



# Identity Intelligence Contributes to Multi-Domain Operations

by Mr. Peter Baber, Ms. Pamela Baker, and  
Lieutenant Colonel Mark Dotson (Retired)

## Introduction

U.S. Army identity intelligence (I2) is a capability to identify foreign persons of military interest. It distinguishes individuals from each other; discovers new threats and links them to other people, places, and things; and characterizes individuals, entities, groups, networks, and populations of interest. I2 fuses data and information with behavioral, reputational, biometrics, forensics, and other associated identity signatures in order to identify military threat persons of interest. The Army's I2 capability has evolved beyond the counterterrorism and counterinsurgency operational environment (OE) into an "all-threats" enduring requirement. In today's era of multi-domain operations (MDO), I2 provides the Army with an unprecedented insight into potential and existing threats and their plans, intentions, and networks. I2 also supports the force on the battlefield. The Army maintains and sustains its I2 capability at echelons above corps, through Headquarters, Department of the Army, G-2, and the U.S. Army Intelligence and Security Command, primarily at the National Ground Intelligence Center.

## Capabilities of Identity Intelligence

I2 identifies and monitors foreign threat-based persons, groups, and networks of military interest and their supporting relationships that are critical to the success of weapons, plans, strategy, and operations; it also identifies and monitors their development, proliferation, and deployment. I2 provides the foundational intelligence that enables the development of a common operational picture (COP) of the OE human layer, determining friend or foe. This includes the ability to maintain situational awareness of connections and changes of key persons of interest of great power competitors, rogue states, violent extremist organizations, and transnational criminal organizations, as well as their proxies, associates, and allies. I2 also identifies individuals and populations that are either vulnerable to malign influence or receptive to building partner-nation capacity.

Imperative to the success of I2 in the conflict phase is conducting I2 operations "left of conflict" (i.e., early in an engagement) by establishing foundational capabilities, including driving collections, and conducting engagements that leverage foreign-partner and U.S. interagency relationships. This includes forensic, intelligence, and biometric partnerships, practiced in joint-combined exercises and executed in cooperative operations, thereby building partner-nation capacity and enriching foundational intelligence. Some means include—

- ◆ Developing the environment to establish foreign partner information and intelligence sharing and leveraging current agreements.
- ◆ Conducting and collaborating on activities to collect, analyze, and disseminate information about foreign individuals and networks of military interest and their capabilities.
- ◆ Collaborating with foreign and U.S. interagency partners to monitor foreign persons of military interest.
- ◆ Driving collections, evaluating, and analyzing identity and biometric-match information.
- ◆ Confirming the identity of non-attributed foreign individuals and forces of military interest, monitored and disseminated via I2 analytical applications, such as the Biometric Identity Intelligence Resource/Identity Intelligence Analytic Resource and the Department of Defense (DoD) Biometrically Enabled Watchlist, to establish the foundational layer of military threat persons of interest, the COP of the OE human layer.
- ◆ Using weapons technical intelligence to collect, exploit, analyze, and disseminate information on foreign persons of military interest and their capabilities and attribute them to threat-based devices.
- ◆ Tracking adversaries' and other actors' surreptitious activities, in particular malign influence efforts.

## Multi-Domain Operations

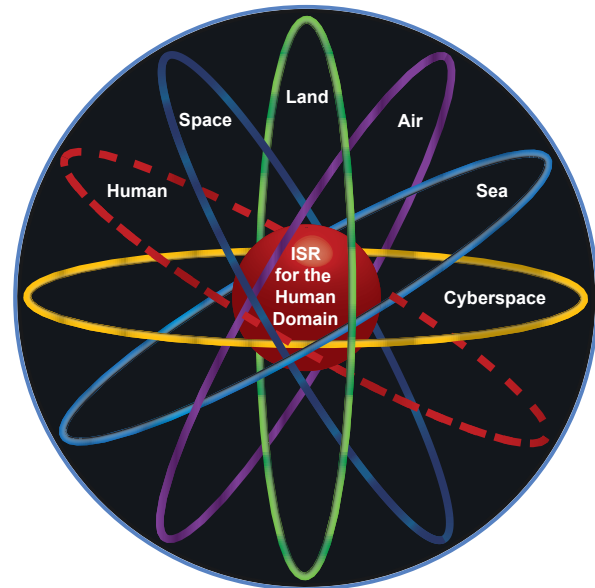
LTG Eric J. Wesley, U.S. Army Futures Command Deputy Commanding General and Director, Futures and Concepts Center, describes MDO as “how the Army envisions a joint warfighting concept that will bring to bear all of the fire-power, both kinetic and non-kinetic, to help the U.S. military regain superiority in what is increasingly becoming a contested, access-denied world of near-peer competitors such as China and Russia.”<sup>1</sup> U.S. Army Training and Doctrine Command (TRADOC) describes MDO as “designed to achieve U.S. strategic objectives articulated in the National Defense Strategy, specifically deterring and defeating China and Russia in competition and conflict.”<sup>2</sup> MDO optimizes effects from across multiple domains identified in joint Service doctrine—land, sea, air, space, and cyberspace—as well as the electromagnetic spectrum and the information environment. A shared trait among the domains, electromagnetic spectrum, and information environment is people—the human element. Humans make decisions and make mistakes. Humans design, deploy, and operate weapons and war plans. According to MDO, “at some point, all the abstract elements (cognitive, virtual, informational, and human) demonstrate their effects physically at a place or in an area through a system or people,”<sup>3</sup> and those systems are designed, proliferated, deployed, and operated by people. Identity intelligence—

- ◆ Provides the “so what” that distinguishes individuals from each other (identity resolution).
- ◆ Discovers new threats (identity discovery) and links them to other people, places, and things (identity/device attribution).
- ◆ Characterizes an individual or network for kinetic and non-kinetic outcomes, supporting the National Defense Strategy and Army’s strategic roles.

JP 5-0, *Joint Planning*, states that the OE is the composite of the conditions, circumstances, and influences that affect the employment of capabilities and bear on the decisions of the commander, encompassing physical areas and factors of all domains. Included within these areas are the adversary, friendly, and neutral actors relevant to a specific joint operation. The OE includes the human element because a human aspect is present in each domain. Understanding the OE, including the human aspect of the domains, helps the commander to better identify the problem; anticipate outcomes; understand the results of various adversary, friendly, and neutral actions; and understand how these actions affect the military end state.<sup>4</sup>

### Identity Intelligence (I2) is the ISR for the “Human Domain”

There is a human aspect to every domain: land, sea, air, space, cyberspace, the electromagnetic spectrum, and information environment



Humans make decisions; make mistakes; design, deploy proliferate, and operate weapons and war plans

Army I2 identifies foreign persons of military interest; it distinguishes individuals from each other, discovers new threats, links them to other people, places, and things, and properly characterizes the human element, sometimes non-doctrinally characterized as the “human domain”

Although MDO is a new and evolving operational warfighting concept, in 2012 the 38<sup>th</sup> Chief of Staff of the Army retired GEN Raymond Odierno stated, “The world has always been defined by uncertainty and change, but in reality the fundamental nature of war remains the same—a struggle to influence key terrain, populations and governance. Preventing conflict is better than reacting to it, and to prevent it you must understand its causes, but understanding is best gained through presence, presence on the ground. Understanding the human dimension and human domain... We must never forget that conflict in any form at its core is a human endeavor.”<sup>5</sup> Army I2 properly characterizes the human element, sometimes non-doctrinally characterized as the human domain.

TRADOC Pamphlet 525-3-1, *The U.S. Army in Multi-Domain Operations 2028*, states that to be successful in the complex, lethal, and chaotic MDO environment, the Army must build trusted teams of professionals that thrive in ambiguity and chaos. These teams are empowered through a doctrine

of mission command to rapidly react to threats and opportunities based on a commander's intent.<sup>6</sup> I2 can identify—

- ◆ Foreign individuals critical to adversarial success in MDO.
- ◆ Personalities who author, define, and field military plans and doctrine.
- ◆ Commander's intent.
- ◆ Personalities who successfully thrive in ambiguity and chaos.

### Identity Intelligence Addresses the Multi-Domain Problems

According to TRADOC, we must solve five multi-domain problems to meet the strategic objectives of MDO. I2 can contribute to resolving each of these problems.

The first problem is competing to defeat aggression short of armed conflict and to deter conflict. Great power competitors and rogue states continue to use gray-zone tactics (political, economic, and hybrid warfare) short of armed conflict. These tactics include exploiting economic and diplomatic levers, conducting information confrontation, and using proxies and associates to undermine and fracture U.S. partnerships and U.S. access globally. Rather than reacting late, we must recognize that the early identification and monitoring of malign actors and the identification of other individuals driving these initiatives are critical to the success of MDO and will contribute to defeating aggression and deterring conflict.

The second and third problems are penetrating and later dis-integrating enemy antiaccess and area denial (A2AD) systems to enable tactical, operational, and strategic maneuver. Crucial to success against these problems in the armed conflict phase of MDO is the application of I2 before conflict (during the competition phase). This involves building partner-nation capacity and enriching foundational intelligence by establishing a foundational layer of military threat persons of interest and the COP of the OE human layer.

The fourth problem is exploiting freedom of maneuver to defeat the enemy and achieve U.S. strategic objectives. I2 identifies foreign individuals critical to adversarial success in MDO, including personalities who define and establish adversarial plans and doctrine, effectively execute commander's intent, and thrive in ambiguity and chaos.

The fifth problem is re-competing to consolidate gains and expand the competitive space to enable policy makers to resolve the conflict. For almost 18 years, the Army has effectively applied its I2 capability to stability operations in alignment with the re-compete phase.



Multi-Domain Problems

### Phases of Multi-Domain Operations

MDO has three phases: competition, armed conflict, and return to competition. To be successful, we must defeat adversaries and achieve strategic objectives in all three.

**Competition.** The application of I2 before conflict (during the competition phase) is key to identifying the individuals and networks of interest who are critical to adversarial success in MDO, including understanding their development, proliferation, and deployment of weapons, plans, and strategy. In the competition phase of MDO, the joint force expands the competitive space through active engagement to counter malign influence, unconventional warfare, and information warfare directed against partners. These actions simultaneously deter escalation, defeat attempts by adversaries to “win without fighting,” and set conditions for a rapid transition to armed conflict. LTG Wesley said, “If there’s a word that you want to remember in terms of identifying the challenges we face within the pacing threats, it is the word ‘standoff’...We talk about this in two periods. The competition period and the conflict period, and what we find is our peers are fully engaged in the first layer of standoff by investing in efforts of democratic elections. Not only U.S. elections but Brexit, Catalonia and others, and that becomes the first layer of standoff.” “Deterrence should be the first available option but ‘is challenged’ because the threat of massive retaliation loses its values if adversaries are achieving their operational and strategic objectives left of conflict.”<sup>8</sup>

Early engagement is a key aspect not only of MDO success but also of the success of I2 in MDO, both for the United States and its adversaries. According to TRADOC Pamphlet 525-3-1, since war is fundamentally and primarily a human endeavor, the United States must work with partners to address the cognitive aspects of political, human, social, and cultural interactions to achieve operational and national

objectives. Establishing capabilities early in an engagement (i.e., “left of conflict”) is crucial to I2 success in MDO, including integrating I2 into concept plans and operation plans. This includes leveraging foreign-partner relationships “left of conflict” for forensic, intelligence, and biometric partnerships. These foreign-partner relationships are practiced in joint-combined exercises and executed in cooperative operations, to build partner-nation capacity and enrich foundational intelligence. Also important is establishing the foundational layer of military threat persons of interest and developing the COP of the OE human layer (foreign persons of military interest in the “human domain” of the OE) executed by I2 operations and disseminated through Biometric Identity Intelligence Resource/Identity Intelligence Analytic Resource and the DoD Biometrically Enabled Watchlist. Army I2 plays a key role in identifying great power competitor malign influence actors and activities. The ability to identify individuals, groups, and populations either vulnerable to malign influence or receptive to building partner-nation capacity can defuse the effects of great power competitor malign influence and information warfare.

**Armed Conflict.** In the conflict phase of MDO, the joint force defeats aggression by optimizing effects from across multiple domains at decisive spaces to penetrate the enemy’s strategic and operational A2AD systems, dis-integrate the components of the enemy’s military system, and exploit freedom of maneuver necessary to achieve strategic and operational objectives that create conditions favorable to a political outcome.

Once again, establishing I2 capabilities “left of conflict” is crucial to I2 success in MDO. We can do this by building partner-nation capacity and enriching foundational intelligence by establishing the foundational layer of military threat persons of interest, the COP of the OE human layer. “Left of conflict” identity discovery of foreign intelligence and special operations personnel who may operate in friendly or allied spaces during conflict is included in that layer. A body of evidence states our adversaries are effectively using engagements to shape the field and are establishing their I2 foundational layer “left of conflict.” If we wait until armed conflict to establish the I2 foundational layer, it will be too late.

Army FM 3-0, *Operations*, describes armed conflict with great power competitors as intense, brutal, complex, and chaotic. This conflict will include noncombatants and will likely be in and around large cities, with adversarial use of terror, criminal activity, and information warfare.<sup>9</sup> Warfare results in the movement of civilians and stresses the resources of nations. Current counterterrorism and coun-


terinsurgency (non-great power competitor) conflicts, according to the United Nations, have resulted in the highest number of people fleeing conflict since World War II. Refugee sites are exploited to harbor terrorists and to radicalize and recruit new members. I2 can support the rule of law and security to identify friend or foe, to verify individuals authorized to enter refugee and internally displaced persons sites, and to identify and exclude threat personalities (criminal and radical) attempting to exploit those sites. In a similar manner, we can use I2 to support noncombatant evacuation operations. We have used I2 effectively at coalition counterterrorism and counterinsurgency detention facilities, and similarly we should use I2 for enemy prisoners of war to establish a baseline identity, confirm identity, and identify deceptive individuals.

The United States will be required to penetrate and dis-integrate enemy A2AD systems to enable tactical, operational, and strategic maneuver in armed conflict. Again, we can address this through the application of I2, “left of conflict.” I2 has the ability to provide insight on adversarial force modernization that threatens Army and DoD modernization priorities, supports the protection of U.S. critical technology, deters the theft of technologies, and potentially slows or prevents the integration of DoD technology into adversarial systems.

**Return to Competition.** In this phase, the joint force consolidates gains and deters further conflict to allow the regeneration of forces and the re-establishment of a regional security order aligned with U.S. strategic objectives. While the Army’s I2 capability has evolved beyond counterterrorism and counterinsurgency applications, we have applied it liberally and effectively to stability operations in alignment with the re-compete phase. The ability to identify individuals, groups, and populations vulnerable to malign influence or receptive to building partner-nation capacity will enable commanders and policy makers to capitalize on gains, stabilize and resolve conflicts, and return to competition.

## Conclusion

The Army’s I2 capability has evolved beyond the counterterrorism and counterinsurgency OE to an “all-threats” enduring requirement relevant to MDO. I2 has been characterized as intelligence, surveillance, and reconnaissance for the “human domain.” I2 also contributes to intelligence preparation of the battlefield in relation to the “human domain.” As the Army further develops MDO, intelligence leaders should reflect on how I2 can be a force multiplier across multi-domain operations. LTG Wesley addressed the importance of getting “left of conflict” and the ability of actions in the competition phase to positively affect the

armed conflict phase or deter conflict. Intelligence leaders should explore how to incorporate I2 into the development and experimentation of MDO. Human aspects are present in each domain. Humans make decisions and make mistakes. Humans design, deploy, and operate weapons and war plans. Intelligence leaders should explore how I2 can present multiple dilemmas to the adversary in the competition phase. They should also explore how to incorporate I2 into the multi-domain task forces and how to use the Intelligence, Information, Cyber, Electronic Warfare, and Space detachments to support I2 operations. 

3. Ibid., C-2.
4. Office of the Chairman of the Joint Chiefs of Staff, Joint Publication 5-0, *Joint Planning* (Washington, DC: The Joint Staff, 16 June 2017), IV-10.
5. U.S. Army, "Gen. Raymond T. Odierno addressing the USMA class of 2013," *U.S. Army Worldwide News*, November 5, 2012, [https://www.army.mil/article/90671/gen\\_raymond\\_t\\_odierno\\_addressing\\_the\\_usma\\_class\\_of\\_2013](https://www.army.mil/article/90671/gen_raymond_t_odierno_addressing_the_usma_class_of_2013).
6. Department of the Army, TRADOC Pamphlet 525-3-1, *Multi-Domain Operations 2028*.
7. Jed Judson, "US Army capabilities integration chief talks multidomain ops," *Defense News*, October 8, 2018, <https://www.defensenews.com/digital-show-dailies/ausa/2018/10/08/us-army-capabilities-integration-chief-talks-multidomain-ops/>.
8. Scott King and Dennis Boykin, "Distinctly Different Doctrine: Why Multi-Domain Operations Isn't AirLand Battle 2.0," Association of the United States Army website, February 20, 2019, <https://www.ausa.org/articles/distinctly-different-doctrine-why-multi-domain-operations-isn%E2%80%99t-airland-battle-20>.
9. Department of the Army, Field Manual 3-0, *Operations* (Washington, DC: U.S. Government Publishing Office, 6 October 2017), 1-2. Change 1 was issued on 6 December 2017.

## Endnotes

1. Todd South, "This 3-star Army general explains what multi-domain operations mean for you," *Army Times*, August 11, 2019, <https://www.armytimes.com/news/your-army/2019/08/11/this-3-star-army-general-explains-what-multi-domain-operations-mean-for-you/>.
2. 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), 24.

*Mr. Peter Baber is a program manager for identity intelligence with the Department of Defense. He served on a joint duty assignment as the Chief of the Identity Intelligence Project Office in the Defense Combatting Terrorism Center and deployed in support of establishing Combined Joint Task Force—Operation Inherent Resolve's identity intelligence capability. He served as a branch chief for the U.S. Army Identity Intelligence Division, a plank owner who deployed with, and later led, the Counterinsurgency Targeting Program.*

*Ms. Pamela Baker is currently in the Identity Intelligence Division with the Department of Defense. She provides analysis and production oversight and lends strategic support to the intelligence community. She has 15 years' experience in the identity intelligence enterprise.*

*LTC Mark Dotson (retired) is currently the Defense Forensic Science Center Technical Representative for the U.S. Army. While assigned to the Army, he led a team of intelligence planners implementing a portfolio of programs that evolved into identity intelligence capabilities supporting warfighters and later served as current operations officer for the identity intelligence program. Additionally, he deployed operationalizing biometrics and forensics capabilities as nontraditional intelligence, surveillance, and reconnaissance enablers.*

## Intelligence Today for Tomorrow's Fight



*The National Ground Intelligence Center (NGIC) provides All Source and Geospatial Intelligence on foreign ground force capabilities and related military technologies and integrates with Mission Partners to ensure the U.S. Army, DoD, Joint, and National level decision makers maintain decision advantage to protect the United States and interests abroad.*