



Mission Command Intelligence in Multi-Domain Operations

by Lieutenant General Scott D. Berrier

Introduction

The Army's new operating concept, multi-domain operations, describes how our Service contributes to the joint force's efforts to deter and defeat near-peer and peer aggression in both competition and conflict—our primary task as defined by the 2018 National Defense Strategy. This concept signifies a seismic shift from the counter-insurgency-centric approach the Army has followed in prosecuting multiple conflicts in the Middle East and Africa over the past 17 years. In order for the Army to succeed in multi-domain operations, the Military Intelligence Corps must evolve, innovate, and modernize in order to enable the Nation's premier ground force to achieve overmatch against our Nation's adversaries and win. Mission Command Intelligence (MCI) is our framework to achieve this goal by the year 2028.

Strategic Context

Our operating environment is changing rapidly, with strategic competition between nation states now surpassing violent extremism as the central challenge to American prosperity and security. Russia has recovered from more than two decades of degraded military capability and capacity by modernizing weapon systems and reforming its armed forces while evolving niche capabilities for hybrid warfare operations. Russia has coupled this modernization with a foreign policy stance designed to control its near abroad and simultaneously re-establish Moscow's position as a global power. China, bolstered by the world's second largest economy, has extended its global influence through the Belt and Road Initiative. With this initiative, China has skillfully integrated economic, diplomatic, and informational instruments of national power while rapidly improving

its military force projection capabilities and establishing its first enduring overseas bases. These efforts now enable China to contest United States and allied power throughout East Asia, the South China Sea, and beyond. Beijing's adroit posturing of its newfound capabilities poses a significant challenge to the world order cultivated by the victors of the Second World War. In addition to Russia and China, Iran and North Korea threaten the interests of the United States and our allies by fielding forces enabled by advanced technology, backed by weapons of mass destruction, and driven by regimes whose objectives are in sharp contrast to American values. Additionally, violent extremist organizations will remain a persistent menace to U.S. interests for the foreseeable future sustained by both state and non-state actors. In order to mitigate these threats, we must accelerate our ability to understand changes in this environment, enabling commanders to outpace our adversaries' decision cycles.

Multi-Domain Operations Overview

Army forces, as an element of the Joint Force, conduct [multi-domain operations] MDO to prevail in competition; when necessary, Army forces penetrate and dis-integrate enemy anti-access and area denial systems and exploit the resultant freedom of maneuver to achieve strategic aims (win) and force a return to competition on favorable terms.

TRADOC Pamphlet 525-3-1¹

The Army's new concept of multi-domain operations described in TRADOC Pamphlet 525-3-1, *The U.S. Army in Multi-Domain Operations 2028*, addresses how our Service will solve the primary problem posed by near-peer and peer adversaries' standoff in all domains—space, cyberspace, air, sea, and land.

Standoff separates the joint force in time, space, and function, in both competition and conflict. Political action, operations in cyberspace, and information and influence campaigns form just some of the means our adversaries leverage to achieve this separation at the strategic level while setting advantageous conditions at the operational and tac-

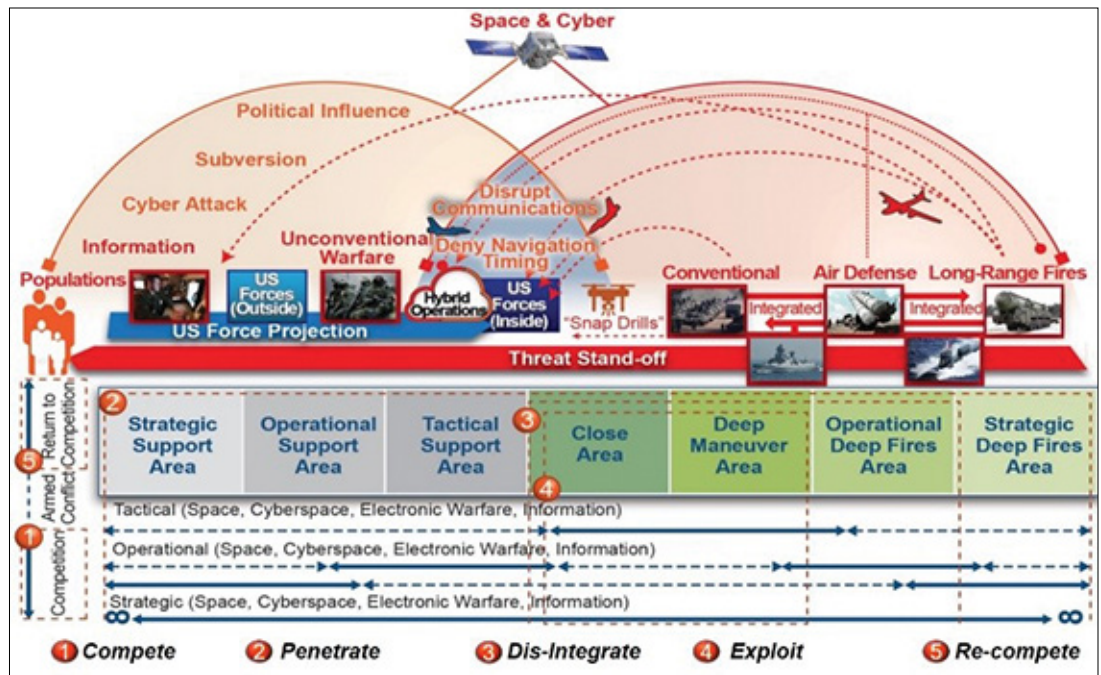


Figure 1. Threat Problems Superimposed on the Multi-Domain Operations Framework²

tical levels. Deep-sensing intelligence, surveillance, and reconnaissance (ISR) systems tied to long-range integrated air defense systems and ballistic and cruise missile forces form antiaccess and area denial (A2AD) conditions that provide standoff at the operational and tactical levels. U.S. Army forces must maintain readiness during extended periods of competition while preparing to penetrate and disintegrate threat A2AD systems early in conflict, create windows of opportunity and periods of advantage, and exploit gains in order to resolve conflicts on terms favorable to American interests. Army intelligence is vital to supporting U.S. land power and supporting the joint force in order to prevail in this environment.

Mission Command Intelligence Overview

MCI is the Army intelligence enterprise's overarching framework to achieve an end state of a ready Army intelligence team supporting mission command against all threats in multi-domain operations by 2028. It aligns intelligence requirements, planning, development, and resourcing efforts with the Army's multi-domain operations concept. MCI will enable commanders to achieve decision superiority with the speed, precision, and accuracy required to integrate and synchronize combat operations in multi-domain environments.

MCI's essential components are sensors, data, and analysis enabled by a cloud-based network architecture. These components empower intelligence professionals to execute doctrinal intelligence process functions assisted by the advantages of advanced technology and cutting-edge capabilities. Accordingly, MCI provides commanders the essential

Mission Command Intelligence is the Army intelligence enterprise's overarching framework to field a ready Army Intelligence team supporting mission command against all threats in multi-domain operations by 2028.

MCI Components Describe Characteristics Driving Our MI Modernization Priorities

Sensors

- Detect and collect advanced signatures in all domains
- Penetrate, collect, and survive in A2 / AD environments
- Collaborative capabilities across terrestrial, aerial, and space layers
- Automated sensor fusion across disciplines
- Direct sensor reporting to data architectures & fire control systems

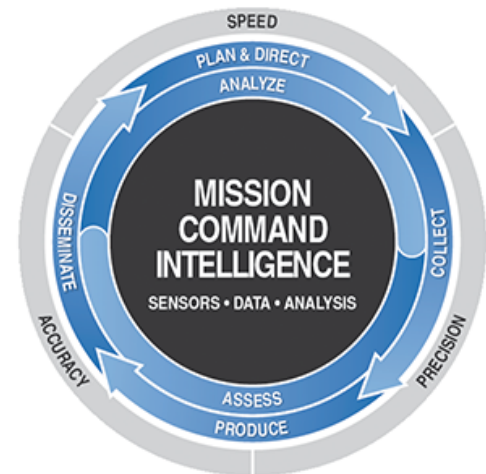
Data

- Assured access to data at echelon and across theaters of command
- Ingest and process data from DoD, IC, commercial, open source and PAI
- Common DoD / IC standards shared throughout DoD, IC, allies and partners
- Seamless transitions from competition to conflict in all environments

Analysis

- Analyst functions integrated within COE
- High compute processing (AI / ML) automates fusion of discrete signatures
- Automated IPB and collection management processes
- Analytic workflows support dynamic modeling and forecasting
- Advanced tradecraft supported by intuitive analyst interfaces
- Rapid generation of user-based tools and applications (DevOps)

A2 antiaccess	DevOps development operations
AD area denial	DoD Department of Defense
AI artificial intelligence	IC intelligence community
COE common operating environment	IPB intelligence preparation of the battlefield



MCI Increases the Speed, Precision, and Accuracy of the Intelligence Process

MCI	Mission Command Intelligence
MI	military intelligence
ML	machine learning
PAI	publicly available information

Figure 2. Mission Command Intelligence³

means to synchronize other warfighting functions and deliver sound, timely decisions, posturing friendly forces with decisive advantage. In the context of multi-domain operations, MCI supports the Total Army's effort to achieve convergence⁴ across time, space, and in all domains.

Sensors

Army Vision 2028 calls for units from brigade through corps to possess the ability to conduct sustained ground and aerial ISR, electronic warfare, and cyberspace operations. By 2028, the Army's access to sensors must enable commanders to illuminate our adversaries' diverse array of formations and capabilities through the depth of the battlefield, exposing vulnerabilities we can exploit at the time, place, and in the domain of our choosing. MCI requires sensors and platforms adaptable to any operating domain, A2AD environments, and contested electromagnetic spectrum conditions while remaining capable of collecting against signatures generated by evolving threats. Sensors must penetrate the battlespace in greater depths than the maximum effective range of enemy A2AD systems. The robust use of human intelligence, as a deep sensor, by conventional and special operations forces will enable tipping and cueing, defeat spoofing and deception, and provide alternate collection in a contested or degraded electromagnetic environment. This framework allows the application of enterprise intelligence capabilities in mass at each echelon. These capabilities are deployable, scalable, and designed to provide commanders

with the timely, accurate, and precise situational awareness they need to fight and win.

Data

Army, joint, and national sensors will produce data in volumes and at velocities that will overwhelm cumbersome legacy processing systems. Commercial collection assets and open source information will only add to this challenge. Consistent access and discoverable data require common data configuration and reporting standards within the Army intelligence enterprise and the intelligence community. Common formatting, standards, and security protocols establish the foundation for seamless collaboration and sharing between all Services and the intelligence community, and facilitate greater forward momentum in our efforts to develop cloud-based networks. We will weave these standards into the fabric of our data technologies before integrating them into our networks. This design discipline will sustain continuity and consistency of access for all consumers operating on any platform. Army intelligence Soldiers, Civilians, and supporting contractors must leverage their access to data in order to increase the speed, precision, and accuracy of their analysis and targeting support to commanders at all echelons on the multi-domain operations battlefield. Dedicated data scientists⁵ must be integrated at echelon in order to facilitate the methods by which our forces ingest, curate, and process data into information suitable for analysis.

The key to converging capabilities across all domains, the [electromagnetic spectrum] EMS, and the information environment is high-volume analytical capability and sensor-to-shooter links enabled by artificial intelligence, which complicates enemy deception and obscuration through automatic cross-cueing and target recognition.

TRADOC Pamphlet 525-3-1⁶

Analysis

In collaboration with our joint Service partners, the Total Army intelligence enterprise must evolve processing, exploitation, and dissemination (PED) data competencies in both competition and conflict. Project Maven's integration with the Army PED enterprise at Fort Gordon, Georgia, represents one of the first steps toward this objective. By 2028, we will have integrated artificial intelligence (AI) and machine learning algorithms into our processes, reducing analytic cognitive burden. We will develop intuitive analyst-system interfaces nested with the Army's Command Post Computing Environment. Doing so will enable our Army to rapidly field tools and applications our Soldiers can configure to their specific roles and functions. These efforts are designed to enhance our analysts' efficiency and effectiveness in applying critical thinking and analytical judgment, based on training and experience, to their assessment of the multi-domain operations battlefield.

Analytic initiatives must remain responsive to the demands of a changing operational environment. They will increasingly draw upon solutions designed through the expertise of a growing talent pool of Soldiers, lessening Army reliance on commercial-sector providers. Our force must incorporate DevOps⁷ practices in order to increase the rate at which software and analytic development interacts with users to deliver actionable tools. DevOps at echelon will be instrumental in enabling intelligence professionals to employ advanced analytics at the same pace as intelligence requirements change in accordance with the unpredictable operational environments we anticipate. These actions will support the creation and management of a global integrated common intelligence picture, which also describes adversarial intelligence collection for counterintelligence purposes.

Enabling Architecture

Secure data and networks must ensure connectivity and data access appropriate to each echelon of command, with seamless transitions from home station to the forward edge of battle. By 2028, the Army intelligence warfighting function must have universal access to secure cloud-based data. Leveraging cloud architectures, our multidiscipline intelligence teams will access data for processing and ex-

ploitation, and disseminate their intelligence products with unprecedented reach using the same architecture. In the event our network is degraded, intermittent, or limited, deployable cloud nodes will sustain our forces with data pertinent to their mission and environment.

Visualizing Mission Command Intelligence

MCI's essential components are applicable at all levels of command and throughout the depth and breadth of the multi-domain operations battlefield framework. At the tactical level, S-2s will leverage AI and data from deployable cloud nodes to expeditiously progress through the manpower-intensive steps of the intelligence preparation of the battlefield process. When describing battlefield effects, AI will assist analysts in rapidly producing an automated modified combined obstacle overlay (MCOO) while dynamically updating the product as factors change in the operational environment. This system will process weather forecasts and incorporate terrain factors such as elevation, slope, vegetation, and hydrology to automatically adjust for cross-country trafficability and anticipated rates of movement, and will refine assessed ranges of observation for both friendly and threat forces. This "live action MCOO" will allow analysts to focus time and energy on evaluating the threat and determining threat courses of action. After the S-2 develops the threat course of action, AI will identify potential changes to the course of action in real time. For example, if a destroyed bridge or other obstacle degrades a proposed enemy axis of advance, algorithms will identify alternate routes with corresponding time-phase lines. These AI-derived deviations within each threat course of action will guide named area of interest development and improve ISR collection planning. This concept is no different from the mapping and route planning applications we use on our smart phones today to account for traffic, weather, and other conditions. We use these tools in everyday life to make decisions. Using the most accurate information available to us, we then apply human experiential judgment to select the best course of action.

At both the tactical and operational level, MCI will be decisive in supporting targeting by increasing the speed, accuracy, and precision with which commanders are able to drive kill chains focused on high-value and high-payoff targets. AI will assist S-2s and targeteers by automatically correlating discreet signatures detected by multi-domain sensor systems, across all intelligence disciplines, rapidly focusing collection on named areas of interest developed through processes similar to the S-2 vignette on the next page. As analysts progress more rapidly through the intelligence preparation of the battlefield cycle and develop more

precise collection plans, modernized ISR sensors will be able to provide high-fidelity targeting information to support long-range precision fires in the deep maneuver and operational deep fires areas of the multi-domain operations framework. This capability could be employed in the following operational setting.

Artificial Intelligence Assists S-2s and Targeteers

A multi-domain task force (MDTF) commander is tasked with disintegrating an enemy A2AD network established by the threat's integrated fires command. The network is composed of long-range air defense forces and land attack missiles tied together by digital mission command systems. In order to accomplish this mission, the MDTF must sense, identify, and target the command and control assets associated with the integrated fires command headquarters, and its subordinate SS-26 short-range ballistic missile and SA-21a surface-to-air missile brigades. The MDTF S-2's collection plan specifies that the command and control vehicles associated with the integrated fires command are high-value targets, each with unique visual, electromagnetic, thermal, and cyberspace signatures.

Essential to the dis-integration effort is continuous refinement of intelligence through multiple domains to enable the Joint Force to see or stimulate and strike the enemy's remaining anti-access and area denial systems.

TRADOC Pamphlet 525-3-1⁸

Drawing from data in a deployable cloud node, AI algorithms search for multidiscipline intelligence reporting associated with these unique signatures, rapidly correlating seemingly disparate information into cohesive reports. This process significantly improves the S-2's ability to eliminate redundant reporting while allowing analysts to confirm templated enemy assets on the situation map, all with greater precision. Using this knowledge, the MDTF commander will be able to employ advanced sensors, such as drone swarms or expendable artillery-delivered unmanned aircraft systems, to collect precise locational information. This information can be injected directly into long-range precision fires delivery systems accurately conducting

near-peer and peer competitors, creating decision space for strategic leaders. In all cases, multi-domain analysis platforms, fusing all intelligence disciplines, enabled by cyberspace operations must employ AI analytics against massive quantities of data to rapidly identify, neutralize, and defeat threats to our force at home and abroad.



Photo by U.S. Navy P01 Danica Sirmans

The Army's multi-domain task force operates from a tactical command post as part of Valiant Shield 2018.

kinetic or non-kinetic fires neutralizing or destroying the high-value targets. Battle damage assessment will be improved as the S-2 leverages AI analytics to rapidly correlate indicators provided by a multidiscipline array of networked sensors to confirm the long-range precision fires' effects successfully destroyed the target. Taking into account the battle damage assessment and targeting effects, AI may also assist in supporting rapid follow-up strikes by using predictive analytics to template the enemy's reaction upon the loss of critical systems or capabilities.

Long-range ground fires offer a responsive strike capability (cued by intelligence within minutes), with the capacity to overwhelm point defenses and strike targets over larger areas.

TRADOC Pamphlet 525-3-1⁹

The multi-domain operations concept is predicated upon our Nation's ability to generate and project power from the continental United States, making MCI's components vital to Army intelligence operations in the strategic and operational support areas in the competition phase as well as during conflict. Adversaries seek to acquire sensitive technologies and to disrupt supply chains and force generation/projection platforms, requiring tailored sensors to meet these threats. Adversary espionage operations and insider threats must also be subject to counterintelligence detection and neutralization in accordance with appropriate legal authorities to enable the protection of critical technologies. Special operations forces will operate throughout all areas of the multi-domain operations framework, leveraging MCI's components to counter adversary gray-zone operations by illuminating threat information campaigns, exposing covert actors, and attributing clandestine shaping operations to

The Way Forward

MCI is not only a framework; it is a call for action and must drive modernization requirements and stimulate innovation. MCI will lead us to field new equipment and systems while empowering our Soldiers and Civilians to develop creative solutions to emerging challenges. The military intelligence generating force, including the U.S. Army Intelligence Center of Excellence and our military intelligence teammates within Army Futures Command, must ardently define and drive these requirements to develop, prototype, test, and field ISR systems at a pace that ensures they will remain relevant and enable Army forces to achieve and maintain technical overmatch in comparison to our peer competitors. Technology protection is paramount to this effort. The generating force must also assess our current military intelligence organizations and modify force design to best position intelligence systems with other warfighting formations


for operations in contested environments. Institutional training and development will ensure our Soldiers and Civilians are prepared to provide a decisive human advantage during MCI-enabled multi-domain operations in both competition and conflict.

The operating force, U.S. Army Intelligence and Security Command, U.S. Army Forces Command, U.S. Army Special Operations Command, and those forces under the operational control of Army Service component commands, will employ modern capabilities to sense throughout the depth and breadth of the operational environment, in all domains, and deny the enemy's ability to do the same. MCI sensors, engaging all intelligence disciplines, will provide volumes of data that will feed the cloud-based architecture and enhance accessibility by all. Analysts will process this data into information and provide accurate and precise intelligence assessments using platform-agnostic user interfaces that are directly incorporated into the future Command Post Computing Environment.

Despite these technological advancements, no amount of technology will replace the Military Intelligence Corps' greatest resource—the experience, judgment, and intuition of highly trained men and women who make up our corps. Fundamentals-based training is vital to ensuring that doctrinal skillsets are thoroughly inculcated within our formations, at each level of professional military education. Furthermore, live, virtual, and constructive training environments called for by the Military Intelligence Training Strategy must stimulate innovation and instill critical thinking throughout our team.

Conclusion

MCI enables mission command in multi-domain operations by the year 2028 by rapidly organizing and analyzing historic and current collected data from all sources, providing relevant conclusions for commander's decision-making processes and multi-domain targeting. Our ability to leverage secure data in all formations in degraded, intermittent, and limited environments is vital to enabling analysts to develop accurate assessments for their commanders and supported forces. Sensors, capable of detecting advanced signatures throughout the depth and breadth of the multi-

domain operations battlefield framework, will feed our cloud-based architecture, allowing us to employ AI analytics. These AI tools will enable our analysts to efficiently apply their training, experience, and judgment, resulting in timely and accurate intelligence assessments. MCI will not replace the fundamental principles of the intelligence process and other doctrinal processes; rather, it will empower our team to harness technological advancements to accomplish the mission. Doing so will ensure our Army can deter, fight, and win on any battlefield, against any foe, now and into the future. 

Endnotes

1. Department of the Army, Training and Doctrine Command (TRADOC) Pamphlet 525-3-1, *The U.S. Army in Multi-Domain Operations 2028* (Fort Eustis, VA: TRADOC, 6 December 2018), 17; emphasis added.
2. *Ibid.*, 16.
3. Illustration provided by COL Justin Haynes, U.S. Army, Deputy Chief of Staff, Intelligence, Initiatives Group.
4. "Convergence is rapid and continuous integration of capabilities in all domains, the [electromagnetic spectrum] EMS, and the information environment that optimizes effects to overmatch the enemy through cross domain synergy and multiple forms of attack all enabled by mission command and disciplined initiative." Department of the Army, TRADOC Pamphlet 525-3-1, 20.
5. Bradley M. Knopp, Sina Beaghley, Aaron Frank, Rebeca Orrie, and Michael Watson, *Defining the Roles, Responsibilities, and Functions for Data Science Within the Defense Intelligence Agency* (Santa Monica, CA: RAND Corporation, 2016), 17-21.
6. Department of the Army, TRADOC Pamphlet 525-3-1, 38; emphasis added.
7. "DevOps (a clipped compound of "development" and "operations") is a software engineering culture and practice that aims at unifying software development (Dev) and software operations (Ops). The main characteristic of the DevOps movement is to strongly advocate automation and monitoring at all steps of software construction, from integration, testing, releasing to deployment, and infrastructure management. DevOps aims at shorter development cycles, increased deployment frequency, and more dependable releases." D. Jeya Mala, *Integrating the Internet of Things Into Software Engineering Practices* (Hershey, PA: IGI Global, 2019), 16.
8. Department of the Army, TRADOC Pamphlet 525-3-1, 38; emphasis added.
9. *Ibid.*, 33; emphasis added.

LTG Berrier has served as a "2" at every level in the Army from battalion through corps. He commanded military intelligence formations at Fort Ord, CA; Fort Wainwright, AK; Fort Drum, NY; the Republic of Korea; and Fort Huachuca, AZ. His joint assignments include U.S. Central Command, Special Operations Command-Central, Combined Joint Task Force-180, Combined Joint Task Force-76, Multi-National Corps-Iraq, U.S. Forces Korea, International Security Assistance Force, and Resolute Support Headquarters. He currently serves as the Army's 46th Deputy Chief of Staff for Intelligence, G-2.