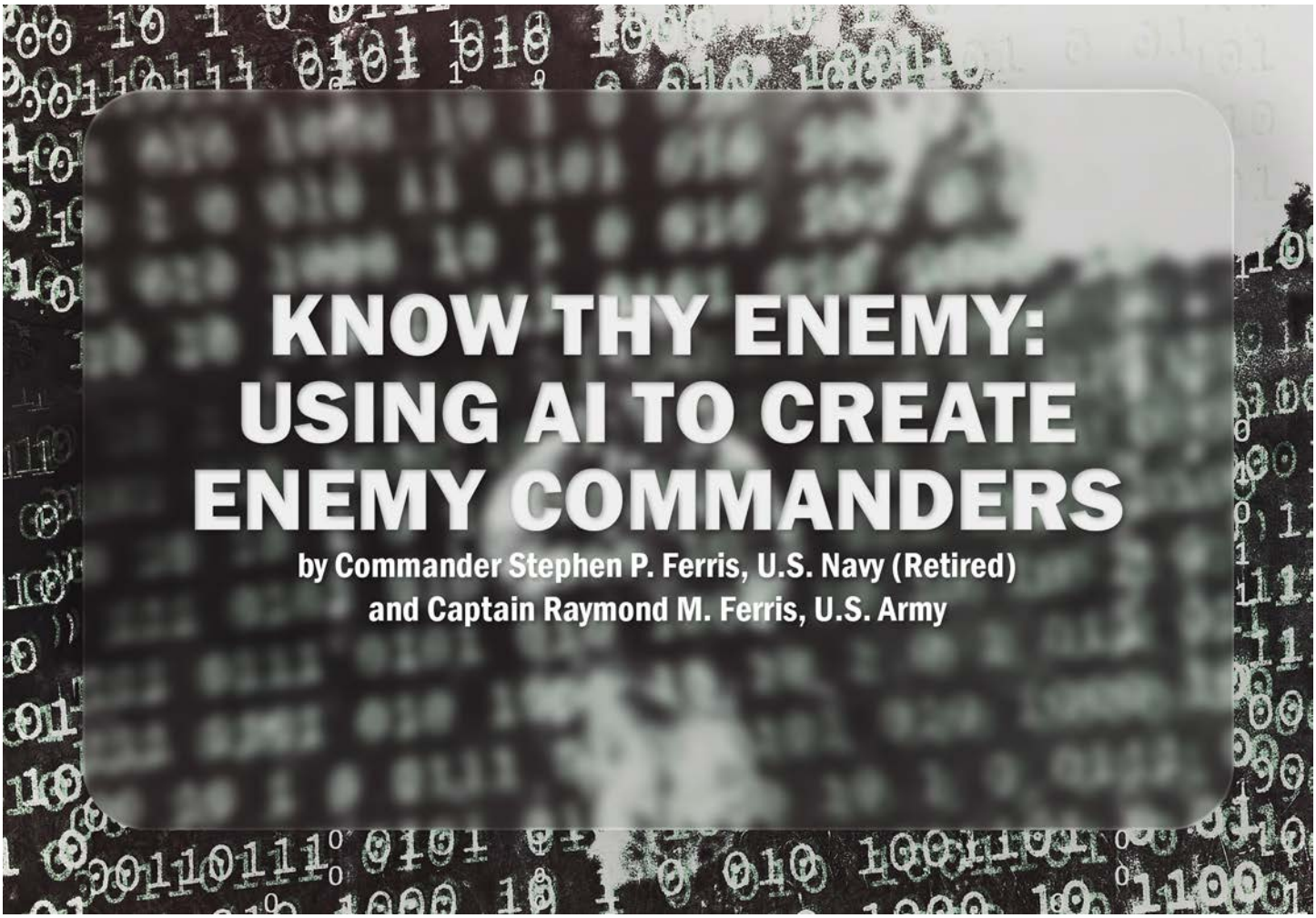
3. Chris Tomlinson, Felix Rodriguez Faica, Ryan Harvey, and Keith Hickman, "Modernizing Intelligence Operations in Africa: Enhancing the Intelligence Cycle through Data Science," *Military Intelligence Professional Bulletin* PB 34-25-1 (January-June 2025), 39-44, https://mipb.ikn.army.mil/issues/jan-jun-2025/modernizing-intelligence-operations-in-africa/.

COL Christopher Tomlinson currently serves as the Director of Intelligence, G-2 for the Southern European Task Force, Africa and is operational director of the Africa Data Science Center for SETAF-AF. His prior intelligence assignments include Director of Intelligence, J-2 Special Operations Joint Task Force—Operation Inherent Resolve, Deputy Director of Intelligence Joint Staff J-2, and Theater ACE Chief USAREUR. He completed a master's in strategic studies from the Marine Corps War College and a BA in political science at Texas Tech University.

CW3 Felix Rodriguez Faica currently serves in the Intelligence Operations Division of the Southern European Task Force, Africa G-2 as an Intelligence Planner and Common Intelligence Picture/Army Intelligence Data Platform lead integrator. His previous assignments were at various unit echelons to include brigade combat team and MI brigade-theater. He received a BA in intelligence studies at American Military University and completed the Digital Intelligence Systems Master Gunner Course.

Angela White is a Data Scientist for the ADSC of the Southern European Task Force, Africa G-2. She previously worked with the Joint Staff Office of the Chief Data Officer to integrate and implement data systems for multiple directorates of the Joint Staff. Before becoming a Data Scientist, Angela studied astrophysics at the University of Pennsylvania and served as an Electronic Warfare Systems Engineer and physicist.

Kathryn Ruhl is a Data Engineer for the Africa Data Science Center. Prior to the ADSC, she worked as a data scientist at the National Geospatial Intelligence Agency and a DevOps engineer deploying various enterprise cloud applications within the IC. Kathryn studied economics at George Mason University and is also a U.S. Marine.



KNOW THY ENEMY: USING AI TO CREATE ENEMY COMMANDERS

by Commander Stephen P. Ferris, U.S. Navy (Retired)
and Captain Raymond M. Ferris, U.S. Army

Introducing the Digital Enemy Commander

Military intelligence faces unprecedented challenges in understanding adversary behavior in this current era of multi-domain warfare. One promising way forward is the use of artificial intelligence (AI), which is rapidly becoming the most transformative technology in military operations since the advent of digital communications, offering unprecedented capabilities to understand enemy intent and predict their behaviors. AI fundamentally reshapes how intelligence officers analyze threats, predict enemy actions, and support their commanders' decision-making. This essay explores a new application of AI for the intelligence officer: the development of an AI persona who can serve as the digital enemy commander or red team. This digital commander can reflect the tactics, strategies, and mindset of the opposing force, allowing intelligence professionals an unprecedented insight into adversary intentions and decisions.

Traditional intelligence analysis faces significant limitations that constrain its effectiveness. Human analysts, despite their expertise and intuition, struggle with inherent cognitive biases which can skew threat assessments and operational recommendations.[1] The information processing capacity of humans becomes increasingly insufficient when confronted with an abundance of data from satellite imagery, signals intelligence, human sources, and open-source materials.[2] Most critically, traditional intelligence methods fail to identify the decision-making patterns of adversaries who operate from fundamentally different cultural, ideological, or strategic frameworks.[3]

The creation of an AI agent who mimics the thinking of an adversary is a significant technological advancement, offering intelligence officers a valuable tool to anticipate enemy behaviors. These sophisticated AI agents can function as digital enemy force commanders, trained on comprehensive datasets of adversary behavior, doctrine, communications, and decision-making patterns. Unlike traditional analysis that simply examines previous enemy actions, these AI agents enable intelligence officers to anticipate the enemy, providing real-time insights into how adversary commanders might respond to dynamic battlefield conditions, strategic pressures, or friendly force actions.

This concept already exists in the private sector with companies employing AI executives or managers to model competitor decision-making processes or regulatory decision making.[4] Companies leverage sophisticated AI systems to analyze executive communication patterns, strategic announcements, and market responses to predict competitor responses. These business applications show the ability of

AI to discover complex human decision-making patterns and predict future actions based on historical data.

The integration of an AI-developed digital commander with current intelligence doctrine and best practices represents an evolutionary leap forward in the practice of military intelligence. These AI systems complement existing doctrinal frameworks by providing dynamic, data-driven insights that augment human analytical judgment. For the intelligence officer, these adversarial agents offer the ability to conduct virtual consultations with the enemy commander and receive an immediate enemy response to a proposed course of action, complete with military reasoning.

Using AI agents to simulate the decision-making of an enemy commander offers substantial benefits. The AI agent's ability to model specific adversarial thought processes, command preferences, and tactical doctrines results in enhanced predictive accuracy. These digital commanders reflect likely enemy responses to friendly force movements by using the cognitive frameworks and strategic priorities of actual opposing leaders. Another benefit is reduced analytical bias: the AI agent has the capacity to think from the adversary's perspective without the constraints of friendly force cultural or doctrinal assumptions. Real-time adaptive modeling allows these digital enemy commanders to evolve their decision-making as new intelligence is collected. This ability to adapt provides intelligence officers with dynamic threat assessments that reflect how adversary commanders might respond to developing situations. Strategic planning also improves through the AI agent's ability to role-play enemy decision-making across multiple military scenarios, resource allocations, and political developments.

"The human element remains critical in final decision-making while AI enhances both the quality and speed of information processing."

Digital Adversaries and Intelligence Doctrine

Current intelligence doctrine emphasizes the analysis of adversary capabilities, intentions, and operational methods through intelligence preparation of the operational environment (IPOE).[5] This analysis of the adversary centers on understanding enemy force structures, operational patterns, decision-making hierarchies, and adaptive capabilities. IPOE focuses on historical precedent analysis, war gaming simulations, cultural and behavioral profiling of enemy leadership, war gaming simulations, and red team exercises.

The U.S. military's red team tradition began with the Army War College's use of opposing forces in the early 1900s, evolved through World War II's strategic war gaming, and was refined during Cold War exercises like REFORGER and ABLE ARCHER.[6] These exercises employed human analysts and military personnel to think and act like enemy commanders. They attempted to replicate adversary decision-making processes, tactical preferences, and strategic posturing. The National Training Center at Fort Irwin institutionalized this approach through the Opposition Forces (OPFOR) program, where American units trained against forces employing Soviet tactics and equipment.

Red force exercises consistently show that human role-players, despite their expertise, face limitations in maintaining adversary perspectives over extended periods. Cultural biases, fatigue, and unconscious adoption of friendly force thinking compromise red team effectiveness.[7] Human cognitive limitations become apparent when processing large datasets from multiple intelligence sources. Time constraints during crisis situations often force analysts to rely on incomplete assessments.

AI adversary agents represent the natural evolution of the use of red force thinking in intelligence assessment. They consistently simulate the enemy's perspective through continuous learning, bias-free analysis, and unlimited processing capacity. AI adversary agents do not suffer the limitations of human red force commanders.

Intelligence doctrine recognizes that military intelligence personnel must continuously adapt their analytical approaches to anticipate adversary actions. Doctrine acknowledges that potential enemies represent sophisticated, thinking opponents with significant capabilities and resources. The existence of these adversaries who creatively respond to our actions necessitates a digital agent to model enemy behaviors in real time.[8]

AI opportunities within existing doctrine focus on areas where human-AI collaboration can enhance analytical capabilities rather than replace human insight. Digital enemy commanders can complement current practices by providing continuous behavioral modeling that updates in real time and processes multi-source intelligence beyond human capacity. They can also identify subtle correlations across vast datasets and generate multiple scenario predictions for strategic planning purposes. Doctrine compatibility ensures that AI agents support rather than supplant human intelligence analysts. The human element remains critical in final decision-making while AI enhances both the quality and speed of information processing.

Technical Foundation and Implementation

Digital enemy commanders represent a specialized application of AI designed to replicate specific enemy decision-making processes and strategic thinking patterns through sophisticated behavioral modeling techniques. These techniques integrate multiple AI technologies such as machine learning algorithms for behavioral pattern recognition, natural language processing for communication analysis, game theory models for strategic decision simulation, and reinforcement learning mechanisms for adaptive behavior modification.

The foundation for AI adversary modeling draws heavily from successful business intelligence applications where AI systems analyze senior executives' behaviors and competitive strategies. The Strategic Consortium of Intelligence Professionals (SCIP), the world's largest global intelligence association with over 15,000 members in 120 countries, emphasizes the growing importance of data-driven competitive intelligence in understanding executive decision-making patterns.[9] Business intelligence practices use AI to model competitor behavior by analyzing communication patterns, press releases, strategic announcements, financial decisions, and operational changes.

Business applications reveal several key insights applicable to military adversary modeling.[10] AI systems excel at identifying subtle patterns in executive communication that human analysts might miss, such as linguistic markers indicating strategic shifts or decision-making stress. Machine learning algorithms can correlate seemingly unrelated data points such as economic indicators, personnel changes, market pressures, and public statements to predict changes in corporate marketing or operational directions. Natural language processing analyzes leadership rhetoric for signals of policy shifts, risk appetite, and strategic priorities.

Training an AI agent to act like an enemy commander requires the collection and analysis of diverse data sources that reveal adversary decision-making patterns. Historical military operations provide foundational training data, including documented enemy tactical decisions, strategic choices, and operational adaptations across various conflict scenarios. Leadership communications, including speeches, military directives, doctrine publications, and strategic guidance documents, indicate cognitive frameworks and operational philosophies. Cultural and ideological materials, such as military education curricula, historical texts, and philosophical or political works that influence enemy thinking, provide essential context for understanding an adversary's worldview.

Intelligence databases containing years of enemy practices, response timelines, and adaptation strategies offer quantitative foundations for behavioral modeling. Economic and political decision-making records show how external pressures influence military choices. Communication patterns reveal leadership interaction styles, decision-making hierarchies, and information flow preferences. Exercise and training records from enemy forces imply preferred tactics, operational concepts, and adaptation capabilities.

Real-time data processing mechanisms employ distributed computing architectures that can scale with intelligence volume and complexity. Historical database integration provides contextual depth by incorporating decades of adversary behavior patterns, enabling digital agents to identify long-term trends and cyclical patterns in enemy decision-making easily overlooked by human observers. Social media and open-source intelligence adds contemporary behavioral indicators that complement traditional intelligence sources.

The computational foundation of digital adversary systems relies on sophisticated decision-making algorithms that enable complex behavioral modeling.[11] Bayesian networks manage uncertainty and probability distributions across multiple scenario possibilities. Neural networks provide complex pattern recognition capabilities for identifying subtle behavioral correlations. Decision trees model tactical choice hierarchies based on adversary doctrine and historical preferences. Monte Carlo simulations generate outcome probability assessments for strategic planning support.

Decision-Making Algorithms Defined

Bayesian Network: A type of graphical model representing probabilistic relationships among a set of variables. A Bayesian network is a visual map of cause-and-effect relationships that assist in making informed predictions.

Neural Network: Unlike Bayesian networks which rely on predefined relationships, neural networks, which are modeled on the human brain, learn relationships directly from raw data. These networks employ interconnected nodes organized into three layers: the input layer receives data; the hidden layer (i.e, the "brains" of the network) processes that data; and the output layer generates a prediction or conclusion.

Decision Tree: One of the most intuitive tools in machine learning, a decision tree is essentially a flowchart using a series of if-then-else rules to predict an outcome. At its simplest, a decision tree breaks complex problems down into smaller, more easily manageable decisions and produces a visual representation of the possible outcomes of each choice.

Monte Carlo simulation: These simulations use probability distributions to solve complex problems by using randomness and repetition to explore many possible outcomes—effectively predicting the future by running "what if" scenarios thousands (or millions) of times to estimate the likelihood of different results.

Behavioral modeling for creating a digital adversary focuses on three primary dimensions: cognitive architecture replication, cultural framework integration, and strategic preference modeling.[12] Cognitive architecture replication involves mapping individual adversary leaders' decision-making patterns, risk tolerance levels, and cognitive biases. For example, an

AI agent might incorporate a specific commander's documented preference for aggressive flanking maneuvers and willingness to accept high casualty rates, thus predicting bold tactical choices over defensive consolidation. Cultural framework integration incorporates social, economic, and political environmental factors that influence adversary behavior. A system modeling a clan-based society leader, for example, would include face-saving requirements, religious calendar constraints, and tribal balance considerations when predicting military decisions. Strategic preference modeling analyzes historical decision patterns to predict future choices under similar circumstances. As an example, an enemy commander who historically reinforces failing positions rather than withdrawing would likely repeat this pattern, allowing the digital adversary to predict the commitment of reserves rather than tactical repositioning.

Applications Across the Threat Spectrum

Digital adversaries demonstrate their versatility across the entire threat spectrum, from immediate tactical challenges to long-term strategic competition. These AI-powered agents adapt their modeling approaches to match the scope and complexity of different operational environments. This section describes how adversary simulation capabilities scale from battlefield-level decision support to national-level strategic planning.

- *Tactical intelligence support* provides immediate operational value through battlefield prediction and counter-strategy development. Unit deployment and movement pattern analysis provided by the digital enemy commander can identify enemy tactical preferences and likely courses of action. Identification of communications and logistics vulnerability reveals weak points in adversary operational systems. Real-time tactical recommendations provide commanders with response options based on evolving battlefield conditions.
- *Crisis response and conflict escalation* scenarios benefit significantly from the modeling of enemy intent. De-escalation strategy development involves predicting adversary responses to various diplomatic and military initiatives. For instance, it might model how a regional power responds to graduated economic sanctions versus immediate military action. Red line identification and boundary testing scenarios help commanders understand adversary tolerance levels and likely escalation triggers. Negotiation strategy optimization provides insights into adversary priorities and acceptable compromise positions. Unintended consequence prediction and mitigation identify potential second- and third-order effects of proposed actions, such as anticipating how arms sales to regional allies might trigger adversary military modernization programs or shift alliance structures.
- *Training and exercise applications* of digital adversaries enhance military preparedness through more realistic adversary simulation. Enhanced red team capabilities provide more sophisticated opposition forces for deployment in military exercises. Realistic adversary behavior simulation creates training scenarios that better prepare personnel for actual combat conditions. Digital enemy commanders can stress the decision-making of friendly forces and create highly challenging scenarios.
- *Counterintelligence operations* gain significant capability with the deployment of a digital enemy commander. This digital enemy acts as a virtual opponent, continuously challenging friendly counterintelligence assessments by simulating hostile intelligence intent and incorporating multi-domain threats. The digital adversary models enemy intelligence collection practices, such as predicting embassy personnel positioning or anticipating coordinated social media strategies. Through adversarial simulation, this digital enemy reveals potential deception campaigns by offering alternative narratives and cross-platform coordination that mirrors actual foreign intelligence behaviors. The virtual opponent validates double agent operations and source reliability by adopting the adversary's perspective to identify operational vulnerabilities and asset compromise indicators. Most critically, the digital enemy commander actively models adversary influence on operational timelines and predicts enemy responses to friendly countermeasures.
- *Strategic intelligence* can incorporate sophisticated digital agents to serve as force multipliers in adversary analysis and long-term planning. By analyzing resource allocation patterns, technology acquisition strategies, and force modernization priorities, digital agents can anticipate how adversaries will evolve militarily over time. This analysis extends beyond hardware to encompass policy and doctrine evolution, forecasting how an adversary's strategic posture might respond to geo-political and military developments.
- *Examining alliance structures and partnership networks* is key to understanding adversary behavior. The digital enemy can describe how adversary coalitions respond to strategic pressures and opportunities, revealing the web of relationships that shape collective decision-making. These agents can explain alliance politics, economic interdependencies, and shared strategic interests that influence how adversary blocs coordinate their responses to external challenges.

The sophistication of these digital agents becomes evident when assessing how economic and political decisions cascade into military action. Digital adversaries can predict the effects of economic sanctions, political transitions, or diplomatic

pressure on enemy military actions or likely countermoves. This capability also allows intelligence officers to anticipate second- and third-order effects before a decision is actually executed, enabling more informed strategic planning.

Mitigation Strategies for Implementation Challenges

Technical limitations present various challenges to adopting adversary digital agents in intelligence operations.[13] Data quality significantly limits AI system accuracy, particularly when historical data is incomplete, fragmented, or unreliable. Computational resource requirements for sophisticated behavioral modeling and prediction can quickly exceed available processing capacity. This is especially true when modeling complex, adaptive adversary networks. Further, model bias and accuracy concerns become critical when training datasets inadequately capture the full spectrum of variability in adversary behavior, tactics, and decision-making processes.

Adversary adaptation and countermeasures pose continual problems to the usefulness of digital adversary effectiveness. Enemies engaged in evasive attacks could attempt to deceive AI systems by developing new types of digital camouflage.[14] Sophisticated adversaries might deliberately alter their behavior patterns to confuse AI agents. Deception campaigns specifically designed to exploit AI vulnerabilities could compromise the accuracy of digital agents. Counter-AI technologies can enable adversaries to identify and neutralize friendly AI capabilities.

Operational challenges can create barriers that complicate the use of digital adversary agents across intelligence organizations. Over-reliance on AI recommendations risks degrading human analytical skills and intuition, potentially creating dangerous dependencies that erode the critical thinking capabilities of human analysts. This concern is compounded by the problem of integration with legacy intelligence systems, which requires new technical resources, specialized expertise, and extensive system modifications. Experienced analysts' resistance to training and adoption can slow implementation even further, as seasoned professionals often cite their own field experience in questioning the usefulness of AI-generated insights. Meanwhile, digital adversaries' real-time processing demands place enormous stress on the existing computing infrastructure, creating bottlenecks that can compromise operational effectiveness during critical intelligence gathering periods.

Human oversight also becomes increasingly difficult when AI agents rely on thousands of data points to draw conclusions, making it nearly impossible for human analysts to verify AI output accuracy.[15] The growing complexity of modern AI systems frequently exceeds human comprehension capabilities, creating significant accountability gaps in intelligence assessment processes. Successful integration, therefore, requires careful consideration of the existing analyst workflow while maintaining human judgment as the ultimate decision-making authority. This ensures that AI enhances rather than replaces human expertise in critical intelligence operations.

Effective mitigation strategies can successfully integrate digital adversary agents into intelligence operations as valuable tools for assessing enemy intentions and likely courses of action.[16] Technical challenges require targeted solutions that ensure system reliability and accuracy. Robust data validation protocols address incomplete historical intelligence by establishing quality thresholds and cross-referencing multiple sources. Classification safeguards prevent inadvertent disclosure by implementing automated security checks and human review processes. Scalable computing architectures accommodate sophisticated behavioral modeling without overwhelming existing infrastructure. Diverse training datasets capture the full spectrum of adversary behavior patterns across operational contexts and geographical regions.

Operational integration demands careful attention to analyst workload and organizational culture. Structured training programs help analysts understand system capabilities and limitations while building confidence in appropriate tool usage. Human-AI collaboration protocols can position digital adversary agents as tools for analytical support rather than decision-making replacements. Experienced analysts maintain primary authority over intelligence assessments while leveraging enhanced processing capabilities for complex pattern recognition. Gradual implementation phases further allow organizations to adapt to this new method of intelligence analysis.

Continuous improvement processes also ensure the long-term effectiveness of digital agents. Regular system updates address evolving adversary tactics and emerging threat patterns. Performance monitoring identifies degradation or potential countermeasures before they impact operations. Feedback mechanisms capture analyst insights to refine system accuracy and usability.

Conclusion

AI is fundamentally transforming how intelligence officers understand, analyze, and predict adversary behavior. This essay focuses on how AI can be used to create digital enemy commanders, providing unprecedented insight into enemy intentions and behaviors. Creation of digital adversary agents represents more than technological advancement; it constitutes a major shift in military intelligence methodology that allows intelligence officers to understand and predict the behavior of enemy commanders.

The development of digital adversary agents offers intelligence officers the capability to engage in virtual consultations with enemy commanders, testing proposed courses of action and receiving immediate adversary responses. This use of AI

enables intelligence professionals to surpass traditional analytical limitations through literal adoption of adversary leaders' mindsets. The intelligence officer gains access to enemy thinking patterns, decision-making processes, and strategic preferences that can be used in real-time.

The implications of digital adversaries extend beyond the immediate tactical advantages they provide to intelligence officers. Intelligence officers supported by a digital enemy commander gain the capability to continuously analyze enemy behavior, predict adversary responses to friendly actions, and identify strategic vulnerabilities often missed by traditional analysis. Digital adversaries allow friendly forces to respond much faster to enemy actions, anticipate enemy intentions more accurately, and develop more effective strategic planning across all levels of military operations.

"As adversaries like China advance their own military AI capabilities, the United States and its allies must leverage these technologies to preserve their intelligence advantages."

The datasets required to develop a digital agent are comprehensive enough to ensure a high degree of reliability for the recommendations that they generate. As they learn through continuous exposure to new intelligence inputs and validation against actual enemy behavior, these digital agents become increasingly sophisticated representations of adversary command thinking.

For the modern intelligence officer, digital adversary agents represent an indispensable tool for achieving analytical superiority in the global security environment. As adversaries like China advance their own military AI capabilities, the United States and its allies must leverage these technologies to preserve their intelligence advantages. The integration of digital agents with intelligence doctrine provides a foundation for revolutionary improvements in understanding and countering enemy threats.

The future of military intelligence lies in the integration of human expertise with AI capabilities.[17] The intelligence officer is the interface between the insights of the digital adversary and command decision-making. Digital enemy commanders will become essential tools in the intelligence officer's tool set. They will provide new capabilities to anticipate an adversary's thinking and to predict enemy actions at a level of accuracy impossible with traditional intelligence analysis. This transformation positions military intelligence at the forefront of the technological innovations that will shape the future of 21st century warfare.

Endnotes

1. Amos Tversky and Daniel Kahneman, "Judgment under Uncertainty: Heuristics and Biases," *Science* 185, no. 4157 (27 September 1974), 1124-1131, https://www.science.org/doi/10.1126/science.185.4157.1124. Human decision-making is systematically influenced by numerous cognitive biases that can lead to errors in judgment and analysis. Kahneman and Tversky's foundational research identified key heuristics including confirmation bias (seeking or giving undue weight to information that confirms existing beliefs), availability heuristic (overweighting easily recalled information), and representativeness heuristic (judging probability by similarity to mental prototypes); Daniel Kahneman, *Thinking, fast and slow* (Farrar, Straus and Giroux, 02 April 2013). Additional biases include anchoring (over-relying on first information), overconfidence in one's abilities, loss aversion, and framing effects, which Kahneman later synthesized in his comprehensive analysis of dual-process thinking; Thomas Gilovich, Dale Griffin, and Daniel Kahneman, eds., Heuristics and Biases: The Psychology of Intuitive Judgment (Cambridge University Press, 08 July 2022). These systematic deviations from rational decision-making models demonstrate how intuitive judgment often leads to predictable errors.

2. Herbert A. Simon, "A behavioral model of rational choice," *The Quarterly Journal of Economics* 69, no. 1 (February 1955), 99-118, https://doi.org/10.2307/1884852. Human cognitive processing is constrained by limited attention, memory, and computational capacity, leading to systematic biases and heuristic-based decision-making rather than optimal choices.

3. David Robson, "How East and West think in profoundly different ways," *BBC*, 19 January 2017, https://www.bbc.com/future/article/20170118-how-east-and-west-think-in-profoundly-different-ways.

4. Pratik Kothari and Stephen P. Ferris, "Strategic Generosity: The Business of Political Contributions," *Social Science Research Network Electronic Journal* (28 April 2025), https://dx.doi.org/10.2139/ssrn.5241811. The authors use a sample of 4,949 digital corporate executives and find that executives primarily view political contributions as strategic investments that extract economic value and secure critical information to navigate policy landscapes.

5. Headquarters Department of the Army, Field Manual (FM) 2-0, *Intelligence* (Government Publishing Office, 01 October 2023). IPOE is defined here as "the systematic process of analyzing the mission variables of enemy, terrain, weather and civil considerations in an area of interest to determine their effect on operations." The name change from "intelligence preparation of the battlefield" to "intelligence preparation of the operational environment" better reflects the multidomain nature of the operational environment.

6. David Alan Rosenberg, "Being 'Red:' The Challenge of Taking the Soviet Side in War Games at the Naval War College," *Naval War College Review* 41, no. 1 (Winter 1988): 81-93, https://digital-commons.usnwc.edu/nwc-review/vol41/iss1/7/; Micah Zenko, *Red Team: How to Succeed By Thinking Like the Enemy* (Basic Books, 2015).

7. Headquarters Department of the Army, *The Red Teaming Handbook*, 9th ed. (U.S. Army, 2024, distribution limited).

8. FM 2-0, *Intelligence*, 1-1—2-35.

9. "Strategic Consortium of Intelligence Professionals (SCIP)," SCIP, https://www.scip.org/. Originally called the Society of Competitive Intelligence Professionals, SCIP was founded in 1986 to promote competitive, market, and strategic intelligence practices in enterprise, academia, and government. This nonprofit organization provides education, certification programs, networking opportunities, and best practices for legal and ethical business intelligence collection and analysis, serving as the premier advocate for intelligence-driven decision-making.

10. Pratik Kothari and Stephen P. Ferris, "Personality-Driven Procurement: AI Executives and Strategies for Federal Contracting" (Working Paper, University of North Texas, 2025). While Kothari and Farris (2025) focus on strategies followed by CEOs to gain advantages in the federal contracting process, in this paper the authors survey a sample of digital CEOs to understand the reasons for corporate donations to political candidates.

11. Stuart Russell and Peter Norvig, *Artificial Intelligence: A Modern Approach*, 4th ed. (Pearson, 08 May 2020).

12. Iuliia Kotseruba and John K. Tsotsos, "40 Years of Cognitive Architectures: Core Cognitive Abilities and Practical Applications," *Artificial Intelligence Review* 53, no. 1 (2020), 17-94, https://psycnet.apa.org/doi/10.1007/s10462-018-9646-y; Aaron J. Barnes, YuanYuan Zhang, and Ana Valenzuela, "AI and Culture: Culturally Dependent Responses to AI Systems," *Current Opinion in Psychology* 58 (August 2024), https://doi.org/10.1016/j.copsyc.2024.101838.

13. Adib Bin Rashid, Ashfakul Karim Kausik, Ahamed Al Hassan Sunny, and Mehedy Hassan Bappy, "Artificial Intelligence in the Military: An Overview of the Capabilities, Applications, and Challenges," *International Journal of Intelligent Systems 2023*, no.1 (2023), http://dx.doi.org/10.1155/2023/8676366.

14. Digital camouflage involves masking authentic signals, communications patterns, and behavioral signatures to deceive adversary AI systems and digital personas. Techniques include spoofing metadata, generating synthetic noise, mimicking benign traffic patterns, and creating false digital footprints that obscure genuine operational activities from automated detection and analysis algorithms.

15. Yavar Bathaee, "The Artificial Intelligence Black Box and the Failure of Intent and Causation," *Harvard Journal of Law & Technology* 31, no. 2 (Spring 2018), 889-938, https://jolt.law.harvard.edu/assets/articlePDFs/v31/The-Artificial-Intelligence-Black-Box-and-the-Failure-of-Intent-and-Causation-Yavar-Bathaee.pdf.

16. Anthony King, "Digital Targeting: Artificial Intelligence, Data, and Military Intelligence," *Journal of Global Security Studies* 9, no. 2 (June 2024), https://doi.org/10.1093/jogss/ogae009.

17. Michael Mayer, "Trusting Machine Intelligence: Artificial Intelligence and Human-Autonomy Teaming in Military Operations," *Defense & Security Analysis* 39, no. 4 (2023), 521-538, https://doi.org/10.1080/14751798.2023.2264070.

CDR Stephen Ferris (retired) is a professor of finance at the University of North Texas. He holds a bachelor of arts from Duquesne University, a master of business administration and a doctorate from the University of Pittsburgh, and a master's degree in strategic studies from the U.S. Army War College. He also holds diplomas from the U.S. Army's Command and General Staff College and the U.S. Navy's College of Naval Command and Staff. His last active-duty assignment was with the J-4 on the Joint Staff.

CPT Raymond Ferris is the counterintelligence operations officer for 2nd Military Intelligence (MI) Battalion, 66th MI Brigade (Theater). He previously served as assistant S-2 for the 1st Armored Division, Division Artillery and as the company executive officer for Bravo Company, 532nd MI Battalion, 501st MI Brigade (Theater).


MIL.RU PHOTO

BEYOND THE COUNT: BDA FOR MODERN WARFARE

BY MAJOR JEFFREY D. WEGMEYER

Introduction

Techniques for conducting battle damage assessments (BDA) during large scale combat operations (LSCO) are sorely lacking in current doctrine. On the surface it seems easy: count what you killed so you know what the enemy has left. Unfortunately, the nuances and complexities of a modern battlefield make this seemingly simple process extremely difficult, especially given minimal doctrinal references. Additionally, U.S. forces have not participated in LSCO in decades, so native institutional knowledge is also lacking. Units have endeavored to piece together BDA teams and solutions, but they all struggle. This paper is designed to set a common baseline for considerations for a division or corps to conduct BDA effectively in an LSCO fight. The principles we observe through simulated battles during Warfighter exercises are equally effective in true conflict.

Pre-Conflict: Build Your Team and Establish Your Process

Roles and Responsibilities. Regardless of echelon, internal roles and responsibilities must be explained thoroughly in a unit's standard operating procedure (SOP). Since division- and corps-level BDA teams are often pieced together from external organizations using, for example, a mobilized reserve component or expeditionary military intelligence brigade personnel, having a clear explanation of their roles and responsibilities upon their arrival in theater is critical to starting strong and minimizing the initial lag that occurs when taking on a new, unfamiliar role. Who provides the collected BDA? Where is it collected? How is the collected data processed? What are the required end products and assessments?

In addition to their standard internal roles, units must explicitly task subordinates with specific responsibilities within the BDA process: corps must direct divisions; divisions must direct brigades; and so on. Failure to provide explicit direction results in duplicated effort and wasted manpower—or, worse, units failing to deliver reports because each echelon assumed it was the responsibility of the other. Both are extremely common pitfalls in Warfighter exercises. Ideally, subordinate responsibilities within the BDA process are published in an operation order, which ensures both organizations clearly understand what is expected and have a reference document, as opposed to relying on a more informal email or verbal conversation.

Units must understand how organizations outside of their control—such as higher headquarters (HHQ), adjacent units, other services, and partner nations—publish BDA, where it is published, how frequently it is disseminated, and how they can incorporate each organization's information into their own BDA processes. This information should be recorded and reviewed regularly for accuracy to prevent inaccurate enemy assessments as the result of incomplete reporting. Most significantly, a specific unit member should be tasked to collect that data and incorporate it into the unit's overall assessment. Keep in mind that allies' BDA may be collected through a liaison or a Security Force Assistance Brigade, not directly from the ally's military force. This information is best captured by stating it clearly within the internal roles and

responsibilities discussed previously. For example: 1) BDA analyst #1 is responsible for collecting Air Force BDA every four hours from portal folder YYY at https://abcd.com; that information should be copied into the unit BDA tracker. 2) BDA analyst #2 is responsible for pulling country M's BDA from chat room XYZ at least once an hour and adding it to the unit's BDA tracker.

Units often conduct sensor-to-shooter technical rehearsals prior to Warfighter exercises. During these rehearsals, units practice receiving reports from a variety of sources, from signals intelligence to full motion video to counterfire radars. Those reports are then processed through the fires channel until a fire mission is executed. A similar rehearsal would be helpful for BDA teams. Overlapping responsibilities can make the BDA process particularly challenging, however, so if possible BDA teams from different echelons should meet to talk through as many different vignettes as possible to clarify responsibilities.

Collection and Dissemination Procedures. With roles and responsibilities established, the next step is to create formats and procedures for collecting BDA from across the battlefield. Units should designate a standard BDA reporting format to ensure not only that reporting is limited to the relevant information, but also to forestall the necessity of interpreting multiple different formats before the battlefield can be assessed productively. Ideally, the chosen format will be mirrored as closely as possible in the requirements from HHQ to minimize reformatting. And once a format is established for subordinates, its use *must* be enforced!

Once the format is standardized, reporting timelines must be established and enforced as well. Not all units will require the same timeline. For example, ground maneuver elements regularly in contact with the enemy along the forward line of own troops (FLOT) may provide updates every four to six hours, while an element operating in the rear area only provides an update once a day. Fires elements may provide updates more or less frequently depending on their operational tempo, but elements focused on the destruction of high payoff target systems should prepare much more frequent updates. Aviation brigades engaged exclusively in deep attacks may need to provide just a single update after each mission, while aviation support along the FLOT may require more regular updates. The takeaway here is that there is no one-size-fits-all solution—each subordinate unit must have a function-specific timeline.

Collecting BDA from external sources is more typical at echelons corps and above, but there may be special situations where lower echelon units should consider some of these sources. For example, Air Force strikes or allied operations occurring within a division's area of operations (AO) could be tallied by the division before submission to Corps, but that should be deconflicted with Corps before operations commence to prevent duplicate reporting.

Once BDA is collected and processed from all applicable sources, the unit must disseminate a consolidated BDA product back out to its HHQ, subordinates, and adjacent units. This allows those elements to refine their understanding of the enemy's remaining capabilities. Reports should be sent on a system and in a format that everyone, especially all subordinate units, can use. An assessment disseminated on the Secure Internet Protocol Router, for example, offers no benefit for allies who can only access the Mission Partner Environment; likewise, an assessment posted to the MAVEN Smart System does not help a subordinate who works in the Command Post Computing Environment but has no MAVEN account.

Finally, all collection and dissemination processes need an established and tested Primary, Alternate, Contingency, and Emergency plan, known as a PACE plan. How deep that plan goes will be based on how much risk the unit is willing to accept, but at the very least it must include contingencies that preserve the ability to assess enemy capabilities at all times.

Working groups and quality control are essential due to the ambiguities inherent in basing enemy capabilities assessments on a wide variety of battle damage reports. Some disagreement between units and echelons about what remains on the battlefield is inevitable; those differences should be resolved within the intelligence warfighting function into a single, cohesive narrative that allows all G-2s to brief the same overall assessment to commanders. Whether BDA discussions happen in a separate BDA working group or as part of the intelligence synchronization meeting, the important thing is that the discussions happen.

As units build trust across the team by identifying and resolving differences in these working groups, there must also be an element of quality control at various points in the process. Remember that high quality BDA reporting enables high quality results and assessments. Divisions should provide quality data consistently, which allows corps to trust divisions' assessments without rechecking their work. The same standard applies from divisions down to brigades. When subordinates report incomplete grids or misidentify equipment in enemy formations, their HHQ loses trust and is forced to check their work, resulting in wasted time and manpower. Before submitting BDA reports, each unit needs to validate both the integrity of their data *and* their assessment of it. Destroyed equipment should be associated with an appropriate enemy unit based on order of battle and location on the battlefield. If incomplete data is received from external organizations such as special operations forces or other services, someone must be tasked to investigate and correct that data. For example, if division artillery (DIVARTY) reports killing 6x multi-launch

Soldiers attack their objective during aerial insertion and battle damage assessment training at the Cincu Training Center, Romania. (U.S. Army photo)

rocket systems, that's not enough information. Either the unit needs to return to DIVARTY for confirmation of the specific system destroyed, or the unit must determine the specific system(s) based on the location of the battlefield. A report cannot simply be discarded if it is incomplete.

Initial Assessment and Ongoing Updates

Understanding how the enemy employs its key systems is critical to identifying which systems matter at each echelon, where to focus BDA tasks for each echelon, and how to weight the effort of the BDA team. The opposing force confronted during a Warfighter exercise will be equipped and organized differently from our real-world adversaries, so it is important to evaluate and understand the enemy in each situation. How the enemy employs its systems will also change over time. For example, fires assets initially employed as battalions may be forced to start operating as batteries, or batteries may have to operate as sections, as attrition takes its toll. The number of air defense systems per radar may increase or decrease in response to battlefield successes or defeats.

Continually assessing how the enemy employs its systems will inform the BDA plan. The type and number of systems a unit targets will change as the enemy adjusts its tactics, techniques, and procedures. One day BDA analysts may be looking for 6-plus systems in formation, while the next day the target has changed to 1 or 2 systems operating independently. The "so what" of the battle damage assessment will also change from day to day. One day, destroying 10x artillery pieces may take out less than 10% of its capability, while a few days later, destroying the same amount of equipment may completely remove the enemy's ability to affect a critical operation and force their commander to reposition assets or commit his reserve.

Understanding the enemy also refines the high-payoff target list (HPTL) to prioritize high-value munitions appropriately. During a Warfighter exercise, the enemy will have 6 or more different air defense systems enabled by 8 or more different radars, totaling hundreds of pieces of equipment. A corps' HPTL that includes simply "air defense" will result in targeting many systems that should not be a corps problem, ultimately wasting hundreds of precision munitions. HPTLs should be refined properly to classify targets carefully, then delegated to the appropriate echelon for disposition. Targeting efforts should then be focused accordingly.

Accounting for the enemy's deception operations, decoys, repairs, reinforcements, and replacements for BDA purposes is the most difficult part of understanding the enemy. Each of these factors is important and must be taken into account when formulating BDA. Often, initial assessments may simply acknowledge an "intelligence gap" and apportion assets to collect against that gap. Later, as intelligence is refined, the unit can begin to understand how widespread enemy decoys are, how quickly they can repair damaged systems, and when/where reinforcements are employed. The BDA team can then incorporate this updated intelligence and adjust their assessment.

Of note, identifying and accounting for enemy decoys is one area where units will see incredible divergence between Warfighter exercises and real-world combat. Many real-world systems and capabilities that help us identify decoys simply cannot be replicated in our current simulated environment.

So, while decoys must be identified in both situations, the final methodology and results used in each will be dramatically different. It is important to remain fluid. Many of these aspects of understanding the enemy will change as the battlefield changes. It is vital that units begin operations with an initial enemy assessment but regularly update that assessment based on the many rapid changes that inevitably occur across the battlespace.

During Conflict

Have an Adaptive Plan for BDA Collection and Targeting. With a clear understanding of the enemy and high-payoff targets selected, the targeting team and the collection team can begin their process of detecting and delivering appropriate effects against those targets. It is critical that BDA is deliberately apportioned as part of the collection plan; otherwise, munitions and other effects will be expended without a clear method for determining effectiveness. The planned BDA must then be executed. This seems like it should go without saying, but often units are unable to confirm target destruction because the necessary collection assets have been redirected. The second critical requirement of BDA collection is ensuring that someone is tasked with processing, exploitation, and dissemination (PED) of collected data. If an asset records an image of a location or tracks a signal for BDA purposes, someone must execute the PED to ensure the results are included in the unit's BDA summary. The final, and often most overlooked, aspect of BDA collection is the use of non-imagery assets. While units are usually capable of successfully planning for full motion video or other imagery of enemy systems, they often overlook other means to confirm the destruction of enemy systems. Counterfire radars, ground moving target indication, and signals intelligence are all effective ways to assess destruction of systems. When the enemy stops shooting, moving or communicating, it signals success that must be assessed, even if there is no image of a burning hulk.

Once a collection plan is created and executed with dedicated PED support, units often find that duplicate reporting can occur as responsibilities overlap on a complicated battlefield. A target destroyed by fires elements, in support of an aviation brigade, operating within a division battlespace, could be reported by all three of those elements. Attack aviation engaging targets along the front line could have their targets reported by active ground elements in the same area. Imagery analysts pulling destroyed equipment reports from routine sources could include equipment already reported destroyed by the Air Force. These conflicts can be mitigated with extremely thorough roles and responsibilities—however, there will always be unique situations that warrant implementing a method to identify and remove duplicate reporting. A combination of grid comparisons and a visual overlay of BDA reporting is recommended; this will identify not only exact duplicates but also those that are slightly offset.

As an effective collection plan identifies targets for destruction, the unit also needs targeting goals tied to critical events, decision points, or triggers. Targeting projections should be based on targeting plans; however, units often struggle to project future BDA that drives those assessments and informs operations planning effectively. Instead of projecting BDA based on which enemy systems are the targeting priorities for each day, units typically default to a standard daily degradation of 10% to 20%. By synchronizing targeting goals closely with targeting projections, units can effectively plan and assess operations to ensure progress and alignment with goals. For example, an operation may require destruction of 20x artillery systems and 8x multiple rocket launch systems (MRLS) in a certain section of the battlefield. Given its available collection assets to detect and precision munitions on hand to deliver, the unit may have a targeting projection of 10x artillery systems and 4x MRL systems per day. At the end of Day One of operations, the unit could assess whether they met their targeting projection, whether they are on track to meet their overall goal on Day Two, and, if not, whether they need to adjust the timeline of their operation.

Create an Assessment. When all the numbers have been crunched and the unit knows how many enemy systems remain, they can move on to the actual assessment, which is the part of the BDA process that provides the most value to other staff sections. As the product that informs the commander's decision-making, this is the most important part of the process. Accurate data is not helpful unless it is turned into information and then distilled into knowledge. Units often get caught up in reporting the number of systems killed but never get around to discussing the "so what" of a true assessment. Stating that "12x 9A52s were destroyed" does not help a commander nearly as much as "we have destroyed half of the enemy's long-range rocket capability in 12th DIV's AO. This forces the enemy commander to reposition fires assets and gives U.S. forces fires overmatch for the next 24 hours."

Things to consider when drafting an assessment include: what was the effect on a specific enemy capability—i.e. half destroyed, no longer combat effective, forced to operate as sections instead of batteries? Is there a gap on the battlefield now? How long will it take the enemy to adjust? Was an enemy decision point triggered? Was the enemy forced to modify its COA? Some of these assessments can be done by the BDA team, while others will require input from fusion analysts with better knowledge of enemy actions. Some assessment sections may require input from specialists in other warfighting functions; for example, the protection team may need to provide information about how the enemy air defenses might adjust coverage after certain losses.

Units also need to consider how they are going to assess non-kinetic effects. Many of the same considerations come into play here, such as how an enemy's capability was affected, how long the effect will last, or how the enemy will adjust; nevertheless, this can be more complicated than assessing kinetic effects. For an accurate understanding of non-kinetic effects so an accurate assessment can be included in their product, BDA teams will need to work closely with the specialty staff sections that coordinate non-lethal effects.

To facilitate understanding of the written assessment, it is helpful to include some sort of visualization. The format for that visualization will depend on how the unit commander assimilates information most effectively. There are a variety of options, e.g. kill charts, color coded percentages, bar charts, or pie charts. Some units utilize a map overlay, while others use a simple cartoon sketch with minimal operations graphics and a few major phase lines. The specific format is far less important than ensuring the commander receives a complete, accurate assessment in a timely manner. The commander thus has the necessary tools to make informed decisions and plan operations against a clear understanding of what enemy capabilities remain on the battlefield and their locations.

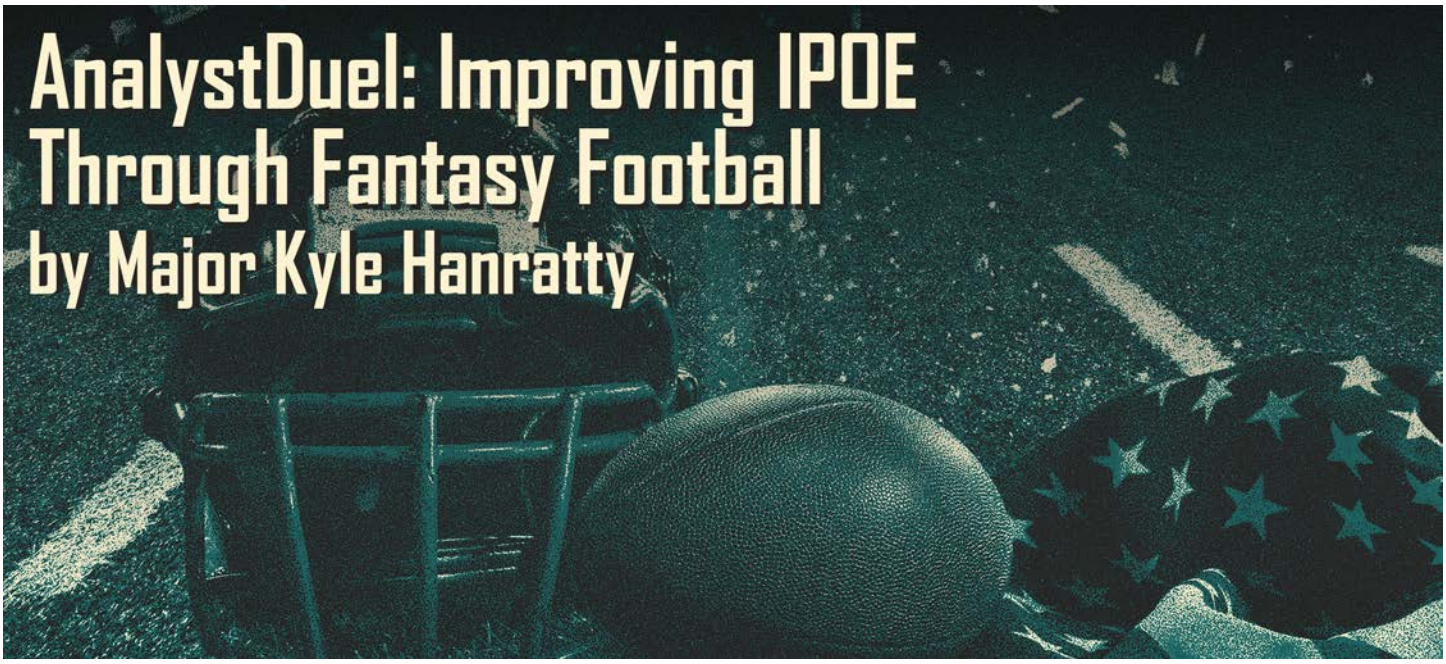
Conclusion

Despite its apparent simplicity, the process of assessing battle damage to produce effective BDAs presents significant complexities. Although doctrine does not currently outline BDA processes for division and corps echelons, commanders still require comprehensive reporting. A thoroughly planned process that clearly outlines roles and responsibilities, combined with a trained and adaptive team, ensures efficient and effective BDA during LSCO. This in turn informs better planning and decision making—and that leads to a more lethal force.

MAJ Jeff Wegmeyer is currently assigned as an Intelligence OC/T at the Mission Command Training Program. Since arriving at MCTP, MAJ Wegmeyer has supported multiple Warfighters and ASCC-level exercises, focusing for the past two years on coaching BDA teams on systems and processes. Previous assignments include 1st Infantry Division, ARCYBER, 25th Infantry Division, USARPAC, and 4th Infantry Division, plus one combat tour in Afghanistan and a non-combat tour to Europe.

AnalystDuel: Improving IPOE Through Fantasy Football

by Major Kyle Hanratty



"SOMEONE FIND THE S-2," bellowed the Commander from behind his computer screen. Entering the room a few moments later, the S-2 found the Commander pacing, uncharacteristically nervous.

"Sir?"

The Commander raised his head and addressed the S-2 directly. "You're the best chance we've got, Deuce. Help me understand what we're up against."

"Stop worrying, sir," the S-2 replied confidently. "I've been looking at this all week, and we can win this."

The S-2 launched into a description of the degrading weather conditions and their impact on both sides' aerial capabilities, then spoke about the effect the elevation would have on either formation's endurance. He wrapped up his briefing by explaining that attacking the adversary where they're weakest and exploiting existing intel about their plans would confer a significant advantage and virtually guarantee success.

The S-2 paused to allow the Commander a moment to digest this information. The Commander grimaced. "I want to make sure I fully understand what you're recommending. Do you really think starting Jayden Daniels at quarterback over Jalen Hurts is the right move?!"

"Sir, that's exactly what I recommend. Hurts is playing in Denver, which will be a snowy, blustery mess. Daniels is playing in a dome against the Saints, who lost both of their starting cornerbacks and are weak against rushing quarterbacks."

"Excellent analysis, Two. I simply could never imagine not starting a Pro Bowler like Hurts."

And with that, the Commander completed his lineup and hit SEND.

Introduction

Some analyses are more consequential than others—but the underlying principles remain the same. S-2s often bemoan their difficulties in training analysts to conduct quality intelligence preparation of the operational environment (IPOE). It's not news that IPOE requires a clear understanding of terrain analysis, threat system capabilities, and tactics. However, the patterns of thought and habits of mind required to produce useful IPOE products—that is, transforming disparate data sets (steps 1-3) into a cohesive narrative (step 4) to drive operational recommendations—are strikingly similar to those needed to win at fantasy football. Ultimately, the difference between good IPOE versus *great* IPOE—or winning versus losing at fantasy football—is found in the quality of the recommendations drawn from the analysis.

Still skeptical? Stick with me. Using a combination of real-world vignettes and practical applications, hopefully (for your analysts' sake), I can convince you not just to put away the Distributed Common Ground System next season and improve your section, but to do it in a much more enjoyable manner.

Vignette 1: IPOE Steps 1 and 2

The impacts of terrain and weather on military operations are undeniable. Lieutenant Meehan's iconic proclamation in *Band of Brothers* captured this succinctly: "The Channel coast is socked in with rain and fog! High winds on the drop zone! No jump tonight!" IPOE steps 1 and 2 (*Define the Operational Environment* and *Describe the Environmental Effects on Operations*) enable the Commander and staff to translate these advantages and disadvantages into operational recommendations. This logic translates well from the battlefield to the football field.

Perhaps the most telling example where steps 1 and 2 led to fantasy victories was the December 6, 2021, showdown in Buffalo, NY between the New England Patriots and Buffalo Bills. On the surface, a game featuring Josh Allen (a future Hall of Famer) and Mac Jones (a Heisman Trophy runner-up) looked like a shootout. Leading up to the contest, Allen and Jones averaged 272 and 238 passing yards per week, respectively. In fact, in just the prior week alone Jones threw for 310 yards. The weather, however, dramatically changed this analysis.

The forecast in Buffalo called for winds gusting to 55 miles an hour and a wind chill of -4 degrees Fahrenheit. With that intelligence at hand, an analyst could use IPOE to make several recommendations: First, passing in those conditions seems nearly impossible, so consider benching both quarterbacks. Second, because the teams must prioritize the run game, consider starting the second string running back. Finally, the game is likely to be a messy, low-scoring affair, so consider starting either of the defenses.

In execution, the game was a defensive struggle, but the Patriots ultimately triumphed with a final score of 14-10. The Patriots' Mac Jones threw a total of three passing attempts for 19 yards. Meanwhile, Harris totaled 111 yards on 10 carries, in addition to the starting running back, Rhamondre Stevenson, gaining 189 yards in 24 carries. On the other side of the ball, The Bills' Josh Allen fared slightly better than his counterpart, with 15 completions for 145 yards—but he only completed 50% of his passes. Fantasy team owners who considered IPOE steps 1 and 2 might have seen this coming.

There are countless examples demonstrating the value of IPOE-style analysis. For a simple and more recent example, consider Josh Allen's game-day performance on indoor fields. Analysis before the Patriots' December 15, 2024 game against the Detroit Lions revealed that in seven previous dome games, Allen's record was 6-1 with 20 total touchdowns (15 thrown and 5 rushing). Moreover, in a league with an average passer rating of about 90, Allen's rating is 119. In the December 15 game, Allen threw for 362 yards with 2 touchdowns, plus an additional 2 rushing touchdowns, giving him a passer rating of 122 for that game alone. While correlation does not prove causation, the value of analyzing the operational environment in fantasy football seems obvious.

Putting It into Practice

S-2s are often teased as the staff's "weatherman." But think about it: how often has an S-2 briefed weather effects like the local news station? S-2 reports typically sound like this: "Sir, the high for tomorrow will be 52 with a low of 28. There will be a moderate cloud cover through the early evening. Oh, also, illumination will be 76% tomorrow night." The Commander (and staff) are left doing the mental gymnastics to tease out why any of that matters. This analysis is akin to seeing the weather report for the Bills-Patriots game and thinking simply, "wow, I'm glad I'm not playing in that weather!"

Commanders need an S-2 with enough analytical insight to say, "Sir, no significant impacts to operations tomorrow morning. However, the combination of freezing temperatures and cloud cover in the early evening may restrict our ability to utilize unmanned aerial systems as the Battalion moves to its attack positions. Moreover, while illumination is 76%, the moon will set at 2230 and leave 8 hours of total darkness until sunrise at 0630. I recommend adjusting our line of departure to midnight to exploit the cover of darkness and increase the likelihood of support from unmanned systems." This data→analysis→conclusion→recommendation methodology is analogous to not starting the quarterback in a game being played in subzero temperatures with 55-mile-per-hour winds.

Vignette 2: IPOE Step 3 and 4

In IPOE steps 3 and 4 (*Evaluate the Threat* and *Determine Threat Courses of Action* [COAs]), analysts seek to understand the threat's capabilities and translate these into predictive analysis of how those capabilities will be employed. This process includes an analysis of threat composition, disposition, and strengths, identifying high-value targets (HVTs), and understanding threat tactics. Once again, football presents a similar dynamic.

NFL teams publish an injury report each week to capture which players are active, questionable or doubtful to play, or out completely. This report is mirrored in an analysis of battle damage assessment of a threat's order of battle. After identifying unavailable assets (i.e., players), an analyst must forecast the impact of their absence.

The 2024 Tampa Bay Buccaneers ("the Bucs") game versus the Las Vegas Raiders provides dramatic examples. On October 13, the Bucs lost Mike Evans and Chris Godwin, their top two starting wide receivers, to injury. Two days later the Raiders traded *their* top wide receiver, Devante Adams, to the New York Jets. In evaluating this "threat," Evans, Godwin, and Adams are identified as HVTs. The question for fantasy team managers would be to determine how the Bucs and Raiders would compensate for their loss.

For the Bucs, the answer was tight end Cade Otton. Over the next three weeks, Otton's performance increased from his average of 3 receptions for 27 yards to 9 receptions for 86 yards. The Raiders responded by prioritizing their number 2 wide receiver, Jakobi Meyers. Since the Adams trade, Meyers's performance increased from an average of 5 receptions for 54 yards to 7 receptions for 74 yards. In both cases, analyzing the "order of battle" utilizing a depth chart prepared by each team's coaching staff that ranked each player's anticipated performance, then applying IPOE steps 3 and 4 revealed the likely solution.

More broadly, fantasy football also provides an opportunity to consider when and how these assets may be employed, a process very much like COA development. In the same way the threat has preferred tactics, so do football teams—but instead of a doctrine manual, football strategists use a playbook. While the football analyst doesn't need to know which specific tactics an offensive line will use, they do need to understand how the team will adapt its strategy that weekend given the weather, field conditions, and available capabilities.

To visualize this style of thinking, let us revisit the Bills-Lions game discussed earlier. The Detroit Lions use a "pass funnel" defense, which means that opposing teams are typically more successful if they pass instead of run, regardless of whether they focus on any combination of formations, called plays, or players' talent. The opposing Bills offense often utilizes

"2-safety zone coverage," in which the team's 2 safeties split responsibility for protecting the deep end of the field. This coverage typically allows "slot receivers" to run routes straight up the center of the field with less defensive pressure.

This threat template-style analysis yields several key insights. Josh Allen, the Bills' quarterback, will likely have ample passing opportunities, augmenting the above terrain-based (dome-covered stadium) analysis. As for the Lions offense, analysts may prioritize playing Amon-Ra St. Brown, the team's top wide receiver, who plays in the slot more than 50% of the time.

A fantasy team manager who applied these recommendations very likely won their matchup. We already noted Allen's exemplary performance: 362 yards gained, with 2 passing touchdowns. Likewise, St. Brown also took his opportunity and ran with it: 193 receiving yards and a touchdown. There are certainly instances where the analysis is not nearly as successful; nevertheless, fantasy football team owners will undeniably benefit from this thinking style over time.

Putting It into Practice

The same S-2 who briefs weather effects like a news reporter likely briefs step 3 as a catalog of capabilities. It typically sounds something like, "Sir, here is the threat order of battle. As you can see, he has 12x S219s, 1x 1L220 radar … [laundry list of assets continues]." Update briefs during the execution of operations sounds similar: "Sir, we've killed 3x 2S19s and 1x 1L220 radar…" In both cases, the S-2 has deferred analytic responsibility to the Commander (and staff).

The Commander needs the relative combat power analysis to identify strengths that can be exploited and weaknesses that must be mitigated. Here's a brief that meets the Commander's requirements by adding analysis to the factual data: "Sir, the threat only has 1x counterfire radar (1L200). This represents a critical vulnerability. Once it is destroyed, our artillery batteries can mass with impunity." The logic behind this recommendation mirrors the logic of a fantasy football team owner evaluating the significance of losing a key wide receiver.

Moreover, the process of analyzing how a football team will build its game plan and playbook exercises is very similar to COA development. Rather than simply scribbling enemy icons on an acetate overlay, the S-2 must consider whether the plan makes sense in the bigger picture. In football, one team may have a Hall of Fame quarterback, but if analysis indicates the opposition is weak against the run, a passing play might not be the best option. Likewise, just because an enemy in the battlespace has breaching assets does not mean they will conduct a breach. If the conditions to perform an infiltration or bypass are more favorable, then the COA should be adjusted to accommodate.

Recommendations for Implementation

If you've made it this far, I hope I've started to make a believer out of you and you agree that IPOE can help you win at fantasy football…or maybe you're just a big football fan. Either way, I have two recommendations to maximize this training event.

First, instead of a traditional season-long draft league, use a weekly league like FanDuel or DraftKings. By opting for a weekly format, each week provides a fresh game cycle. This allows an analyst who neglected the weather impacts in Buffalo one week, for example, to remedy that going forward. Arguably the most significant benefit of "IPFFE" (intelligence preparation of the fantasy football environment) is the immediate feedback loop allowing analysts to compare their assessments with results. Whereas most IPOE training in garrison often concludes with a simple analysis brief and suggestions about where it could be improved, fantasy football provides an "execution phase" that enables reflection.

Second, each week have an analyst brief the section on why they chose their lineup. This recommendation not only encourages analysts to focus on analytic rigor when making their selections, it also provides a valuable opportunity to practice briefing skills. Although this article focuses on the thinking required for effective IPOE, this analysis is wasted if it cannot be communicated effectively to the boss. Briefings like this in a low-stress situation ensure the section gets practice on *both* critical tasks.

Addressing Anticipated Misconceptions

I would be remiss if I didn't address two anticipated misconceptions. First, some readers may object that there is a distinct difference between the consequences of military intelligence analysis versus a fantasy football manager's analysis, arguing that intelligence analysts inform life-or-death decisions while fantasy football managers certainly do not. They're not wrong. The benefit of fantasy football analysis, however, is not linked to outcomes; instead, its value lies in the analytical process itself. Stated differently, analysts do not drown in the magnitude of the analysis, they drown in the data points. Fantasy football provides an easily accessible medium to refine this pattern of thinking, translating a myriad of data points into a compelling recommendation for the boss.

Others may contend that fantasy football wastes time that should focus on building knowledge of threat systems and tactics. Of course, IPOE requires a thorough knowledge of the threat, and fantasy football cannot (and should not) replace threat-focused training. It can, however, reinforce IPOE training and augment analysts' abilities to draw coherent conclusions and provide realistic recommendations. Even a savant-level knowledge of the threat is only useful if an analyst can make sense of it. Fantasy football offers a low-pressure environment to practice those sense-making skills.

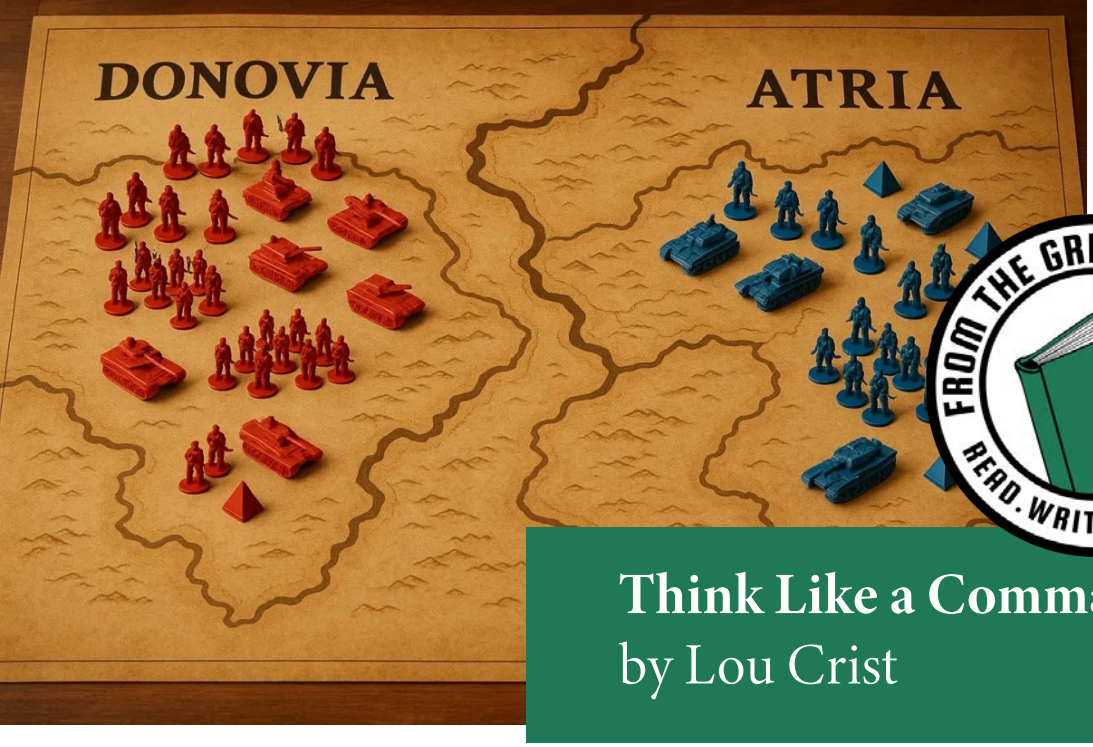
Conclusion

For many S-2s and analysts, IPOE is a daunting process, but we must not overcomplicate it. Ultimately, IPOE is a methodology for structuring analysts' thinking when determining how the operational environment and the threat can and will impact friendly operations. While intelligence analysts

leverage the methodology to determine how a threat will operate, it is a methodology applicable to numerous scenarios.

In particular, fantasy football managers use the same pattern of thinking. The difference is that fantasy football managers do it every week for four-plus months. In contrast, a typical intelligence analyst might get a similar opportunity once a quarter. Next season, instead of grinding through another analysis of the Suwalki Gap, why not train the same thinking processes while debating whether Lamar Jackson or Derrick Henry is more important to the Ravens' success next Sunday? 

MAJ Kyle Hanratty is currently the Brigade Combat Team (BCT) S-2 for 3 BCT, 82d Airborne Division. He previously served as an Observer, Coach, Trainer at the Joint Multinational Readiness Center, the Military Intelligence Company Commander for 2 BCT, 82d Airborne Division, and the Battalion S-2 for 2nd Battalion, 325th Airborne Infantry Regiment. His operational experience includes deployments to Kandahar, Afghanistan, and Mosul, Iraq with the 65th Engineer Battalion and 2 BCT, 82nd Airborne Division, respectively. He holds master's degrees from the U.S. Naval War College and U.S. Army School of Advanced Military Studies, plus a dual Bachelor of Arts in Chinese (Mandarin) and Political Science from the University of Notre Dame, South Bend, Indiana.



Think Like a Commander

by Lou Crist

This article was originally published on November 18, 2025, by From The Green Notebook at https://fromthegreennotebook.com/2025/11/18/think-like-a-commander and is reprinted here with their permission.

Several years ago, during an interview, I was asked, "What is the most important thing an S2 does?" The question took me aback. After some thought, I answered that the S2 should impart their understanding of the enemy to the commander. The interviewer sighed and replied, "No. Your job is to think like a commander." At the time, I didn't fully grasp his meaning. Years of experience and reflection have since convinced me that he was right.

A good S2 masters Intelligence Preparation of the Operational Environment (IPOE) and becomes the subject matter expert on the enemy. A great S2 studies friendly maneuver, knowing their unit's mission, organization, and tactics to make intelligence relevant. An exceptional S2 goes further, becoming the commander's intellectual partner in defeating the enemy.

The Role of the S2

Military intelligence doctrine is thorough, and IPOE is indispensable for threat analysis. Yet many S2s stop at describing the environment and the enemy. For years, I did the same, assuming that if I filled out the IPOE template and briefed the checklist, the "So What" would reveal itself. It seldom did. As an Observer Coach Trainer, I saw the same pattern: S2s competently outlined the threat but failed to make recommendations that shaped operations. When the analysis lacked relevance, commanders inevitably asked, "Give me the So What." What they really wanted was a bridge between enemy understanding and friendly action. To achieve that bridge, the S2 must understand friendly maneuver.

Intelligence officers must study their unit's mission, organization, and doctrine. Understanding what the unit does, and how it fights, is the foundation of relevance. Every branch has distinct intelligence needs. Field artillery units want to know how the enemy detects and targets them: radar coverage, long-range fires, and position areas for artillery. Airborne units care about drop zones, enemy air defense artillery, and counterattack forces. Armor and logistics formations have equally specific priorities. Knowing the unit's tactics allows the S2 to translate intelligence into operational value. Without that understanding, analysis often remains obscured.

Visualization Drives Relevance

Visualization is the first tenet of thinking like a commander. Clausewitz compared war to a wrestling match between two opposing wills. Sun Tzu taught that victory depends on knowing both the enemy and oneself. The S2 must visualize this interplay across time, space, and purpose, not just describing the enemy, but anticipating the fight. Understanding friendly maneuver provides the lens through which the enemy's reactions become visible. It enables predictive analysis, focuses attention on what matters, and removes the burden of presenting everything. Visualization also cultivates a shared language. Every branch has its dialect, and learning to "speak maneuver" builds credibility and trust. Mastering that language is the first step toward thinking like a commander.

Risk Lives in Uncertainty

Risk framing is the second tenet of thinking like a commander. Commanders live in uncertainty, and the degree of that uncertainty defines their risk. The S2 cannot remove risk, but by reducing uncertainty about the enemy, they shape how the commander perceives and manages it. If we knew everything about the enemy, intent, disposition, and capability, there would be no risk. But we never do. The S2's role is to define that gap between what is known and unknown, to describe how it threatens the mission, and to drive collection to close it. Risk to force matters only in how it endangers

mission success, and risk to mission begins where uncertainty lives. When the S2 frames intelligence in terms of uncertainty, they give the commander what they need most, a clearer picture of what is at stake and where to act.

Frame Decisions, Not COAs

Decision framing is the third tenet of thinking like a commander. Commanders think in terms of decisions. So should the S2. Rather than drowning in multiple enemy courses of action, define what the enemy is trying to achieve, and identify when, where, and how they will fight. Reducing enemy intent to a sequence of decisions makes the threat both intelligible and actionable. This approach naturally drives wargaming and supports decision-point tactics. It also sharpens the S2's recommendations for disrupting the enemy's decision cycle, whether through fires, deception, or maneuver. The commander decides, but the S2's excellence lies in anticipating those decisions and linking them to enemy action in time and space.

Objections & Emotional Intelligence

Some may argue that the S2's job is to define the problem, the S3's to propose solutions, and the commander's to decide. Doctrinally true, but practically incomplete. The S2 cannot define the right problem without thinking like a commander. If the S2's understanding ends at the enemy, the staff's options will be limited and cautious because they can only see half the picture. The commander will be left to do the imaginative work of connecting threat, terrain, and friendly action. In such cases, intellectual capacity across the staff goes unused. Others suggest that better staff integration, early S3 coordination, reverse IPOE, or full wargaming, compensates for this gap. Those methods are ideal but rare. Wargaming is often skipped, and reverse IPOE seldom performed. When time limits integration, the S2 must still wargame mentally, anticipating commander questions and shaping mission analysis from the outset.

Thinking like a commander does not mean overstepping authority. It demands tact, self awareness, and timing. Not every commander welcomes intellectual challenge, and some discourage staff initiative. But great commanders value subordinates who think, anticipate, and contribute meaningfully. The S2 must gauge the environment, read the personality of the commander, and know when to offer insight and when to listen.

I will leave you with an example. Commander Edwin Layton, Admiral Chester Nimitz's intelligence officer during the Pacific War, exemplified what it means for an intelligence officer to think like a commander. In the weeks before the Battle of Midway, Layton and his team synthesized signals intelligence, reconnaissance reports, and enemy logistics patterns to assess both the timing and direction of the Japanese attack. But Layton went further than analysis. He recommended how Nimitz should posture the fleet to exploit that expectation. His framing of the situation in terms of friendly maneuver allowed Nimitz to mass his limited carriers northeast of Midway, positioning them to strike the Japanese first. When the Japanese fleet appeared exactly where and when he anticipated, the result was one of the most decisive victories in naval history. Layton's brilliance lay not only in knowing the enemy but in sharing the commander's visualization of how to defeat him.

A good S2 owns their lane and knows the enemy. A great S2 understands friendly maneuver and delivers relevant, predictive intelligence. An exceptional S2 transcends both, becoming the commander's intellectual partner in defeating the enemy. Excellence for the intelligence officer lies not in the perfection of process, but in the alignment of thought, thinking with the commander.

Major Lou Crist serves as the Executive Officer for the 10th Support Group, U.S. Army Japan, Okinawa. A prior Infantry Intelligence Officer, he led a platoon in Afghanistan and, after transitioning to MI, served as an S2 in infantry, armor, aviation, airborne, field artillery, and logistics units. A SAMS graduate, he supported the Afghanistan withdrawal and later helped stand up Ukrainian assistance operations. His most notable assignments include XVIII Airborne Corps G35 Planner, First Army OC/T, and Devil 2 in the 1st Brigade Combat Team, 82nd Airborne Division.

From So What to Therefore

by Lou Crist

This article was originally published on November 20, 2025, by From The Green Notebook at https://fromthegreennotebook.com/2025/11/20/from-so-what-to-therefore and is reprinted here with their permission.

This is part II of a two-part series for intelligence officers. Read part I at https://mipb.ikn.army.mil/issues/jul-dec-2025/think-like-a-commander/.

Have you ever been told, "Just give me the 'so what'!" I saw this over and over again as an OC/T, watching commanders frustratingly critique their S2s during mission analysis briefs in time-constrained environments. The issue is not limited to intelligence briefs; however, Intelligence Preparation of the Operational Environment (IPOE), if not managed well, often overwhelms and obscures what matters to the commander. Yet the call for relevance did not teach relevance, and it did not help me understand what the commander was asking.

> An intelligence officer is an operator who understands the intelligence needs of the unit.
>
> -Marine Corps Doctrinal Publication 2, Intelligence 1997

Relevance Is Not Universal

The phrase "So What" is common in command discussions, but it often does more harm than good. Its meaning depends entirely on context. Having served in infantry, armor, aviation, field artillery, airborne, and logistics units, I learned that each formation defines relevance differently. Field artillery officers want to know how the enemy detects and targets them. Airborne commanders care about drop zones, air defense, and counterattack forces. Logistics leaders focus on sustainment routes and threats to movement. Each community has its own version of "So What," which means that without shared understanding, the question itself can confuse more than clarify.

Rather than fixating on "So What," I found it more useful to think in terms of "What, So What, and Therefore." What is happening, why does it matter to my unit, and what should we do about it? Situation, problem, and solution. The "So What" is important, but stopping there leaves the analysis unfinished. The true value of intelligence comes from turning understanding into action, moving from the descriptive to the prescriptive, from awareness to decision.

The What: Building the Foundation of Understanding

The "What" forms the base of the pyramid, the foundation of understanding. It establishes the facts before assessment begins. For intelligence officers, it corresponds to the first three steps of IPOE: terrain, weather, enemy composition, strength, and capabilities. During planning, these are essential elements. During execution, the "What" is often represented by incident trackers and templated graphics. Unfortunately, many S2s stop there. They brief data instead of analysis, and when that happens, they inevitably hear the frustrated "Give me the So What." The issue is rarely effort; it is often education. Most MI captains are generalists. They graduate from standardized courses and are scattered across diverse formations, often with limited familiarity with that unit's mission or how to make intelligence relevant. Under stress, they revert to what they know: basic IPOE. Without mentorship, they are unlikely to progress from information to insight. Commanders should remember Hanlon's Razor: never attribute to malice what can be explained by ignorance or inexperience. Demanding the "So What" without teaching what matters will only result in more noise. Teaching takes time, but it pays dividends in combat power.

IPOE is a box, not a cage. It is a checklist to ensure thoroughness, but it can trap analysts in process over purpose. The four steps of IPOE should build toward a single goal: enabling the commander's decision. Too often, we become lost in the details of terrain, weather, and equipment, only to forget what the enemy is trying to achieve. Doctrine should serve understanding, not replace it. In a time constrained environment, good intelligence officers know what to prioritize and what to set aside. At the top of the IPOE pyramid sits predictive analysis, the golden point that transforms data into decisions. Everything below it should be a means to that end.

The So What: Making Meaning from the Fight

The "So What" or basic relevance, represents the shift from the facts to what the enemy will do in relation to friendly forces. It corresponds to IPOE step four and the creation of enemy courses of action and decision support matrices. A good "So What" produces anticipation. When the commander begins directing the S3 during your brief, you are driving operations. That is progress, but it is not the summit. For years I thought the pinnacle for an S2 was effectively imparting an understanding of the enemy to the commander. I now believe the true role is to think like the commander and become an intellectual partner in defeating the enemy. Understanding is not the end state. Driving the fight is.

To find the "So What," junior intelligence officers must begin by studying their unit. Learn its mission, its training focus, and its doctrine. Read the Army's publications. Understand where your commander's attention lies: two levels down for training, one level up for context. Know what questions your commander will ask before they are voiced. At the battalion level, that usually means understanding the company and platoon fight. The S2 is the bridge between the larger intelligence community and the tactical edge. Make intelligence relevant by making it actionable at that level.

The Therefore: Turning Insight into Action

The final step is the "Therefore." This is where intelligence transitions from description to prescription, from information to operational art. It is the step most often avoided, either out of caution or lack of confidence. S2s hesitate to recommend action because they fear being wrong or overstepping. Yet the commander is required to decide under uncertainty. A well reasoned recommendation, even if imperfect, reduces risk and saves decision time. Without a "Therefore," the intelligence officer has simply presented an elaborate problem and walked away. The commander will always retain the responsibility to decide, but the S2 must share the responsibility to think. Intelligence without recommendation is awareness without action.

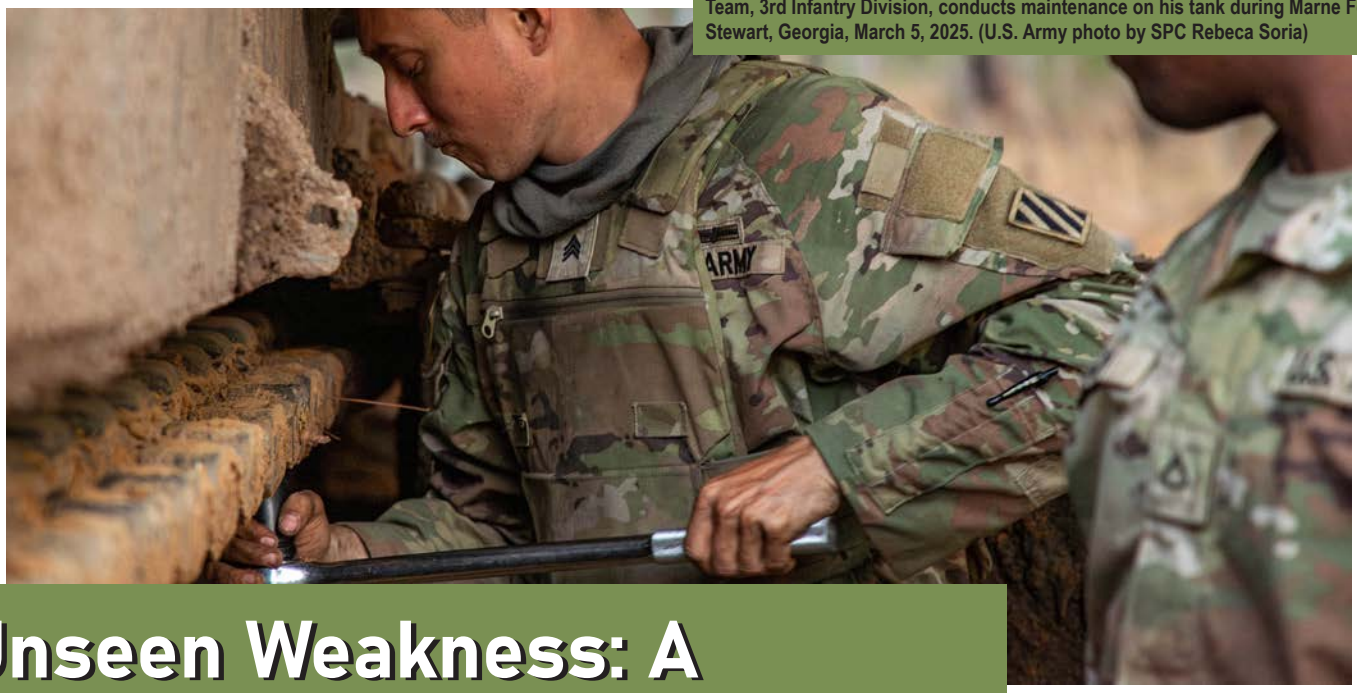
For the S2, the key is to work backward from the "Therefore." Every product, every graphic, every brief should trace its purpose to that end. Ask why you are producing it. Does it drive operations, or is it simply interesting? In garrison, make the threat real to your commander. In training, make the fight real to your Soldiers. In combat, make your analysis count by shaping what the unit does next. If it does not influence a decision, it is probably not worth saying.

Objections & Intent

Some might argue that the intelligence warfighting function exists to support operations and that the S2 is not the commander, and they would be doctrinally correct. Others might contend that they do not have time to be both the S3 and the S2, and they would also be right. Yet it remains true that an intelligence officer who confines themself to description, fails to understand friendly maneuver, and offers no recommendation on how to defeat the enemy is an ineffective S2. The intent of this paper is to encourage intelligence officers to think and act as operators, intellectual partners who share responsibility with their commanders for visualizing, understanding, and defeating the enemy.

Commanders and S2s should climb this pyramid together. Commanders must mentor their S2s, helping them understand what drives decisions. S2s must educate themselves on both enemy and friendly doctrine and constantly ask what comes next. The S2 who ends every assessment with a "Therefore" becomes a trusted agent in the fight. Intelligence that stops at "So What" merely informs. Intelligence that reaches "Therefore" drives operations.

Major Lou Crist serves as the Executive Officer for the 10th Support Group, U.S. Army Japan, Okinawa. A prior Infantry Intelligence Officer, he led a platoon in Afghanistan and, after transitioning to MI, served as an S2 in infantry, armor, aviation, airborne, field artillery, and logistics units. A SAMS graduate, he supported the Afghanistan withdrawal and later helped stand up Ukrainian assistance operations. His most notable assignments include XVIII Airborne Corps G35 Planner, First Army OC/T, and Devil 2 in the 1st Brigade Combat Team, 82nd Airborne Division.



An M1 armor crewman with the 6th Squadron, 8th Cavalry Regiment, 2nd Armored Brigade Combat Team, 3rd Infantry Division, conducts maintenance on his tank during Marne Focus 2025 at Fort Stewart, Georgia, March 5, 2025. (U.S. Army photo by SPC Rebeca Soria)

Unseen Weakness: A Critical Oversight for Specialized Maintenance in Modern Warfare

by Chief Warrant Officer 3 Jay D. Darnell and Mr. Justin W. Stancell

Amateurs talk about strategy and tactics. Professionals talk about logistics and sustainability in warfare.

—General Robert Hilliard Barrow, 27th U.S. Marine Corps Commandant

A Framework for Maintenance

As the Army transforms in contact to better prepare for multidomain operations, maintenance in this new paradigm must transform as well. Initial concepts for what future maintenance may look like are currently under development by U.S. Army Combined Arms Support Command working groups. The planned framework will encompass three levels of maintenance: strategic, support, and tactical.

The strategic maintenance level begins in the corps' rear area and works toward the forward line of own troops. This level contains depot flyaway teams and other U.S. Army Tank-Automotive and Armaments Command depot-level capabilities, a concept designed to bring continental United States (CONUS) capabilities–from depot-level maintainers to advanced manufacturing–into the theater to the point of need.

The support maintenance level services more advanced diagnostic and repair capabilities to build combat power by accelerating repairs and rapidly returning equipment to the user.[1] As this level will support combat nearly exclusively, the supply support activities (SSAs) will transition to purely technical supply. For those outside the maintenance realm, this means that maintainers will keep on hand only a minimal stock of spare parts and equipment needed to repair and maintain equipment and components. The goal here is to reduce the footprints of brigades and divisions.

Furthest forward is the tactical maintenance level. The most significant proposed change to effect maintenance at this level is a time constraint before evacuation to a higher maintenance level. Repairs exceeding, or expected to exceed, two hours will be candidates for immediate evacuation to allow advanced technicians to complete repairs away from combat operations. Most maintenance at the tactical level will be field-level diagnosis and preventative maintenance.

Intelligence Maintenance

The nature of the intelligence warfighting function is to gather information that supports commanders' decision making across the battlefield. This requires the physical presence of the systems and Soldiers that comprise the warfighting function. Intelligence systems reside at rear-area strategic

command posts and extend up to the forward line of own troops, providing support to commanders at every echelon. The most recent changes to the Army force structure have placed the lowest echelon of intelligence maintenance at the division intelligence and electronic warfare (IEW) battalion or the division general support military intelligence company. While some brigades (mainly in the Army National Guard) maintain a brigade military intelligence company, most are transitioning to the new structure.

One of the principal challenges for intelligence maintenance is the complexity and low density[2] of systems. These systems are often quick reaction capability or limited material release systems and are frequently updated faster than they can reach sustainment-supported status. This creates additional hurdles for repairs as parts are often available only at the vendor level. The vehicle fleet, in contrast, has the density to keep tires and engine components stocked at the brigade level. When a vehicle component is placed on order, it can often be retrieved from the local stock or the SSA within an hour, allowing work to begin immediately.

Intelligence system parts ordered through the Army Supply System often require months-long lead times due to low demand, resulting in insufficient warehouse stock. The relevant Army depot or the manufacturer typically receives most requisitions for manufacture and release. Utilizing this alternative source of supply can add months to the maintenance process, reducing equipment availability and the odds of mission success. During armed conflict, this could mean a part arriving after a campaign has ended.

For repairs that require vendor-derived parts, the fault must be validated first by Soldiers, then by the U.S. Army Communication-Electronics Command Logistics Assistance Representative, and only then can it be requested from the vendor with the approval of the Integrated Logistics Support Center. This can be a lengthy process, as it depends on contracts between the Army and the vendor. The requested parts arrive directly from vendors and not through the standard supply system. The parts do not have national stock numbers and thus cannot be delivered to an SSA. Moreover, in a CONUS garrison (and even in some established locations outside the continental United States), this transaction is completed utilizing commercial shipping. During some operations, and in particular during armed conflict, this can preclude parts from even entering the theater.

Furthermore, evacuating systems for repair is problematic because intelligence maintenance support activities are structured differently from their ordnance counterparts. Ordnance maintenance is generally structured so that a forward maintenance company at the battalion level can evacuate systems from the brigade support battalion to the division sustainment brigade or the division sustainment support battalion before they reach depot-level maintenance. For intelligence maintenance support activities, the IEW battalions at the division and corps are structured to operate independently at their respective echelons. If an intelligence system requires evacuation, however, there are no specialized maintenance activities at the theater or corps areas to which maintainers can send that equipment. Instead, it must be transferred directly to the depot level or to the vendor for repairs. Vendor transactions require commercial shipping for evacuation, which requires special approvals to secure funding and further delay shipment.

The Way Ahead

As new intelligence systems are developed for the multidomain battlefields of the future, military intelligence systems maintainers must be documented as the primary maintainers of those systems and trained in their maintenance and repair, regardless of whether the vendor or program manager provides this training as a part of the initial fielding or as a stand-alone course. Army Regulation 750-1, *Army Materiel Maintenance Policy*, states that "Maintenance by contract personnel is prohibited" in "systems operating forward of the Corps rear boundary during Large Scale Combat Operations."[3] While exceptions can be requested for weapons systems requiring contractor logistics support forward of the corps' rear boundary, this policy clearly articulates that Soldiers must be recognized as the primary maintenance solution.

With Army Soldiers taking the lead as primary maintainers, the Army supply system must incorporate specialized parts and lowest replaceable units and make them orderable through a full material release upon system fielding. Parts not in the supply system cannot be ordered through the Global Combat Support System—Army (the program of record for sustainment). They cannot travel using organic systems, Soldiers, or combat logistics trains that can deliver parts to a conflict zone. Releasing the parts in this manner will allow stockage of low-density parts across the battlefields at SSAs, as well as viability for spares.

The complexities inherent with multidomain operations and intelligence systems distributed across the battlefield create a need for IEW maintenance sections to store spare components and repair parts locally for immediate accessibility. Division and corps IEW battalions' maintenance sections have AN/ASM-146/147 transportable electronic shop shelters,[4] allowing for the transport and storage of critical spares at the site of repair. Storing repair parts at the forward echelon enables sourcing critical components to complete repairs in hours rather than weeks or months. This minimizes downtime for repairs and ensures commanders have access to the maximum amount of intelligence for making timely decisions.

Depending on future restructuring decisions for Army maintenance, there may be a need to restructure intelligence maintenance to enable a scaffolding progression.[5] This would facilitate the repair of more complex parts and advanced training for maintainers further from the forward line of own troops. Preventing the need to evacuate intelligence systems from the theater will allow return to service in mere days, as the transportation burden of shipping components or systems to U.S. locations is eliminated. As IEW sections support more complex systems through transformation, the need for more complex intelligence maintenance structures is an inevitability.

Intelligence systems maintenance is critical to sustaining the intelligence enterprise at every echelon. Unlike fleet maintenance, intelligence systems maintenance is a low-density and often invisible component of the maintenance enterprise that is rarely, if ever, included in plans or orders. The unseen weakness is the critical *omission* of specialized maintenance in modern warfare. For intelligence system maintenance, reliance on contractor logistics support to sustain systems during multidomain operations is impractical.

Epigraph

"Q&A: Marines' (General Robert—ed.) Barrow Backs SALT—And Conventional Rearming," *San Diego Union*, November 11, 1979, C4.

Endnotes

1. Combined Arms Support Command (CASCOM), "Sustainment Today, Tomorrow and the Future," PowerPoint presentation for Multidomain Operations Maintenance Concept Development Touchpoint with CASCOM, November 22, 2024, slide 4.

2. Low density, in this context, refers to a process that considers a range of factors to ensure sustainability and efficiency and can significantly reduce development time and cost.

3. Department of the Army, Army Regulation 750-1, *Army Materiel Maintenance Policy* (Government Publishing Office [GPO], 2023), 34-35.

4. Department of the Army, Technical Bulletin 43-0123, *Aviation Electronics Configuration Directory* (GPO, 1981[obsolete]), 113, https://aviationandaccessories.tpub.com/TB-43-0123/TB-43-01230030.htm.

5. Scaffolding is a teaching technique that delivers lessons in units requiring progressively less instructional support as training proceeds. For a more detailed discussion, see "Scaffolding Content," Office of Curriculum, Assessment, and Teaching Transformation, University at Buffalo, 2025, https://www.buffalo.edu/catt/teach/develop/build/scaffolding.html.

CW3 Jay Darnell is the course manager for the Intelligence Systems Integration and Maintenance Technician Warrant Officer Basic Course, U.S. Army Intelligence Center of Excellence, Ft. Huachuca, AZ. His earlier assignments include service with the 2nd Stryker Brigade Combat Team (BCT), 4th Infantry Division, the 1st Armored (BCT), 1st Cavalry Division, the 3rd BCT (Rakkasan), 101st Airborne Division (Air Assault), and the 1st Military Intelligence (MI) Battalion (Aerial Exploitation). CW3 Darnell deployed to Afghanistan multiple times in support of Operation Enduring Freedom, in addition to completing rotational deployments in support of Operation Atlantic Resolve and the Korea Rotational Force.

Mr. Justin Stancell is the Intelligence Systems Integration and Maintenance Discipline Technical Advisor for the Directorate of Training and Doctrine, U.S. Army Intelligence Center of Excellence, Ft. Huachuca, AZ. His earlier assignments include service with the 527th MI Battalion, the 101st MI Battalion, 1st Infantry Division, the 3rd BCT, 82nd Airborne Division, the 1st Battalion, 79th Field Artillery, 434th Field Artillery Brigade, and the 111th MI Brigade. He deployed multiple times in support of Operation Iraqi Freedom. Justin holds a bachelor's degree in technology management and an associate of applied science in electronics technology.

OPERATIONALIZING INTELLIGENCE THROUGH SMALL UNMANNED AIRCRAFT SYSTEMS

BY CAPTAIN JOSE A. LOPEZ

U.S. Army Soldiers assigned to 1st Battalion, 4th Infantry Regiment, Joint Multinational Readiness Center, Hohenfels, Germany, remotely operate a quadcopter in the Hohenfels Training Area, during Combined Resolve X, May 2, 2018. (U.S. Army photo by 1LT Matt Blubaugh)

Silent Wings Over Donetsk Ridge

Author's note: This vignette is a fictitious representation of a nonexistent unit.

The frigid winds swept across the Donetsk Ridge as the first light of dawn struggled to pierce the overcast skies. Snow-covered hills and dense forests flanked the valley, masking the movements of both Russian and Ukrainian forces. Kaptain Oksana Marchenko, intelligence officer for Ukraine's 123rd Mechanized Brigade, stood in the tactical operations center at Kramatorsk, her brow furrowed as she analyzed the fragmented intelligence reports coming from forward positions.

The brigade's mission was to advance along the ridge toward the transport hub at Bakhmut, a vital supply line for ongoing defensive operations to the east. Success depended on precise coordination, reliable intelligence, and the ability to outmaneuver the Russian forces entrenched in the area. However, the enemy's activity was subtle but ominous. Intermittent artillery fire and sightings of loitering munitions suggested a coordinated Russian presence. The valley's jagged terrain, narrow routes, and frequent electromagnetic interference rendered traditional reconnaissance assets almost useless.

The brigade's imported small unmanned aircraft systems were limited by range and increasingly affected by Russian electronic warfare systems. The cavalry reconnaissance unit, maneuvering along icy trails, had limited visibility and feared ambushes. Their approach was deliberate and in line with the brigade's sectored collection plan, assigning areas of responsibility to each organization in an effort to synchronize collection and maximize visibility of the enemy.

The Russian response came swiftly. As two companies from the 1st Mechanized Battalion pushed through a bottleneck near Chasiv Yar, a carefully orchestrated ambush unfolded. Lancet loitering munitions struck the lead vehicles, sowing confusion. Concealed infantry and anti-tank guided missile teams launched a second wave of strikes. With visibility low and communication disrupted by jamming, the forward units were pinned down, unable to advance or retreat.

At the tactical operations center, Marchenko realized the adversary was exploiting the brigade's intelligence gaps, leveraging terrain and electronic warfare. Without real-time situational awareness, the brigade risked losing tempo and its ability to counterattack. The limits of traditional intelligence, surveillance, and reconnaissance platforms were evident, and immediate action was needed to avoid catastrophe.

Maximizing Capabilities

The fictional scenario of Kaptain Marchenko's struggle in Donetsk illustrates a critical challenge modern militaries face: the integration and synchronization of small unmanned aircraft systems (SUAS) within combat operations. This article seeks to drive a necessary discussion of the critical role of SUAS in enhancing situational awareness, target acquisition, and decision making at the brigade level. The introduction of SUAS revolutionized traditional reconnaissance methods and continues to empower commanders to shape the battlefield, enabling greater agility and precision in dynamic environments. This article presents two key frameworks—the Sector Collection Approach and the Ready Reserve Concept—to optimize SUAS employment and emphasizes the importance of integrating collection management into operational planning. These processes align with the Army's Transformation in Contact effort, where the collection manager must evolve from an asset allocator to an advisor on effects and capabilities.

Recent military conflicts illustrate the consequences of desynchronized intelligence, surveillance, and reconnaissance (ISR) collection. Uncoordinated and ill-equipped collection efforts create intelligence gaps, often leading maneuver forces to advance blindly into well-prepared enemy defenses. The U.S. Army is currently fielding short-, mid-, and long-range reconnaissance capabilities (particularly SUAS) at the brigade level that present a new set of opportunities and challenges. Without a standardized framework for integrating SUAS, intelligence professionals struggle to effectively drive operations and targeting. The war in Ukraine provides a clear demonstration of this challenge, with units facing ambushes and tactical setbacks due to inadequate real-time intelligence.[1] These lessons underscore the urgent need for brigades to evolve their ISR collection practices. By leveraging SUAS capabilities,

units can maintain continuous surveillance, enable timely targeting decisions, and reduce operational vulnerabilities. Adapting ISR methodologies at the brigade level is crucial to preventing tactical paralysis and maintaining a decisive edge on the modern battlefield.[2]

To fully leverage SUAS capabilities, commanders must fundamentally shift their perspective on reconnaissance. Instead of viewing it as a set of discrete tasks, they need to embrace reconnaissance as an interconnected system.[3] This paradigm shift treats SUAS as expendable assets, prioritizing intelligence gathering over platform preservation and accepting calculated losses to ensure mission success. This allocation of assets and the acceptance of potential losses will always be a commander-dependent decision based on the overall maneuver.[4] By adopting this mindset, brigade-level leaders can maximize their collection assets, ensuring timely, reliable intelligence that drives decision making. This approach mitigates reactive information gaps and fully harnesses the transformative potential of SUAS in modern warfare.

Maximizing the use of SUAS fundamentally transforms reconnaissance and intelligence operations by reducing risk, extending operational reach, and shaping the battlespace.[5] A U.S. Army brigade with short-, mid-, and long-range reconnaissance SUAS can simulate activity, deceive adversaries, and gather intelligence in real time, rather than relying solely on physical troop movements to provoke enemy reactions. For example, SUAS equipped with electronic warfare payloads could potentially disrupt enemy air defense radars, a capability previously limited to higher-echelon assets. Such capabilities conceal true operational intent and manipulate adversary perceptions, shaping their decision making before direct engagement.[6]

Theoretical Frameworks for Employment

The modern battlefield demands rapid intelligence collection, analysis, and action for operational success. The Joint Multinational Readiness Center is uniquely postured to observe diverse collection practices across light, medium, and heavy U.S. units undergoing transformation in contact, as well as multinational brigades, and, most importantly, through dialogue with Ukrainian soldiers being trained as part of the Joint Multinational Training Group-Ukraine mission. Emerging tactics, techniques, and procedures identified through training with the Ukrainians showcase innovative SUAS employment and enhance brigade-level intelligence operations, particularly through the Sector Collection Approach and the Ready Reserve Concept.

The Sector Collection Approach. This approach divides the area of operations into smaller sectors aligned with named areas of interest and target areas of interest.[7] This division prioritizes collection efforts, mitigates SUAS capability gaps (terrain and limitations), and enhances control and coverage. Together with the centralized intelligence collection synchronization matrix, this approach empowers subordinate commanders to allocate SUAS within their sectors based on specific threats while maintaining the brigade's overall collection priorities. The brigade sections the area of operations and assigns requirements to its battalions, while battalions operate within these sectors, dynamically allocating and re-tasking the SUAS based on real-time threat activity and environmental factors. This structure enables early threat detection, supports the cueing of fires and maneuver forces, and creates redundancy in SUAS collection across the brigade front. By integrating doctrinal planning tools with responsive drone employment, units establish a layered SUAS network capable of adapting to complex and evolving threats.

For example, as part of a brigade defense (see figure 1 on the next page), the intelligence section divides the area of operations into battalion sectors, and then further subdivides each sector into smaller collection sectors (e.g., Sector Red, Sector White, Sector Blue). Each battalion is assigned named areas of interest within its sector based on likely enemy avenues of approach.

In Sector Blue, Task Force Blue observes enemy mechanized infantry elements probing near Sector Blue 1. A battalion's organic SUAS detects the movement and initiates surveillance. Minutes later, more enemy forces appear in Sector Blue 2, forming what appears to be a flanking maneuver. The battalion assigns another drone to maintain custody of the second element while cueing the brigade's mid-range reconnaissance assets forward into the brigade sector to look for follow-on forces. This also allows the long-range SUAS to continue with the developed collection plan to further confirm or deny enemy actions. These actions prevent enemy deception or a multi-pronged breach. Task Force White repositions its drones to cover adjacent sectors, enabling cross-cueing between battalions.

Because each battalion controls its ISR assets within clearly defined sectors, and brigades retain flexible ISR options, the unit reacts in real time to a complex enemy movement, reallocates sensors dynamically, and denies the adversary freedom of action.

The Ready Reserve Concept. Supporting this framework is a tactical drone reserve composed of SUAS capable of multiple effects (collect, decoy, jam, one-way attack, etc.) that offer the brigade commander operational flexibility. The Ready Reserve responds rapidly to threats or fleeting opportunities while enabling intelligence collection to develop the operational environment. The Ready Reserve's intent is to provide a flexible framework that supports operational needs, targeting, and intelligence collection, thus creating a layered intelligence network that enhances situational awareness and operational agility. (See figure 2 on the next page.)

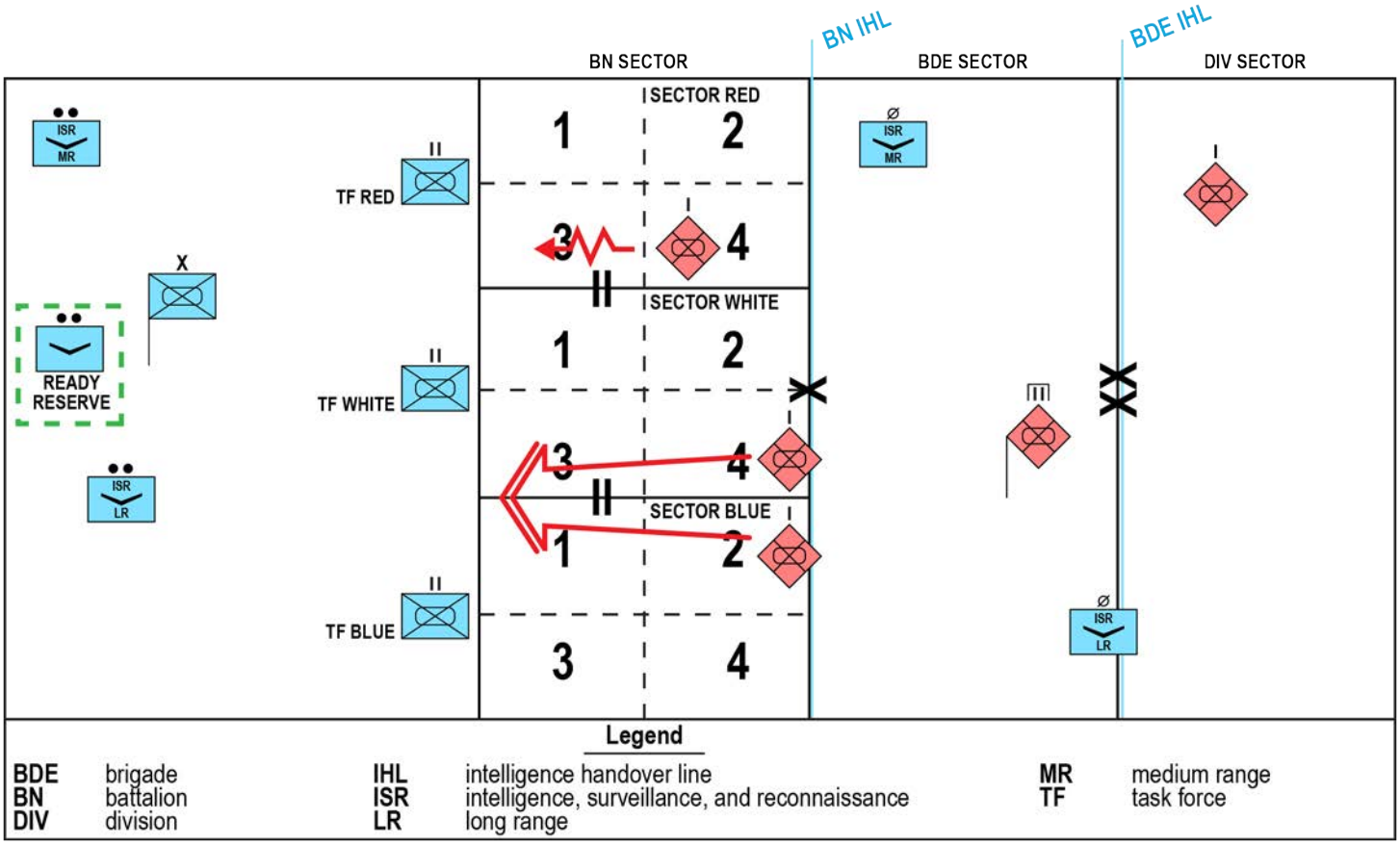


Figure 1. Sector Collection Approach

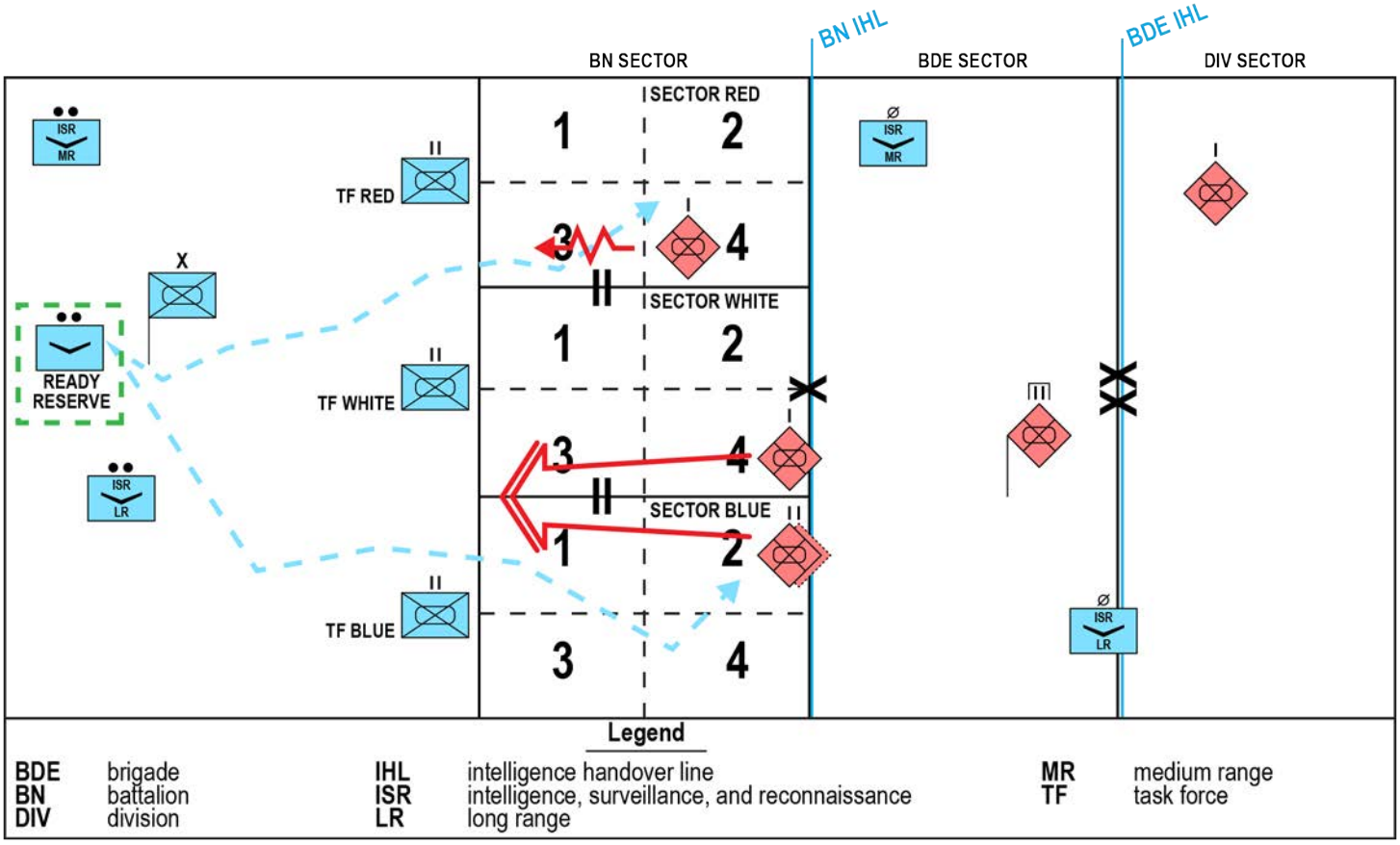


Figure 2. Ready Reserve Concept

A 3rd Brigade, 10th Mountain Division Soldier conducts security at Hohenfels Training Area, Joint Multinational Training Center, Germany, January 30, 2025. (U.S. Army Reserve photo by SSG Miguel Miolan)

For instance, consider the previous scenario. Following the detection of enemy elements in Sector Blue, the battalion's SUAS maintain persistent observation, confirming that the enemy is shaping conditions for a breach. As two mechanized enemy companies mass at the boundary between Sector Blue 2 and the battalion intelligence handover line, Task Forces Blue and White identify indicators of a coordinated penetration attempt.

Despite maintaining ISR coverage within its sector, Task Force Blue's organic SUAS are already fully tasked. To address the threat without stripping coverage from other sectors, the brigade collection manager activates the Ready Reserve. The Ready Reserve rapidly launches additional drones to reinforce surveillance in Sector Blue and extend observation into the adjacent brigade sectors.

As these reserve drones begin tracking follow-on enemy echelons along a concealed route, the intelligence section directs the cueing of mid-range reconnaissance SUAS to extend depth and maintain continuous custody. Fires and maneuver elements adjust their disposition based on real-time imagery and target confirmation. The ability to surge SUAS from the Ready Reserve enables the brigade to maintain situational awareness, support fires coordination, and deny the enemy freedom of movement—all without degrading the ISR posture in other sectors. This capability challenges the traditional tenet of "no reconnaissance in reserve." The Ready Reserve SUAS are best viewed not as assets to be conserved, but as a force ready to be committed to gain and maintain contact with the enemy.[8]

Transforming Collection Management in Contact

One of the primary challenges to fully operationalizing a SUAS framework is the brigade collection manager's limited, often reactive role. Many collection managers today focus on tasking and asset allocation but lack the training to integrate SUAS into operational planning and maneuver synchronization.[9] This reactive posture results in drone missions driven by immediate requests rather than proactive collection plans, perpetuating the enduring dilemma of "fighting the plan, not the enemy."

To meet the demands of modern warfare, the collection manager must evolve from a platform allocator into a force enabler—one who drives collection by managing effects and capabilities as integral components of operational design. The brigade collection manager's span of control is limited; this requires collection managers at all echelons to prioritize establishing a clear commander's intent and enabling subordinate battalions to independently plan and execute SUAS missions that support the brigade's objectives.

The collection manager of 2030 must possess a unique blend of technical expertise, operational awareness, and doctrinal fluency. Courses like the Information Collection Planners Course are essential, but collection managers must also develop a deep understanding of SUAS employment—specifically the range, payloads, and limitations that shape tactical options. This role also exceeds the capacity of a single individual. Dedicated collection management teams at brigade and battalion levels are essential for distributing responsibilities between current and future operations to ensure continuous support, proactive planning, and timely employment of collection assets.[10]

For this framework to succeed, collection management teams must integrate with maneuver units throughout training, rehearsals, and execution. Integration of SUAS should be a core element of operational planning, enabling SUAS

to function as organic extensions of maneuver forces for target development, reconnaissance, deception, and force protection. During operational planning at the brigade and battalion levels, intelligence sections should proactively recommend how to maximize SUAS employment to commanders and operations elements.

Consider a scenario where the brigade's objective is to attack and seize key terrain held by a degraded enemy force in hasty defensive positions. The enemy consists of two mechanized infantry companies in the front, and one in the rear as a second echelon. Intelligence assessments indicate that the rear company lacks sufficient combat power to maneuver and has entrenched itself in a tactically advantageous position that could threaten friendly forces during their approach.

To mitigate this threat, the intelligence section proposes to the operations element that a portion of the SUAS assets be employed to fix the degraded enemy force. This can be achieved through a combination of drone sound propagation, one-way attack SUAS, and jamming, synchronized with a coordinated fires plan. By executing this plan, friendly forces can divert minimal combat power to fix the entrenched enemy, freeing maneuver elements to sustain the main effort and achieve a successful penetration and envelopment of the adversary.

This example illustrates how deliberate SUAS integration can enhance operational flexibility, maximize combat power, and create opportunities for battlefield success. Lessons from the Ukrainian conflict underscore the urgency of doctrinal adaptation to match the rapid pace of technological advancement. Integrating SUAS into traditional reconnaissance and operational planning enhances decision making and creates new opportunities for ISR-driven maneuver warfare. However, success hinges on robust training, resilient communications, and a deliberate approach to integrating SUAS into tactical and operational frameworks.

At the center of this transformation is the evolving role of the brigade collection manager, who must shift from an asset allocator to a capabilities-and-effects integrator. The collection manager ensures SUAS operations align with the commander's intent, synchronizing real-time intelligence collection with maneuver and targeting to generate decision advantage in dynamic environments. Frameworks such as the Sector Collection Approach and Ready Reserve enable this integration, providing structured methods for SUAS employment that support reconnaissance, targeting, and strike operations. By leveraging these frameworks and embedding SUAS into doctrinal planning, training, and execution, brigades can achieve intelligence overmatch—empowering commanders with superior decision making, enhanced lethality, and operational adaptability on the modern battlefield.

Turning the Tide

Author's note: This vignette is a fictitious representation of a nonexistent unit.

Kaptain Marchenko quickly leveraged the Sector Collection Concept, prioritizing critical zones near Chasiv Yar and along the surrounding ridgelines. Each grid received overlapping coverage tailored to terrain and threat indicators, enabling persistent and responsive intelligence collection.

Flying low and exploiting terrain for concealment, the SUAS network began to illuminate the battlefield. In one sector, drone feeds identified concealed mortar teams responsible for earlier indirect fire. In another, intercepted signals and thermal imagery revealed a Russian command post camouflaged within a cluster of abandoned buildings. The brigade's decentralized, but synchronized, plan allowed subordinate units to control their organic SUAS while remaining nested within the broader collection architecture, ensuring rapid exploitation of sensor data and reducing intelligence, surveillance, and reconnaissance latency.

As the intelligence picture developed, Marchenko identified a critical gap in the enemy's array—a seam between two Russian elements that left their flank exposed. Acting as the brigade's collection manager and subject matter expert, she immediately advised the operations officer and the commander that conditions had been met to transition from shaping to decisive action. She recommended employing the Ready Reserve, specifically its strike drone capability equipped with a first-person view, to fix the enemy in place and deny maneuver options. This would create conditions for committing Anvil Company, the brigade's reserve force, to exploit the gap and strike deep into the enemy formation, forcing an early culmination of the enemy's attack.

Moments later, a Ready Reserve drone confirmed the command post's location in real time. The tactical operations center coordinated an immediate artillery strike, disrupting the enemy's ability to command and control. With their leadership node destroyed and forward elements disoriented, Ukrainian forces regained momentum and pushed through the ridge to secure Bakhmut. Deprived of coordination and overwhelmed by precision effects, Russian forces were forced into a hasty retreat.

Endnotes

1. Dominika Kunertova, "Drones Have Boots: Learning from Russia's War in Ukraine," *Contemporary Security Policy* 44, no. 4: 576–91, https://doi.org/10.1080/13523260.2023.2262792.

2.Jeffrey A. Edmonds and Samuel Bendett, "Russia's Use of Uncrewed Systems in Ukraine," Center for Naval Analyses, March 31, 2023, https://www.cna.org/analyses/2023/05/russias-use-of-drones-in-ukraine.

3. Department of the Army, Field Manual (FM) 3-98, *Reconnaissance and Security Operations* (Government Publishing Office [GPO], 2023), 1-7.

4. Anthony R. Padalino, "The Army Needs to Quickly Adapt to Tactical Drone Warfare," *Infantry* 113, no. 2 (2024): 32–36, https://www.benning.army.mil/infantry/magazine/issues/2024/Summer/pdf/10-Padalino_txt.pdf.

5. Kerry Chávez and Ori Swed, "Emulating Underdogs: Tactical Drones in the Russia-Ukraine War," *Contemporary Security Policy* 44, no. 4, 592–605, https://doi.org/10.1080/13523260.2023.2257964.

6. David Hambling, *Swarm Troopers: How Small Drones Will Conquer the World* (Archangel Ink, 2015).

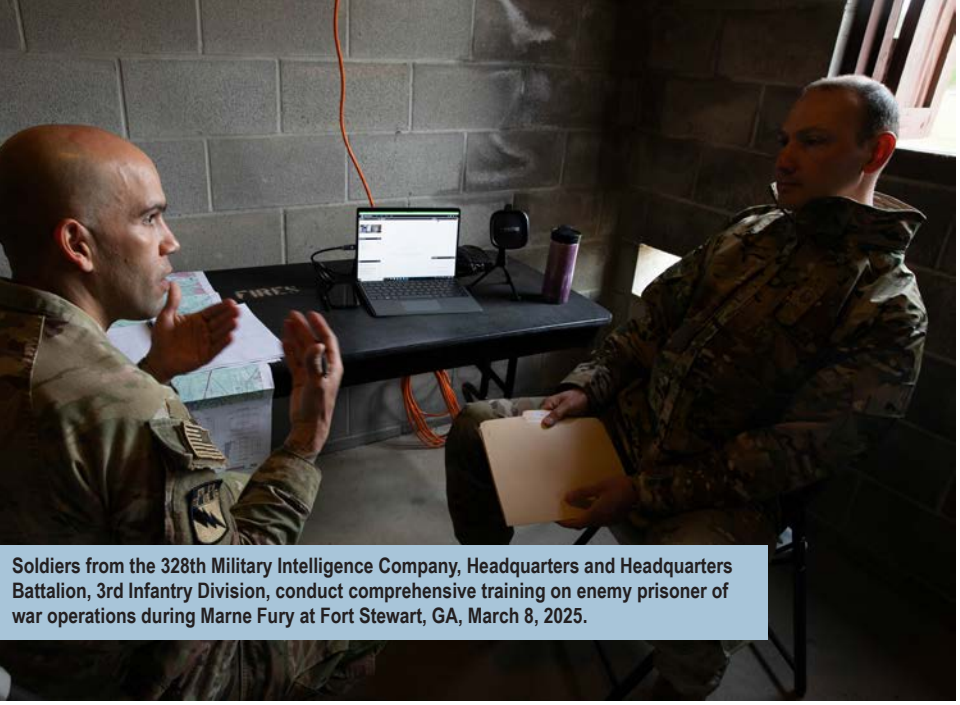
7. Department of the Army, Army Techniques Publication (ATP) 2-01, *Collection Management* (GPO, 2021), 5-3. Incorporating change 1, September 2025.

8. Department of the Army, FM 3-98, *Reconnaissance and Security Operations*, 4-1.

9. Matthew F. Smith, "Enabling Success of Brigade Combat Team's Collection Management in the Era of Multi-Domain Operations," *Military Intelligence Professional Bulletin* 47, no. 1 (2021): 69–76, https://mipb.ikn.army.mil/media/maaf330m/mipb-2021-01-03-full-issue.pdf#view=fit&page=71.

10. Department of the Army, ATP 2-01, *Collection Management*, 1-2.

CPT Jose Lopez is a strategic intelligence officer pursuing a master of science and technology intelligence with a concentration on data science in intelligence at the National Intelligence University. His previous assignments include serving as the deputy brigade intelligence trainer and brigade collection manager trainer at the Joint Multinational Readiness Center in Hohenfels, Germany. CPT Lopez deployed to Al Qaim, Iraq, with the 3rd Squadron, 3rd Cavalry Regiment, where he served as the collection manager for Task Force Thunder and Task Force Lion supporting operations against the Islamic State. He is a graduate of the Intelligence Collection Planners Course and holds a master of arts in intelligence studies from the American Military University.



Soldiers from the 328th Military Intelligence Company, Headquarters and Headquarters Battalion, 3rd Infantry Division, conduct comprehensive training on enemy prisoner of war operations during Marne Fury at Fort Stewart, GA, March 8, 2025.

Marne Fury: Modernizing Interrogation and Language Training

by Chief Warrant Officer 2 Steven Betancourt

Introduction

Human intelligence (HUMINT) collection stands as the oldest form of information gathering in military operations. Despite the military's technological advancements, the human mind remains the most complex and unpredictable element in intelligence collection. Traditional HUMINT operations often face significant challenges from a reliance on interpreters, leading to translation inaccuracies and slower intelligence collection. Marne Fury, a first-of-its-kind field training exercise that offered HUMINT collectors from the 328th Military Intelligence Company a novel opportunity to practice their interrogation skills with "enemy" role players in their native languages, addressed these limitations by integrating direct language proficiency into interrogation operations, boosting efficiency and accuracy. Marne Fury integrated HUMINT techniques with remote instruction, synchronizing interrogation operations and language training to improve operational readiness and intelligence collection.

In her 2014 co-authored study, forensic psychologist Dr. Beth H. Richardson's research demonstrated that linguistic alignment between interrogators and suspects, a technique known as language style matching, significantly improves interrogation effectiveness.[1] By mirroring interrogees' linguistic patterns, interrogators foster rapport and increase the likelihood of obtaining reliable information, especially in high-pressure environments. Military operations increasingly demonstrate that integrating language skills into HUMINT collection yields better, more actionable intelligence. Marne Fury's strategic fusion of language capabilities with interrogation techniques enhanced questioning precision, strengthened rapport, and produced more accurate intelligence under demanding conditions.

The 3rd Infantry Division developed Marne Fury to bridge the gap between theory (i.e., traditional interrogation training) and the seamless integration of practical language skills in real-world scenarios. This exercise moved beyond theoretical knowledge by equipping Soldiers with dynamic communication skills necessary for high-stress operations. The lessons learned during Marne Fury offer military personnel and decision makers valuable insights into enhancing intelligence-gathering capabilities in complex global environments.

Modernizing Interrogation Operations

Effective interrogation operations play a vital role in military success, particularly in combat situations where timely and accurate intelligence shapes tactical decisions. Successful interrogations reveal enemy troop movements, planned attacks, and adversarial objectives. This intelligence safeguards friendly forces, identifies threats, and supports mission success.

Traditional HUMINT training typically focuses on questioning techniques, psychological strategies, and legal compliance. However, a heavy reliance on interpreters weakens effectiveness. Interpreter dependency slows information processing, introduces translation inaccuracies, and creates communication barriers. These challenges reduce the reliability and timeliness of intelligence. Marne Fury eliminated this obstacle by deploying Defense Language Institute-trained and native-speaking U.S. Army HUMINT collectors. These Soldiers conducted interrogations in the detainee's native languages, including French, Spanish, and Russian, in accordance with Article 17 of the Third Geneva Convention.[2] Direct communication improved rapport, enabled more accurate assessment of verbal and nonverbal cues, and increased the reliability of intelligence.

A 2021 article in the New York University School of Law's law and policy journal, *Just Security*, emphasizes the importance of rapport building through a discussion of "The Méndez Principles," the United Nations standards and guidelines governing investigations and information gathering.[3] The article

argues that trust-based communication significantly improves information reliability. Marne Fury adopted these principles by prioritizing direct engagement with detainees, which improved the quality and accuracy of intelligence collected.

Marne Fury also expanded language training beyond speaking and listening skills. HUMINT collectors analyzed handwritten notes containing misspellings, slang, and cursive writing to simulate realistic conditions. This approach enhanced their ability to interpret captured documents, which play a critical role in intelligence planning and preparation.

Strengthening Interrogations Through Language

Proficiency in detainees' native languages gives HUMINT collectors key advantages that significantly enhance the interrogation process. Direct communication fosters trust and rapport, increasing detainees' likelihood to cooperate. Detainees engage more openly with interrogators who speak their language fluently rather than through interpreters, a connection that leads to more detailed and reliable information. Linguistic proficiency also allows HUMINT collectors to detect subtle nuances in speech, including tone, inflection, and word choice. These details provide insight into a detainee's credibility and state of mind. Understanding cultural and linguistic contexts helps collectors interpret idioms, slang, and dialects that might otherwise be misunderstood or lost in translation.

Eliminating the need for interpreters during Marne Fury reduced the potential for translation errors and biases. HUMINT collectors communicated directly with detainees, ensuring accurate and secure exchanges. Real-time direct questioning, with no translation delays, allowed HUMINT collectors to respond dynamically. They immediately followed up on statements, probed inconsistencies, and adapted their approach based on detainee responses. This agility is a critical enabler in high-pressure situations, where timely intelligence drives tactical and strategic decisions.

Enhancing Language Training Through Immersion

Marne Fury enhanced language training by immersing participants in real-world scenarios. Traditional military language programs rely on classroom instruction, memorization, and scripted conversations. These methods establish basic skills but fail to replicate combat stress and unpredictability. Marne Fury introduced immersion by requiring HUMINT collectors to apply their language skills under pressure. Participants operated in authentic scenarios that reinforced vocabulary, improved fluency, and strengthened their ability to interpret regional dialects and slang.

Marne Fury also introduced a new standard of realism in interrogation training. Traditional exercises often treat detainee handling as a secondary element, simplifying language barriers by using English as the default *lingua franca*. In contrast, Marne Fury fully replicated real-world conditions. Participants conducted interrogations in a simulated division holding area that mirrored actual deployment settings. Role players acted as enemy prisoners of war, introducing unpredictability and challenging HUMINT collectors. By interacting with native or fluent language speakers in enemy prisoner of war roles, participants strengthened their language skills without fallback options.

Improving Intelligence Collection and Analysis

The direct use of language skills during interrogations significantly enhanced intelligence collection and analysis during Marne Fury. Without interpretation delays, HUMINT collectors responded quickly, probed deeper into detainee statements, and uncovered unexpected revelations. Linguistic proficiency enabled Soldiers to accurately interpret slang, idioms, and cultural references. This skill improved the precision of intelligence assessments and reduced the risk of miscommunication. Marne Fury demonstrated that integrating organic language capabilities into interrogation teams streamlined intelligence collection, making it more efficient and accurate.

Army doctrine highlights the value of deploying HUMINT collectors fluent in local languages.[4] The doctrine indicates that language proficiency strengthens rapport with detainees, leading to more reliable and actionable intelligence. Marne Fury proved this concept by demonstrating that direct communication enhances both intelligence quality and collection speed.

Department of the Army Support

The Department of the Army Counterintelligence and Human Intelligence Staff Element, also known as the DA G-2X, played a critical role in Marne Fury's success by supporting the Language Infused HUMINT Training pilot. This pilot program paired U.S. Air Force Language Enabled Airman Program, or LEAP, scholars with 3rd Infantry Division HUMINT collectors. The LEAP scholars provided native-language expertise, enhancing the realism and effectiveness of interrogations.[5]

The Language Infused HUMINT Training also partnered with the California Army National Guard to deploy mobile language labs equipped with commercial internet capabilities. These labs allowed HUMINT collectors to receive remote instruction from professors specializing in Russian, Spanish, and French through The Unconventional Training on Request (TUTOR) platform.[6] This continuous language development strengthened Soldiers' skills throughout the field exercise.

The TUTOR program demonstrably improved HUMINT collectors' language proficiency by utilizing a standardized language proficiency rubric and tracking collector progress across multiple interrogation iterations. Analysis of these scores revealed the following:

- **Significant Improvement.** HUMINT collectors demonstrated statistically significant improvement in their average language proficiency scores after each four-hour TUTOR session.
- **Consistent Rate of Improvement.** The program fostered ongoing language development even as proficiency increased, as evidenced by the consistent rate of improvement across multiple iterations.
- **Targeted Skill Development.** A breakdown of rubric scores revealed specific strengths in vocabulary range and accuracy, as well as in fluency and coherence. This indicates that the program's focus on the structuring of questioning, vocabulary building, and pronunciation directly translated into measurable language gains.

The TUTOR program proved especially effective in expanding HUMINT collectors' vocabulary related to military topics. Pre- and post-program assessments demonstrated a significant increase in collectors' ability to understand and utilize military-specific terminology. TUTOR professors' observations and HUMINT collectors' self-reports further corroborated this finding. HUMINT collectors consistently reported that the TUTOR program enabled them to acquire vocabulary absent from their regular language training, directly addressing a critical gap in their linguistic repertoire.

TUTOR professors noted a marked increase in collectors' confidence and fluency when communicating in the target language, particularly during the interrogation simulations. This suggests that the program fosters a more natural and intuitive command of the language, going beyond rote memorization.

The program also demonstrated the value of language exposure compared to active learning. While continued exposure to the target language in the field is undeniably beneficial, structured feedback, task-based practice, and focused instruction appear to be crucial catalysts for accelerated and sustained language acquisition. Future research should examine the program's long-term impact and explore the potential to integrate similar methodologies into future training opportunities.

The TUTOR program successfully integrated language learning with operational tasks. The results suggest that this approach enhances language proficiency and equips HUMINT collectors with specialized vocabulary and communication skills for success.

Meeting Modern Combat's Language Demands

Future military operations will increasingly require language proficiency. Military forces operating in linguistically and culturally diverse environments must communicate effectively with local populations, allies, and detainees. Language barriers delay decision making, hinder cooperation, and obstruct intelligence gathering. Misunderstandings stemming from poor communication breed distrust and jeopardize missions. Marne Fury demonstrated that HUMINT collectors must develop language proficiency to meet modern combat demands.

Marne Fury's success highlights its potential for expansion. The Army can scale this model to other commands, tailoring language requirements to evolving mission needs. This approach offers significant applications for counterterrorism, peacekeeping, and humanitarian operations, where effective communication remains critical. Because it reduces reliance on expensive contract interpreters, the lessons learned during Marne Fury offer long-term cost-saving opportunities. By leveraging existing resources such as native-speaking Soldiers and remote language labs, the exercise minimized logistical expenses. Mobile language labs and online platforms reduce the need for costly, on-site language courses, allowing continuous training without extensive travel. This cost-effective model strengthens HUMINT capabilities without straining budgets.

Conclusion

Marne Fury modernized HUMINT training by integrating language skills into interrogation exercises. This approach improved operational readiness by enhancing communication, increasing realism, and boosting intelligence collection efficiency. Its scalability, cost efficiency, and applicability to future operations position Marne Fury as a valuable training model, ensuring military forces remain adaptable and effective in complex global environments. To maximize the benefits of Marne Fury, the Department of War should expand its implementation across multiple commands. Its cost efficiency, realism, and effectiveness make it a valuable model for joint operations, particularly in linguistically diverse theaters.

Endnotes

1. Beth H. Richardson et al., "Language Style Matching and Police Interrogation Outcomes," *Law and Human Behavior* 38, no. 4 (2014): 357–366, https://doi.org/10.1037/lhb0000077.

2. International Committee of the Red Cross Database, Treaties, States Parties and Commentaries, Convention (III) relative to the Treatment of Prisoners of War. Geneva, 12 August 1949, Article 17–Questioning of prisoners, https://ihl-databases.icrc.org/en/ihl-treaties/gciii-1949/article-17.

3. Laurel Brimbal et al., "The Méndez Principles: Building Rapport and Trust in Interrogations to Elicit Reliable Information," *Just Security*, June 15, 2021, https://www.justsecurity.org/76920/the-mendez-principles-building-rapport-and-trust-in-interrogations-to-elicit-reliable-information/.

4. Department of the Army, Field Manual 2-22.3, *Human Intelligence Collector Operations* (Government Publishing Office, 2006), 11-1. Incorporating administrative changes required by Executive Order 14168, effective on April 25, 2025.

5. Mikala McCurry, "LEAP: The Solution to Language, Culture Barriers in Large-Scale Military Exercises," U.S. Air Force website, October 24, 2023, https://www.af.mil/News/Article-Display/Article/3566792/leap-the-solution-to-language-culture-barriers-in-large-scale-military-exercises/; and Air Force Culture and

Language Center, "LEAP—Language Enabled Airman Program," U.S. Air Force Air University, 2024, https://www.airuniversity.af.edu/AFCLC/Language-studies/.

6. "The Unconventional Training On Request," Yorktown Systems Group, 2024, https://www.theunconventional.com/tutor/.

References

Baker, M. *Translation and Conflict: A Narrative Account*. Routledge. 2006. https://doi.org/10.4324/9780203099919.

CW2 Steven Betancourt leads the human intelligence (HUMINT) analysis cell at Fort Stewart, GA. He has held various positions within strategic, U.S. Army Forces Command, and U.S. Army Training and Doctrine Command assignments at multiple posts, including Fort Bragg, Fort Sam Houston, Fort Drum, and with the 3rd Infantry Division. He served as a senior instructor for the HUMINT Collector Advanced Individual Training Course at Fort Huachuca, AZ, and has completed multiple deployments, including service as a HUMINT collector, desk officer, and deputy HUMINT operations cell for V Corps in Poland.