

INTELLIGENCE SUPPORT TO INFORMATION ADVANTAGE: LESSONS FROM TRAINING IN LIVE ENVIRONMENTS

by Colonel Jonathan S. Steinbach, Major Amy R. Forza,
and Major Scott Fisher (Retired)

Introduction

The U.S. military faces growing challenges in the information domain. While adversaries like Russia and China have adapted quickly to data-driven operations, U.S. forces remain hindered by fragmented doctrine, outdated training models, and a shortage of specialized personnel.¹ Despite warnings in the 2017 and 2022 *National Security Strategies* and the 2018 *Joint Concept for Operating in the Information Environment*, information forces still operate in an ad hoc, inefficient manner.²

To address these gaps, the 151st Theater Information Advantage Group (151 TIOG) developed and assessed a new framework for intelligence support to information advantage (ISIO) through training in live environments. These real-world deployments to U.S. European Command and U.S. Indo-Pacific Command revealed critical intelligence and operational shortfalls, informed new methodologies, and offered a path forward for integrating intelligence into information advantage activities. This article identifies strategic and operational gaps, shares lessons from recent deployments, and presents recommendations to help the Army modernize its approach to data-driven operations and achieve a lasting information advantage.

Role of Intelligence Support to Information Advantage

To strengthen integration between intelligence and information advantage activities, the 151 TIOG created a dedicated ISIO officer position. Unlike traditional intelligence staff officer (S-2/G-2/J-2) roles that support broad warfighting functions, the ISIO officer focuses solely on information advantage activities. Embedded with the planning and targeting teams, the ISIO officer tailors intelligence to support influence operations, military deception, operations security, and cyberspace shaping operations.

These functions enable intelligence to directly inform not just situational awareness but also information advantage activities planning, targeting, and assessment. ISIO officers develop information-specific intelligence requirements, design collection strategies focused on cognitive objectives, and assess how operations affect adversary decision making. This approach aligns intelligence support with Army Doctrine Publication 3-13, *Information*, which emphasizes synchronized intelligence support throughout the execution of information advantage activities.³

During real-world training deployments, ISIO officers used data aggregation tools, trend analyses, and effects-based assessments to deliver actionable intelligence in real time, enhancing synchronization between collection, targeting, and operational outcomes. These methods support the operational guidance in Field Manual 3-0, *Operations*, which emphasizes the application of real-time data across all domains.⁴

Gaps in Information Advantage

Despite strategic guidance, U.S. military doctrine still lacks a unified approach for integrating intelligence with information advantage activities. Several persistent shortfalls are identified in national security and defense publications:

- ◆ **No single, coalescing open-source intelligence (OSINT) proponent.** OSINT lacks doctrinal ownership, limiting integration across the force.⁵
- ◆ **Fragmented information forces.** Unlike logistics, information advantage activities have no centralized oversight, resulting in inconsistent capabilities and institutional inefficiencies.⁶
- ◆ **Limited data analytics.** Intelligence and information advantage activities training rarely includes data science, restricting the use of publicly available information and artificial intelligence-driven tools.⁷
- ◆ **System access barriers.** U.S. Army Reserve and National Guard Soldiers often lack access to sensitive compartmentalized information facilities, the Joint Worldwide Intelligence Communications System, and key mission systems, reducing their contributions to information advantage activities.⁸
- ◆ **Overreliance on simulated training.** Simulations do not prepare Soldiers for the complexity of influence operations. In contrast, training in live environments fosters real-world collaboration and more effective mission readiness.⁹

Training in Live Environments

The 151 TIOG executed four training deployments in fiscal year 2024 to test new approaches for its intelligence support. These included one long-term (22-week) and two short-term (4-week) missions to the U.S. European Command, and a nine-week open-source mission to the U.S. Indo-Pacific Command.

Training in live environments confirmed known strategic gaps and revealed new operational deficiencies. Teams applied skills acquired from their civilian life and training in data analysis and open-source exploitation to meet the demands of modern information advantage activities. In particular, the U.S. Indo-Pacific Command mission underscored the need to modernize information capabilities and exposed doctrinal and training shortfalls.

The U.S. Indo-Pacific Command Deployment. A primary objective of the U.S. Indo-Pacific Command deployment was to improve understanding of adversary operational advances within the human and information domains. The ISIO team discovered that critical operational data from forward civil affairs teams was locked in static PDF reports in a document and content management system, preventing vital civil reconnaissance data from informing trend analysis and cross-regional assessments throughout the greater intelligence enterprise. The inability to store and share information efficiently and comprehensively limited commanders' ability to measure effects or counter adversary narratives.

To close these identified gaps, a team member with Wall Street data analytics experience built automated tools to ingest and visualize reporting across time, geography, and mission lines. Other team members used open-source data to analyze trade patterns, foreign aid, adversary messaging, and public sentiment. Fusing the open-source data with classified reporting, the team identified high-impact partners, platforms, and pathways to support U.S. objectives. Host units praised these products for their speed, clarity, and operational relevance.

The team demonstrated the Army's ability to generate high-impact, data-driven intelligence internally—without outsourcing to contractors. However, this success hinged on individuals' civilian occupational training from outside of the Department of Defense. Because the 151 TIOG is a U.S. Army Reserve unit, its team members brought civilian-acquired expertise and experience in data science and analytics, skills not currently taught in the traditional Army military intelligence institutional training pipeline. These missions show that data analysis is mission-critical for information advantage activities. Army military intelligence will benefit from institutionalizing these skills for the Active component to replicate these effects at scale and build a force capable of thriving in the modern information environment.

The U.S. European Command Deployment. A 151 TIOG ISIO team further demonstrated the operational value of the ISIO approach during a training deployment to the U.S. European Command area of operations. The team focused on strengthening the integration of intelligence into information advantage planning, targeting, and assessment at the operational and strategic levels. They produced cognitive environment overlays, analyzed adversary decision making, and modeled the civil, cyberspace, and psychological domains. Using the SCAME framework's key elements (source, content, audience, media, effect)¹⁰ and center of gravity analyses, they aligned intelligence with nonlethal targeting.

These efforts addressed several previously identified gaps, including the limited availability of data to support cognitive targeting, the insufficient integration of non-kinetic factors into mission analysis, and the persistent disconnect between J-2 intelligence processes and information advantage activities planning requirements. By embedding structured assessments and cognitive-focused intelligence directly into information advantage activities working groups, the U.S. European Command ISIO team demonstrated how intelligence could proactively drive influence, deception, and cyberspace shaping operations within an operational environment. This training further confirmed the need for ISIO officers who specialize in integrating intelligence processes with information advantage activities, providing a model for institutionalizing these practices across future operational planning cycles.

Lessons and Recommendations

The ISIO deployment-based training missions demonstrated that live, data-driven training enables intelligence teams to deliver operational impact that simulations rarely achieve. Additionally, to help institutionalize ISIO practices and address persistent gaps in intelligence support to information advantage activities, we offer the following key findings and recommendations.

Establish a dedicated information warfare career field. Army Chief of Staff General Randy George directed the creation of an Information Warfare Branch, so transformation planning is already underway. As of 2025, this effort has advanced into concept development under the Army's Transformation and Training Command (previously known as the Training and Doctrine Command) with prototype military occupational specialty (MOS) designs expected by fiscal year 2026. The recommendation outlined here contributes directly to that evolving effort.

A formal, dedicated Information Warfare Branch tasked with delivering coordinated cognitive and influence effects might have a structure that mirrors successful past innovations, such as the 1983 creation of the Aviation Branch. The following notional list of recommended MOSs illustrates how the division of expertise, together with specialized training, can close multiple strategic and operational gaps. Suggested MOS designations include—

- ◆ **30B Operations Security Specialist:** Designs and enforces operational security in support of information advantage.
- ◆ **30C Military Deception Specialist:** Plans and executes deception operations to mislead adversaries and protect friendly intent.
- ◆ **30D WebOps Specialist:** Conducts web-based targeting, monitors online influence, and analyzes digital behavior.
- ◆ **30E ISIO Officer:** Integrates intelligence into information advantage activities planning, targeting, and assessment to identify adversary vulnerabilities.
- ◆ **30F ISIO Specialist:** Provides analytic and collection support to information teams focused on influence and deception operations.
- ◆ **30H IO Cyber Specialist:** Supports cyber-enabled information missions and identifies exploitable data sources for decision making.
- ◆ **30O OSINT Specialist:** Collects, analyzes, and operationalizes publicly available information to support information objectives.

Creating this branch will ensure the Army fields a trained, effects-driven workforce equipped to operate in the modern information environment.

Develop data-driven intelligence training pipelines. The Army must develop formal training pipelines that integrate data science, analytics, and OSINT into intelligence training and intelligence support for information advantage activities. Adversaries already use artificial intelligence and machine learning to shape influence operations. In contrast, the Army still relies on more traditional methods that do not address cognitive and informational domains. As identified during the ISIO training deployments, data-driven skills proved crucial for operational success, particularly in analyzing the information environment and developing actionable insights. Findings by the RAND Corporation in 2020 also emphasize that traditional intelligence methods inadequately address the cognitive and informational domains within the information environment.¹¹ Developing structured training in these areas would directly address this critical gap.

Expand training in live environments. Training in live environments delivers greater training and operational impacts than simulations. The ISIO deployment participants trained in real-world conditions and produced actionable intelligence in real time, directly shaping information advantage activities planning. Soldiers developed tools, supported decision making, and learned how to produce measurable outcomes. Their impact led host organizations to request continued collaboration—unmistakable evidence of the value these teams provided. The Army should institutionalize live environment training as recurring training across all components, especially for the Reserve components, ensuring intelligence and information professionals are prepared to support information advantage activities under actual field conditions. During training in live environments, teams achieved positive outcomes in individual and team skills exponentially faster than in simulated environments. Expanding training in live environments across different operational theaters will ensure a more adaptable and skilled information workforce.¹²


Leverage the Reserve components' expertise. U.S. Army Reserve Soldiers played a critical role by applying civilian-acquired skills in data science, analytics, and finance. These capabilities were central to mission success during ISIO training deployments, allowing rapid development of data analysis tools tailored to mission needs. However, the Army's training system does not currently provide Active Duty Soldiers with a means to acquire these data skills. Enhancing integration between the Active and Reserve components would ensure consistent access to critical skills and knowledge that are not always available within the Active Duty force, where these skills are not integrated into training pipelines. The Army should prioritize institutionalizing data-driven competencies and formalize them as core ISIO skills. This would also accelerate learning in the proposed new career fields by uncovering the necessary or desirable skills, acquired through formal training, that are currently unavailable in the Army's schools.

Stand up an Information Forces Command. Finally, structural gaps remain. Although Army Techniques Publication 2-22.9-1, *Publicly Available Information Research and Open-Source Intelligence*,¹³ was published in October 2023, the Army still lacks a centralized proponent responsible for integrating OSINT into force structure, training, and operational planning. The absence of a centralized information command continues to fragment information advantage activities planning and limit intelligence integration. While teams training in live environments overcame these challenges in the field, lasting progress depends on establishing permanent ISIO roles and regular live training across the force. The Army should create a one-star operational command to oversee the manning, training, and deployment of Soldiers supporting information advantage activities. A centralized command would reduce fragmentation, unify doctrine, and ensure integrated delivery of influence, deception, and cyberspace effects across the force. This command should be in the Army Reserve and potentially include multiple components.

Designate the U.S. Army Intelligence Center of Excellence (USAICoE) as the lead for ISIO and OSINT Integration. USAICoE, in coordination with other Army Centers of Excellence, should lead the development of ISIO doctrine, OSINT training, and related career pathways. USAICoE already oversees intelligence instruction and is best positioned to expand Army capabilities in data analytics and cognitive assessment. Assigning USAICoE this role will accelerate the integration of intelligence into information advantage activities at scale.

Conclusion

Through short- and long-term real-world training deployments, the 151 TIOG developed and tested a new ISIO framework. Together with our lessons and recommendations, this framework provides the Army and the broader joint force with a clear path to address the challenges of data and information advantage activities identified in strategic documents, joint studies, think tank reports, and feedback from returning deployers.

We advocate for deliberate institutional reform. Our recommendations range from low-cost adjustments, such as leveraging the unique civilian skillsets of the U.S. Army Reserve and National Guard, to higher-investment initiatives, including new career fields and expanded training pipelines. These proposals align with the existing operational demands placed on Soldiers. The tasks already exist, and the Army would benefit from investing in talent and training aligned with an effects-based approach. We offer these lessons and recommendations to support these efforts and to begin a formalized dialogue about a way forward in this critical area of transformation. 

Endnotes

1. *National Security Strategy* (The White House, 2017), 35, <https://trumpwhitehouse.archives.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf>. The 2017 National Security Strategy described U.S. information efforts as “tepid and fragmented” and “hampered by the lack of properly trained professionals,” reinforcing the need for a doctrinal overhaul in information operations.
2. *National Security Strategy* (2017), 35; *National Security Strategy* (The White House, 2022), 16–18, <https://bidenwhitehouse.archives.gov/wp-content/uploads/2022/11/8-November-Combined-PDF-for-Upload.pdf>; and *Joint Concept for Operating in the Information Environment (JCOIE)* (Joint Chiefs of Staff, 2018), 6–7, https://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/joint_concepts_jcoie.pdf?ver=2018-08-01-142119-830. The 2018 JCOIE states that the U.S. military is “hampered by its policies, conventions, cultural mindsets, and approaches to information” and that adversaries “have adapted rapidly” while U.S. forces remain slow to respond.
3. Department of the Army, Army Doctrine Publication 3-13, *Information* (U.S. Government Publishing Office [GPO], 2023).
4. Department of the Army, Field Manual 3-0, *Operations* (U.S. GPO, 2025), 22–23.
5. Michael Schwille et al., *Intelligence Support for Operations in the Information Environment: Dividing Roles and Responsibilities Between Intelligence and Information Professionals* (RAND Corporation, 2020), https://www.rand.org/pubs/research_reports/RR3161.html; and Brian Cheng, Scott Fisher, and Jason C. Morgan, “Find It, Vet It, Share It: The US Government’s Open-Source Intelligence Problem and How to Fix It,” Modern War Institute at West Point, March 24, 2023, <https://mwi.westpoint.edu/find-it-vet-it-share-it-the-us-governments-open-source-intelligence-problem-and-how-to-fix-it/>.
6. *National Security Strategy* (2022), 20–22.
7. *National Security Strategy* (2017), 3, 20, 22.
8. Timothy Kirschner and Brian McGarry, “The Federated Intelligence Program at the State Level,” *Military Intelligence Professional Bulletin* 40, no. 3: 27–29, <https://mipb.ikn.army.mil/issues/jul-sep-2015>; and Department of Defense, Department of Defense Manual 5105.21, Vol. 3, *Sensitive Compartmented Information (SCI) Administrative Security Manual: Administration of Personnel Security, Industrial Security, and Special Activities* (2012), https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodm/510521m_vol3.pdf?ver=2020-09-15-132603-533. Incorporating Change 2, Effective September 14, 2020.

9. Schwille et al., *Operations in the Information Environment*, 37, 42, 45; and Michael Schwille, Scott Fisher, and Eli Albright, “We Wanted to Implement Data-Driven Operations During an Army Exercise—Here’s What We Learned,” Modern War Institute at West Point, January 24, 2024, <https://mwi.westpoint.edu/we-wanted-to-implement-data-driven-operations-during-an-army-exercise-heres-what-we-learned/>.

10. Press Room, “Strategies to Counter Disinformation and Psychological Operations (SCAME Report),” Disinformation, DISA: Disinformation Social Media Alliance, April 1, 2025, <https://disa.org/strategies-to-counter-disinformation-and-psychological-operations-scame-report/>.

11. Schwille et al., “Intelligence Support for Operations in the Information Environment.”

12. James McNeive, “MCOIOC IO Notes,” Marine Corps Information Operations Center, unclassified staff communication, May 5, 2025.

13. Department of the Army, Army Techniques Publication 2-22.9-1, *Publicly Available Information Research and Open-Source Intelligence* (U.S. GPO, 2023).

COL Jonathan Steinbach is the commander of the 151 Theater Information Advantage Group (TIOG) at Fort Totten, NY. In his 35 years of service, he has held multiple leadership positions, including battalion and group command, and senior staff roles in all three components of the Army across Army Aviation, Infantry, Logistics, and Information Advantage. COL Steinbach holds a bachelor of arts from the University of California at Berkeley, a master of public administration from the University of Washington, and a master of strategic studies from the U.S. Army War College.

MAJ Amy Forza is a military intelligence officer serving as the intelligence support to information advantage officer for the 151 TIOG. She holds a master of science in digital scholarship from the University of Oxford. MAJ Forza served in Afghanistan and Qatar. Her current work focuses on integrating intelligence and data analysis into information advantage activities to enhance mission effectiveness.

MAJ Scott Fisher (retired), PhD, is a professor of security studies at New Jersey City University, where his research focuses on information warfare, U.S. security challenges in East Asia, and open-source intelligence. His previous service in the U.S. Army was primarily with the 151 TIOG, with deployments as an information advantage activities officer to Afghanistan, East Africa, and U.S. European Command in Germany.