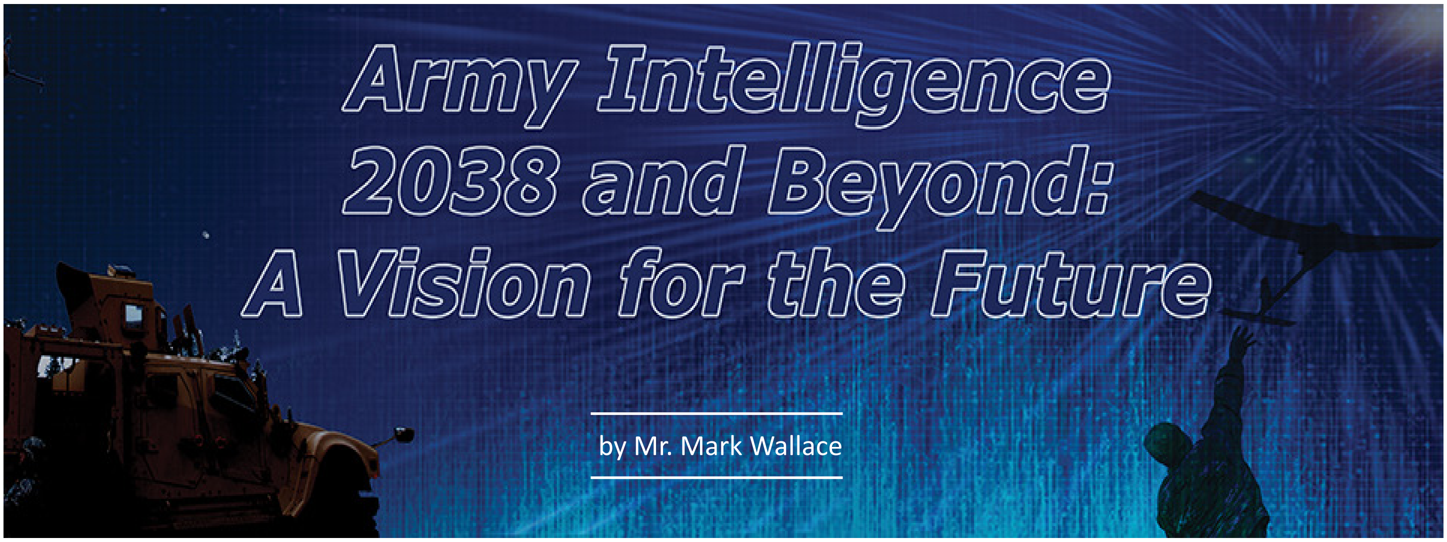


Army Intelligence 2038 and Beyond: A Vision for the Future

by Mr. Mark Wallace

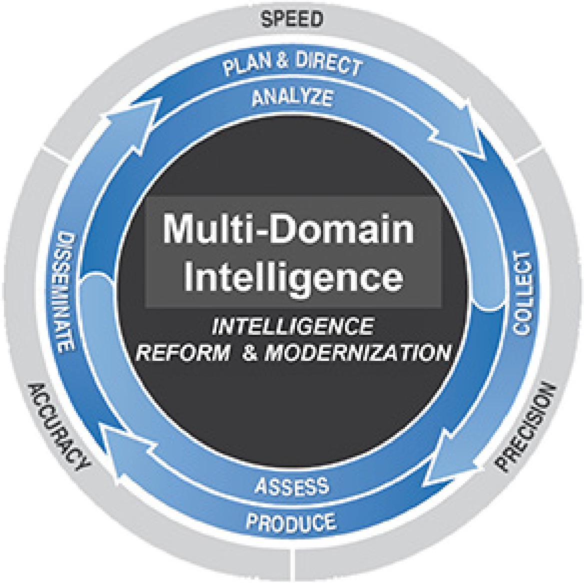
To ensure that the Army will be ready and can win in the future, we must also modernize…But to get to the Army we need in the future requires transformational change, not incremental improvements.

—GEN James C. McConville

This article assumes the successful implementation of the ideas in the Army's operating concept, TRADOC Pamphlet 525-3-1, *The U.S. Army in Multi-Domain Operations 2028,* and anticipates technologically advanced near-peer adversarial countermeasures to those actions.[1] It will imagine the future, provoke thought, and describe how Army intelligence could support warfare beyond 2038. This article describes the current multi-domain operations (MDO) gap and the solutions Army intelligence is pursuing to close the gap. It then focuses on MDO implementation and analyzes potential modernization measures to remain relevant in the face of an evolving threat. Lastly, it describes a potential vision for Army intelligence, providing ideas for the future based on concepts, an assessment of intelligence core competencies, and potential solutions informed through experimentation using research and development and science and technology.

MDO-Capable Army Intelligence, 2020–2028: Near-Term Strategy

The U.S. Army Combined Arms Center completed a 2018–2019 study of large-scale combat operations, which identified the lack of echelons above brigade multi-domain deep sensing; analysis; and processing, exploitation, and dissemination (PED) capabilities to support long-range precision fires as gap 1 of 17 critical gaps. The nature of the emerging threat coupled with emerging technologies capable of delivering lethal and nonlethal fires at much greater ranges drives the requirement for sensors that can see at much greater ranges without latency. Army intelligence force modernization must help to close this critical gap.



Multi-Domain Intelligence[2]

Current organizational changes were designed to ensure military intelligence (MI) forces have the capabilities and capacity required at echelon to support MDO during large-scale combat operations against a near-peer competitor. The multi-domain task force contains a multi-domain MI company to support priority intelligence requirements and targeting with advanced capabilities to identify, locate, and track threat antiaccess and area denial capabilities across all domains at extended ranges. The Army redesigned the MI brigade-theater to increase capacity, doubling the watch section and all-source analysis teams and creating a new open-source intelligence cell. The expeditionary-MI brigade will provide multi-domain deep sensing, analysis, and PED for each division and corps rather than optimize for brigade combat team reinforcement. The Army also restructured the Army National Guard and Army Reserve expeditionary-MI brigades to better support echelons division and above. Finally, the brigade combat team MI company adds an electronic warfare platoon, divides the multifunction teams into separate human intelligence and signals intelligence collection teams, and removes the company intelligence support teams: the counterinsurgency construct was not suitable for supporting large-scale combat operations.

Modernization priorities for Army intelligence materiel support MDO and long-range precision fires against a near-peer competitor through four major programs:

- **Tactical Intelligence Targeting Access Node (TITAN)** provides a scalable and expeditionary intelligence ground station that supports commanders. TITAN does this by leveraging space and high altitude, aerial, and terrestrial layer sensors to provide targeting data directly to fires information systems as well as multi-discipline intelligence support to targeting and situational understanding in support of command and control.
- **Multi-Domain Sensing System (MDSS)** will provide commanders with an agile, interoperable, and self-healing network of highly relevant and integrated sensors from low altitude to space. The MDSS will offer extended endurance over wide areas and denied airspace providing precision target location using multiple sensors in fluid environments.
- **Terrestrial Layer System** modernizes the terrestrial layer through a globally deployable intelligence, surveillance, and reconnaissance system containing signals intelligence, electronic warfare, and cyberspace operations capabilities.
- **Distributed Common Ground System-Army** will transition to applications on the command post computing environment after it upgrades capabilities from battalion through theater in the near term to improve data analytics.

MDO-Ready Army Intelligence, 2028–2035: Mid-Term Strategy

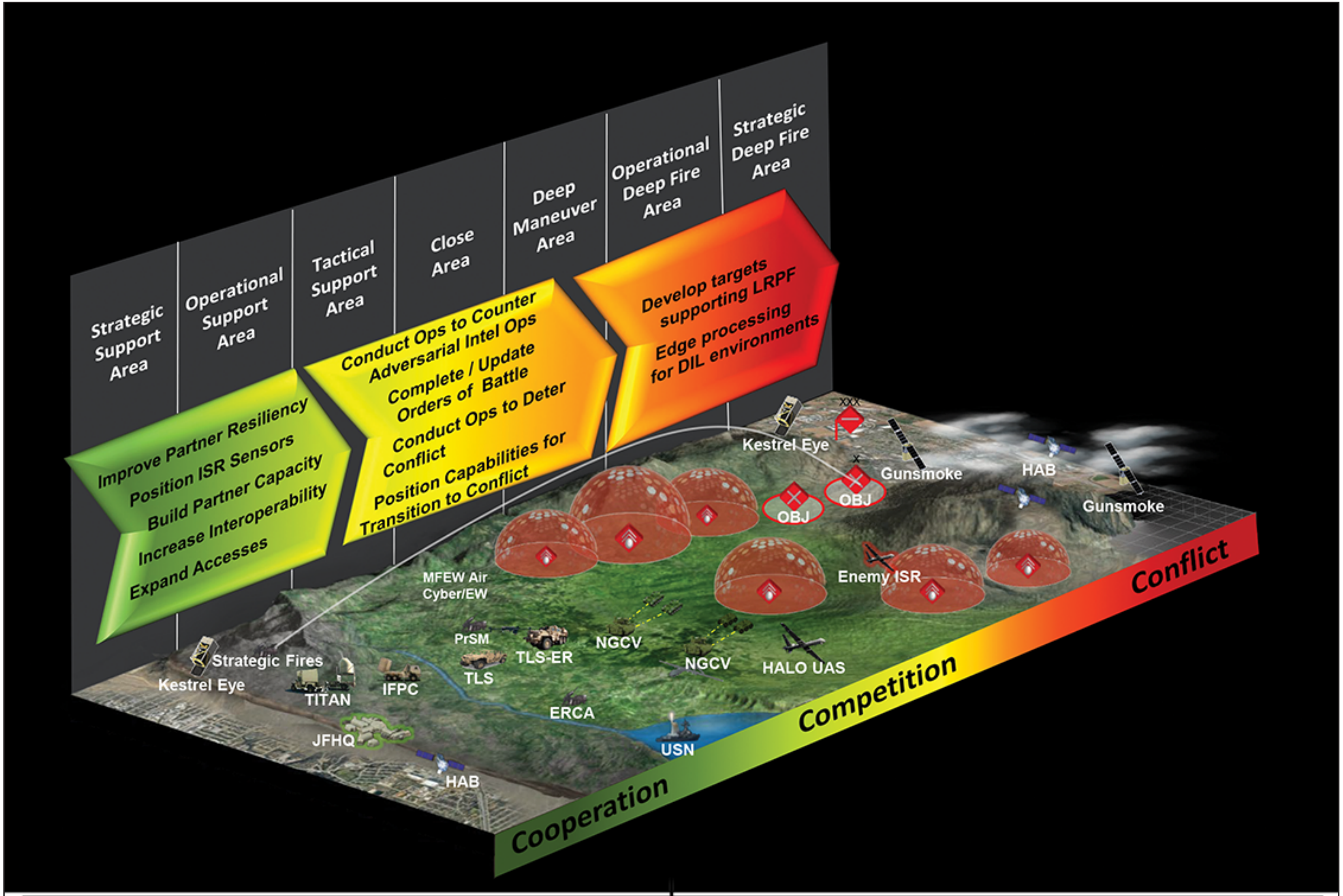
Operational environment assessments anticipate expanded effects of globalization in addition to competition with near-peer threats. It is a multipolar world, complicated with super-empowered individuals and non-state actors, hybrid capabilities, feral megacities with populations exceeding ten million, and hostilities below the threshold of war. Foreign adversaries conduct cyber espionage and technical operations against U.S. civil and military interests around the globe, and they continue to develop new and more effective capabilities in these areas. Readily available and advanced cyber and technical surveillance tools offer threat actors a relatively low-cost, efficient, deniable, and high-yield means of accomplishing their goals. The development of next-generation technologies, such as fifth-generation cellular communications technology, artificial intelligence, and quantum computing, present new opportunities for foreign entities to collect intelligence and conduct cyberspace operations against the United States and its allies.

Near-peer military threats will develop and proliferate capabilities to counter the U.S. MDO strategy and to contest sanctuary. They will field a myriad of capabilities and manpower: armed drone swarms, long-range missiles and rockets with advanced munitions, autonomous unmanned vehicles, soldiers powered by exoskeleton technologies, special forces commando teams (possibly posing as refugees from sleeper cells that activate to disrupt domestic harmony), increased air and land mobility, and electronic warfare capabilities to jam satellites and digital and voice communications. Near-peer competitors will be on the verge of militarizing artificial intelligence, machine learning, block-chain, cloud-independent edge computing, and quantum computing capabilities. Combined together and synchronized during large-scale combat operations, these modernized capabilities form a potent counter to the U.S. Army's MDO strategy.

The Army and Department of Defense (DoD) must adjust if they are going to retain the military advantage. Similarly, the U.S. Government cannot sit idly by while DoD does all the heavy lifting. The evolution of MDO involves a comprehensive whole-of-government, allies, and private-sector partner approach. Realizing that foreign governments are threatening key and vital national interests short of war, the U.S. Government must synchronize a whole-of-government approach. The Director of National Intelligence must expand critical infrastructure information exchanges with federal departments and agencies; state, local, tribal, and territorial governments; private-sector partners; and allies. New analytic tools will improve threat warning and enable offensive and defensive operations. The U.S. Government must enhance capabilities to share best practices with partners—in the areas of threat, incident, vulnerability, risk data, and security.

Army intelligence must still provide timely, accurate intelligence support to inform commanders' decision making, leaving intact Army intelligence's core competencies: intelligence operations (collection), intelligence analysis, intelligence PED, and intelligence synchronization. It is certain that the Army MI Branch will not own all the friendly sensors on the battlefield—it does not today. All collection, including cyberspace, will seamlessly integrate into the overall information collection process. Open-source intelligence and initiatives such as Every Receiver a Sensor and Artillery Delivered Intelligence, Surveillance, and Reconnaissance, using common data standards, will add to the "ocean of data" available to intelligence analysts. MI will continue to provide commanders with predictive intelligence based on modeling and simulation tools to get inside the enemy's decision cycle and make better friendly decisions. Analysis is an art and a science assisted by artificial intelligence and machine learning and driven by automation, robotics, and emergent technologies. PED, distributed and accessible, will evolve from a push construct to one of pulling. By 2028, Army intelligence will field automated tools to develop, integrate, and synchronize the collection plan, track sensor locations and status in real time, visualize available systems and gaps, and tip and cue appropriate sensors. Rapid technology advances will radically change *how* Army intelligence gets inside the enemy's decision-making cycle to provide friendly forces windows of superiority.

How the Army fights will change as the U.S. Government embraces a whole-of-government approach to synchronize capabilities across all domains, the electromagnetic spectrum, and the information environment. The lines between the Services and other branches of government will begin to blur as these organizations work closer together.



Space Layer
- National-to-tactical integrated platforms and sensors
- Small satellites and emerging/commercial technologies
- Army prioritization for targeting and collection

Aerial Layer
- Survivable, penetrating, high-altitude ISR
- Human-machine teaming
- Swarm and expendable ISR

Terrestrial Layer
- Human-AI teaming
- Integrated operations and intelligence
- User interfaces and experiences

Foundation Layer
- Degraded, intermittent, low-bandwidth data transfer
- Edge processing nodes and sensors

AI	artificial intelligence	IFPC	indirect fire protection capability	OBJ	objective
DIL	degraded, intermittent, low-bandwidth	Intel	intelligence	OPS	operations
ERCA	extended range cannon artillery	ISR	intelligence, surveillance, and reconnaissance	PrSM	precision strike missile
EW	electronic warfare	JFHQ	Joint Force Headquarters	TITAN	Tactical Intelligence Targeting Access Node
HAB	high-altitude balloon	LRPF	long-range precision fires	TLS	Terrestrial Layer System
HALO–UAS	high-altitude, long operation unmanned aircraft system	MFEW	multi-function electronic warfare	TLS–ER	Terrestrial Layer System-Extended Range
		NGCV	next-generation combat vehicle	USN	U.S. Navy

Operationalizing Multi-Domain Intelligence to Support Multi-Domain Operations

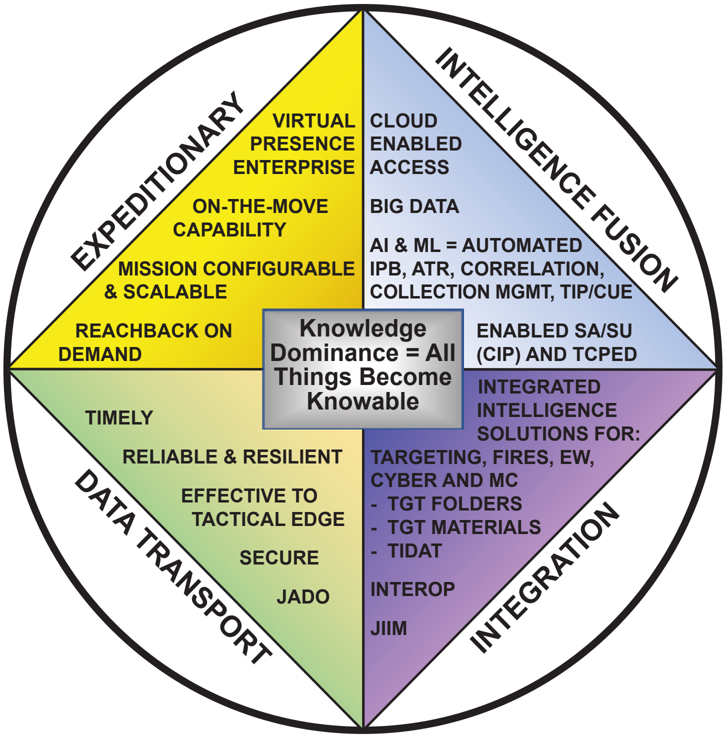
The ubiquitous nature of data, storage capacity, and accessibility will necessitate new rules and regulations governing who can access and share certain types of data and for what purposes. As doctrine evolves, Army intelligence will continue to tailor support to every echelon based on the supported unit's tasks and missions.

Army intelligence will develop materiel solutions that are scalable and tailorable to each echelon. A modular open system architecture will allow rapid technology insertion, especially in sensor design and fielding. Joint common data standards will normalize data and facilitate seamless integrated data sharing between sensors, shooters, and command and control nodes. Miniaturization will enable onboard sensor preprocessing and secure transmission. Artificial intelligence will speed analysis and support the military decision-making process, intelligence preparation of the battlefield, and collection management. Machine learning and natural language processing will enhance predictive analysis, deep data analytics, data sharing, and automated solution development. National functional managers such as the National Security Agency or National Geospatial-Intelligence Agency will have an increased role to improve the materiel development process, creating a next generation of sensors across all observable spectrums and in cyberspace.

Talent management must keep pace with innovation. Through early and often assessment of technical and leadership skills, the Army can implement several initiatives. Separate leadership and technical tracks will align the appropriate Soldier with assigned duties. Training will support new career fields such as data scientists, decision analysts, data managers, and ethical hackers. While initial entry Soldiers will still attend basic and advanced individual training in their respective branch training centers, virtual and online classrooms will provide professional military education after initial assignments. A step-increase program will help recruit and retain highly skilled and trained Soldiers, while regimental assignments will ensure regional continuity and develop cultural expertise. All-source analysts should transition to "decision analysts," mechanical translators will assist linguists, and contractors will add technical know-how. The Army should create a career field for cyberspace counterintelligence to enhance technical security, assess friendly vulnerabilities, defend against hybrid attack methods, and detect insider threats. Human-machine interface and virtual reality will enhance human performance but may bring with them unforeseen mental and physical issues.

Beyond MDO-Ready Army Intelligence, 2038 and Beyond: Far-Term Strategy

The operational environment of 2038 will be significantly different from the early 2030s as adversaries aggressively challenge U.S. overmatch. Nation states will likely form new alliances for survival, super-empowered individuals will threaten stability and international norms, and lines between government and business will become blurred. The threat is not constrained; it lives in a digital world without boundaries. The U.S. Government needs to be mentally and technically prepared to address these threats. Large-scale combat operations against a near-peer competitor remains the worst case scenario for the U.S. military, and nuclear proliferation is still a menace. Highly advanced adversaries will continue to develop methods to transcend U.S. strengths in traditional fire and maneuver capabilities across


EXPEDITIONARY
VIRTUAL PRESENCE ENTERPRISE
ON-THE-MOVE CAPABILITY
MISSION CONFIGURABLE & SCALABLE
REACHBACK ON DEMAND
INTELLIGENCE FUSION
CLOUD ENABLED ACCESS
BIG DATA
AI & ML = AUTOMATED IPB, ATR, CORRELATION, COLLECTION MGMT, TIP/CUE
ENABLED SA/SU (CIP) AND TCPED
Knowledge Dominance = All Things Become Knowable
DATA TRANSPORT
TIMELY
RELIABLE & RESILIENT
EFFECTIVE TO TACTICAL EDGE
SECURE
JADO
INTEGRATION
INTEGRATED INTELLIGENCE SOLUTIONS FOR:
TARGETING, FIRES, EW, CYBER AND MC
- TGT FOLDERS
- TGT MATERIALS
- TIDAT
INTEROP
JIIM

AI	artificial intelligence	MC	mission command
ATR	automatic target recognition	MGMT	management
CIP	common intelligence picture	ML	machine learning
EW	electronic warfare	SA/SU	situational awareness/situational understanding
INTEROP	interoperability	TCPED	tasking, collection, processing, exploitation, and dissemination
IPB	intelligence preparation of the battlefield		
JADO	joint all-domain operations	TGT	target
JIIM	joint, interagency, intergovernmental, and multinational	TIDAT	target intelligence data

Knowledge Dominance

domains while disrupting access to space, the electromagnetic spectrum, and most significantly the cyberspace domain, all across a vastly extended area of operations. Adversaries will also use multi-domain economic and information warfare throughout the operational continuum to gain advantage, achieve decisive effects, shape domestic and international sentiment, and influence decision makers.

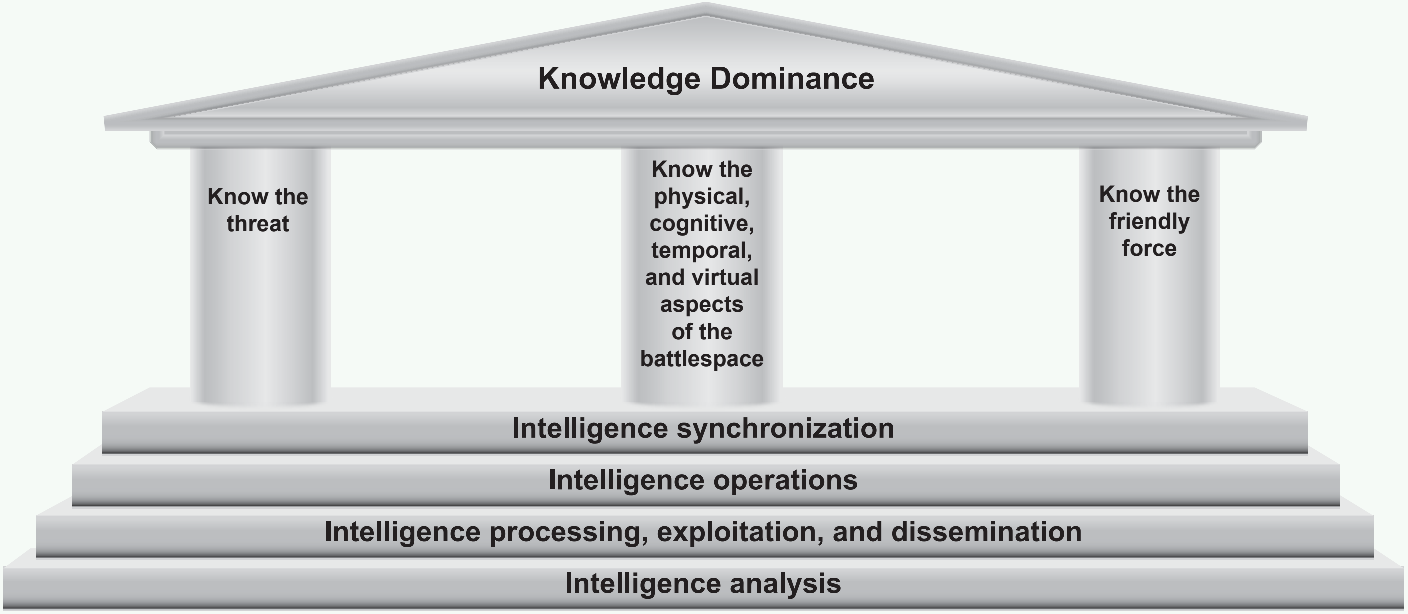
In response, DoD agencies, military services, academia, and the industrial complex must cooperate at an unprecedented level on research and development and science and technology innovation: militarization of new technology must occur faster than ever before. Today's acquisition process will be obsolete to support the demands of increased lethality of weapon systems, sensor proliferation and accuracy, processing speed, ubiquity of data, miniaturization, and other advances. Army intelligence is a high-tech consumer and is not immune to this trend. While efforts made in the 2020-to-2028 timeframe made great strides in closing the deep sensing and data processing gap, the Army must continue to look for ways to achieve overmatch against the threat. Army Futures Command must continue to experiment with concepts designed to address the future operational environment, leverage advanced technology, and inform force structure and materiel development.

How the Army fights beyond 2038 will evolve in every domain and the electromagnetic spectrum and will include economic, knowledge, and temporal considerations while the diplomatic aspect will remain outside of DoD's purview for integration. Information in all its forms becomes a commodity for producing knowledge. The future of the intelligence warfighting function becomes knowledge dominance.

Information operations for an effect remains a separate function from the collection and processing of information to generate knowledge. Knowledge dominance takes situational awareness to the next level as all things potentially become knowable. Priority intelligence requirements are coordinated with stakeholders the same as they were in the past. Knowledge dominance becomes a core competency of Army intelligence. Knowledge dominance is achievable through transforming intelligence organizations and

Alternative Analysis

This article's author and contributors artificially constrained themselves to what Army MI can control. Upon further examination and deliberation with senior leaders, there is likely a more effective way to implement knowledge dominance (KD) in the future. During open dialogue about the potentially revolutionary effects of technology insertion resulting in KD, it became evident that KD has broader implications across the Army and that there are ramifications for stakeholders well beyond MI. KD is potentially much more than simply a core competency for MI. ADP 6-0, *Mission Command: Command and Control of Army Forces,* says, "Knowledge management is supported by four tasks that bring an organization closer to situational and shared understanding. The four knowledge management tasks are creating knowledge, organizing knowledge, applying knowledge, and transferring knowledge."[3] The suggested alternative solution for the Army is to replace the Army Universal Task "Conduct Knowledge Management and Information Management" with "Conduct Knowledge Dominance." By using technology to expand the scope of knowledge and information management, KD could become the qualitative and quantitative mechanism by which the Army provides support to situational understanding for our commanders. We hope this article and alternative analysis will spark the imagination of capability developers across the Army and generate intellectual dialogue that will drive innovation.


Knowledge Dominance
Know the threat
Know the physical, cognitive, temporal, and virtual aspects of the battlespace
Know the friendly force
Intelligence synchronization
Intelligence operations
Intelligence processing, exploitation, and dissemination
Intelligence analysis

structure with Global Information Grid server farms, high-tech data scientists, and skilled ethical hackers working in a federated and distributed enterprise approach, centralized at echelons corps and above and tailored to meet command and control requirements. These high-cost, high-demand, low-density capabilities will downward reinforce division and brigade formations. Army intelligence organizations at divisions and brigades become smaller and are more capable because of technological enhancements. The ability to collect all available information and potentially "know all things" could create the opportunity to use data for illicit purposes, requiring a revision of intelligence oversight regulations. Policy changes may also address additional ethical considerations, including neural implants that enable direct human interaction with machines, and thoughts with other humans, and implications of autonomous machine warfare. In this era, time and knowledge become the critical factors because information and data are widely and openly available. A commander's ability to make the right decision faster than his opponent is the key to success.

U.S. Army photo illustration

The Army's modernization approach requires updating its doctrine, organizational designs, and training to conduct operations as a multi-domain force.

Technology will leap ahead by 2038. Artificial intelligence, machine learning, and quantum computing will greatly accelerate capabilities for research and development and science and technology. DoD and Army acquisition processes will become more streamlined as industry becomes more closely aligned with DoD. A genuine modular open system architecture design will allow rapid technology insertion. Supported by these technologies, the global sensor grid will render range less relevant and crypto less secure. No information will be "off limits," and PED becomes nearly instantaneous. Next-generation technologies will augment analysis and predict indicators of adversarial intent. The tactical cloud will become a virtual Global Information Grid fed by, and accessible from, anywhere in the world using self-healing networks. Nanotechnology will help scale and tailor capabilities to each echelon. Every piece of equipment and every Soldier has an organic, automated, multimodal sensor pod linked to the Global Information Grid and managed by artificial intelligence. Biotechnology, neural implants, and personal avatars improve Soldier capabilities and capacities. Augmented and virtual combined environments with four-dimensional displays enhance visualization. Together these capabilities have the potential to revolutionize commanders' situational understanding by creating an environment where it is possible to collect and know everything.

Soldiers continue to provide the advantage over near-peer adversaries. Future intelligence Soldiers are curious, mentally agile, ethical, adaptive, passionate, and predictive. Well trained and continuously educated, they understand culture, technology, and context and can calmly communicate their contributions to both human and machine. Previous initiatives such as regimental assignments, area specialists, separate leadership and technical tracks, a step-increase program, and linguist management will become routine talent management practices. New training in economics and temporal analysis will supplement increased technical training, all in a virtual environment. Augmented reality, virtual avatar personal assistant, and biotechnology provide opportunities for analysts to collaborate and learn. Infrastructure will reduce as a combination of remote workers/locations, virtual training and interaction, distributed offices, and robotic capabilities. Leaders will adapt to these changes and the increased operational tempo. Contractor experts will augment uniformed personnel at corps and echelon above corps levels.

Conclusion

If technology trends continue to change at an exponential rate, the U.S. military can ill afford complacent thinking about the future. Army intelligence modernization must not overlook less conspicuous low-tech threats from third-world adversaries. Optimizing to fight future threats requires an adaptive intelligence force capable of supporting competition short of war and maneuver and fires during large-scale combat operations, in all domains with increased speed, accuracy, and lethality throughout the depth of the extended battlefield. As the Army continues adapting to the current and future operational environment, developing a capable intelligence force that exceeds the challenging demands of commanders' expectations is critical. Highly capable Army intelligence organizations are essential to success now and in the future. The Army must not only continue its pursuit of materiel solutions to support MDO and beyond, but it must also recruit and retain highly skilled Soldiers. It must also build the right force structure to collect, process, and disseminate relevant, timely, predictive intelligence in all domains from theater to tactical levels in support of the joint force.

Epigraph

GEN James C. McConville, "2020 Posture Statement House Armed Services Committee," U.S. Army Worldwide News, March 3, 2020, https://www.army.mil/article/233474/2020_posture_statement_house_armed_services_committee.

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).

[2] Figure is adapted from Figure 3-1. The intelligence process, Department of the Army, Army Doctrine Publication (ADP) 2-0, *Intelligence* (Washington, DC: Government Publishing Office [GPO], 31 July 2019), 3-2.

[3] Department of the Army, ADP 6-0, *Mission Command: Command and Control of Army Forces* (Washington, DC: U.S. GPO, 31 July 2019), 3-8.

Mr. Mark Wallace retired from active U.S. Army service in 2009 as a colonel in the Military Intelligence Corps. Currently, he works as a defense contractor in the Intelligence-Capabilities Development and Integration Directorate (I–CDID), Concepts Division at Fort Huachuca, AZ.

Contributors:

Ms. Mary Ellen D'Amico, a retired U.S. Army military intelligence noncommissioned officer, is the Concepts Team Chief for the I–CDID, Concepts Division.

Mr. James Harper retired from the U.S. Army after 30 years in military intelligence. He is currently a defense contractor writing intelligence concepts in the I–CDID, Concepts Division.

Doctrinal Proficiency and Doctrinal Assistance

PANIC ...... 34 publications and over 5,500 pages of doctrine spread across multiple domains and I just want to know the responsibilities of an OMT. What do I do?

- Answer -

Email usarmy.huachuca.icoe.mbx.doctrine@mail.mil for friendly doctrinal assistance. We will not read it for you, but we can point you in the right direction. We will provide you an answer as quickly as possible, but please allow at least two business days.

Want to be in the doctrinal know?

USAICoE doctrine maintains an email notification list to announce —

- Publication of new issues of MIPB.
- Publication of new U.S. Army intelligence doctrine.
- Notification of draft U.S. Army intelligence doctrine staffings.

If you wish to receive these notifications, send a message to the email address listed above and you will be added to the list.