Multidomain Observing and Orienting

ISR to Meet the Emerging Battlespace

Maj Sean A. Atkins, USAF

Disclaimer: The views and opinions expressed or implied in the Journal are those of the authors and should not be construed as carrying the official sanction of the Department of Defense, Air Force, Air Education and Training Command, Air University, or other agencies or departments of the US government. This article may be reproduced in whole or in part without permission. If it is reproduced, the Air and Space Power Journal requests a courtesy line.

The complexity and speed of future multidomain operations (MDO) hold deep implications for how military forces conduct John R. Boyd's famous observe, orient, decide, and act (OODA) loop. Increased domain interconnectivity and growing cross-domain interdependence underpin an emerging vision of future warfare that is beginning to take shape. Publications that include the DOD's Joint Operational Access Concept family of documents and the Army's multidomain battle operating concept describe the contextual drivers and outline the idea's central elements.[1] At its core, the MDO concept is a response to a changing competition-space characterized by complex problems that defy current approaches and anti-access/area-denial (A2/AD) challenges that require more fluidly integrated capabilities across all domains to overcome.[2] As Dr. Jeff Reilly, the Air Command and Staff College director of Future Warfare Studies, warns: "historical approaches to achieving superiority in the air, land, and sea domains may no longer be valid."[3] To address this, the nascent multidomain idea aims to make an expansion of jointness within and across domains.[4] To better understand what this means for how militaries observe and orient (OO), this article first explores the context, defining a domain, a continuum of domains, and their relevant features. Second, given this context, it aims to outline future OO requirements and determine the likely implications for the intelligence, surveillance, and reconnaissance (ISR) enterprise.

Defining an Operational Domain

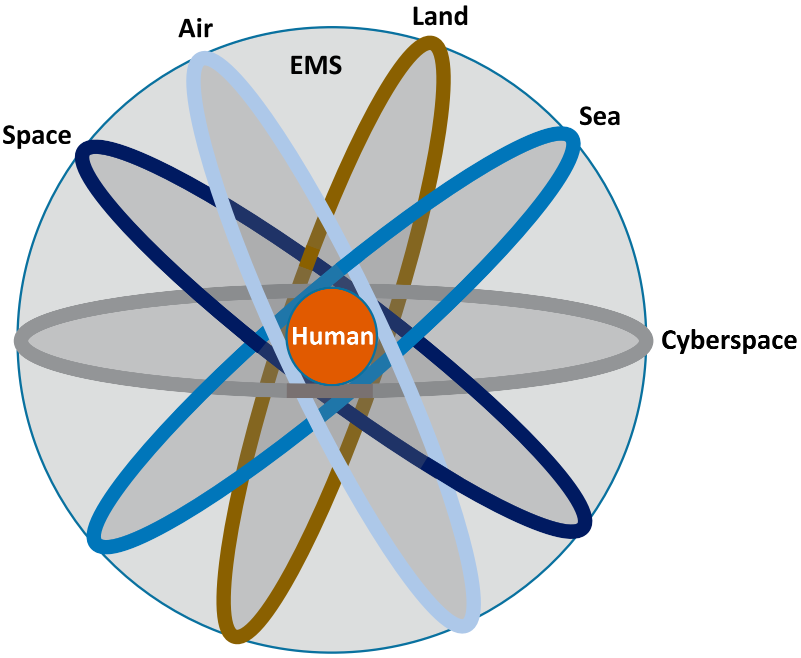
Defining and designating operational domains remains a much-debated topic within the defense community. Since the addition of cyberspace in 2011, the DOD officially recognizes five operational domains: land, air, sea, space, and cyberspace.[5] Still more are under consideration, including the electromagnetic spectrum and the human or cognitive domain.[6] The doctrinal debate on what does or does not make the cut as an operational domain is beyond the purpose of this article. It is, however, important to progress with a common conception, and since this article is concerned with examining the practical implications of MDO, a more flexible definition will serve to enable a fuller conversation on its application. In this article, a domain is simply defined as a characteristically distinct maneuver-space within or through which advantage can be achieved over an adversary.

Operations within a Continuum of Domains

Technological developments have long driven evolutions in the way wars are fought.[7] One of the more profound impacts of these developments is found in the way in which they connect domains. By enabling a projection of power and influence beyond where armies could previously travel, early sea power capabilities provided new ways to gain an advantage on land. Similarly, with the advent of airpower came new ways to connect, maneuver, and gain an advantage over both land and sea forces. More recent advances, particularly but not exclusively in information technology, have created new maneuver spaces, as well as new ways to connect other operational domains, further altering how we perceive domain interdependence.[8] Central to these changes is the emergence of cyberspace and space as increasingly important and contested domains.[9] As recently described in the *Air & Space Power Journal*, "advances in technology have subtly nudged the entire globe into a realm where all previous notions of the battlespace have been radically altered by domain interdependence."[10]

Increasing domain connectivity and interdependence are pushing the battlespace toward a more fluid continuum of domains. Within this context of increasing cross-domain opportunity, the MDO concept involves the exploitation of asymmetric advantage across multiple domains to achieve the freedom of action and effects required for mission success.[11] It is more than simply conducting operations in multiple domains—it is about synchronized maneuver between domains to create asymmetric effects at speeds that ultimately complicate and outpace adversaries'

OODA processes. The core thesis is the complementary, vice merely additive, use of capabilities across domains to create moments of superiority that can be leveraged to achieve mission objectives.[12] Future war fighters will need to be able to gain superiority at the right time, place, and combination of domains to succeed.



Continuum of domains

Not New in Concept but New in Character

Although the idea of conducting operations across domains is as old as antiquity, today's MDO concept has increasing relevance and distinctive features. One of the first recorded examples of an MDO occurred in 1187 BC when a coalition of tribes collectively known as the Sea Peoples threatened Ramses III's Egypt with superior naval forces.[13] Instead of conducting a traditional naval battle as his predecessors had done, Ramses III secretly maneuvered his land-based archers to the Nile shoreline while presenting a weak naval element to draw the enemy within bow range. As his archers began annihilating the Sea People's fleet, the bulk of Ramses' naval forces blocked their retreat, permanently eliminating this threat.[14] Airpower, 3,100 years later, further advanced the concept of MDO, altering the character of war with its ability to conduct a quick strategic attack from afar, as well as meaningfully influence operations on the land and sea domains.

So, if the multidomain idea is a long-standing part of the evolving character of war, what is new about the current MDO concept that requires attention? Beyond the recognition of technological advances and A2/AD challenges, which have been well covered elsewhere, there are distinctive characteristics these produce that demand a more sophisticated MDO approach. Exploring these salient emerging features that define the new MDO provides the foundation necessary to begin to understand how to approach effective multidomain OO.

Focus on Cross-Domain Synergy and Maneuver

At the heart of new multidomain thinking is the idea of cross-domain synergy based on deeper interdomain connectivity. Cross-domain synergy is the synchronization of individual domain activities to establish superiority in or through a combination of domains to achieve mission success.[15] Commanders, staffs, and operators should be able to think beyond their organization's home domain, equipping and training forces to conduct cross-domain maneuver, pivoting between domains for access and advantage. Just as the *Joint Concept for Entry Operations* (*JCEO*) highlights, "maneuver capabilities in multiple domains present many potential threats to the adversary, overloading his decision cycle and allowing the joint force to seize and retain the initiative."[16]

Windows of Superiority or Access

Recognizing increasing A2/AD challenges, today's MDO concept is focused on establishing windows of localized superiority, often opportunistically derived and fleeting in duration. The aim is to penetrate enemy defenses with defined areas of domain superiority where joint and partner forces can achieve operational objectives and prevent adversaries from disrupting friendly operations.[17] As the director of the Army Capabilities Integration Center highlights, the military needs to be able to "create and exploit temporary points of advantage."[18]

This concept differs significantly from traditional concepts of domain superiority that focus on gaining and maintaining superiority over broad swaths of battlespace for longer periods of time. Just as the Air-Sea Battle team noted, this shift in thinking "acknowledges that a joint or combined force may not be able to achieve either theater-wide domain superiority or an enduring and constant superiority, but that it can achieve operational objectives with control that is limited in time or space."[19] Success in future operations will likely reside in a force's ability to create precision access in one or multiple domains to enable effects and achievement of objectives in others.[20]

Increased Emphasis on Speed

The fleeting and often opportunistic nature of this new environment places increased emphasis on the speed of MDO. The Chief of Staff of the Air Force underscored this point at a recent panel on multidomain battle, stating that speed and multidomain maneuver at a pace the enemy cannot keep up with "is a defining concept for multi-domain operations."[21] Success will likely be found by the force with the ability to create and act on fleeting opportunities the quickest, making the OODA competition between opposing forces even more intense.

Emphasis on Lower-Echelon OODA

The likelihood of disrupted communications in a contested battlespace combined with the focus on creating opportunistic advantage increases emphasis on the OODA cycle at lower echelons of action. MDO expertise, authority, and capability must exist at the component-level and below to enable cross-domain actions that support commanders' intent and schemes of maneuver.[22] Jeffrey Reilly again highlights that, "the requirement to think across domains is occurring at increasingly lower levels and will be essential in the future to generating the tempo critical to exploiting fleeting local opportunities for disrupting an enemy system."[23]

More Possibilities in More Domains Means Increased Complexity

The emerging battlespace has three key characteristics that create a far more complex operating environment. First, the addition of cyberspace as a new human-constructed and changeable domain offers new possibilities to impact operations within cyberspace as well as in all other cyber-connected domains. Second, advances in technology have created new possibilities for maneuver and action in space as well as throughout the electromagnetic spectrum. Finally, advances in technology are also increasing physical and virtual connection within and between traditional maneuver domains, creating more cross-domain options. Combined, these three characteristics lead to an increasingly complex battlespace with exponentially more combinations of opportunities and risks for war fighters to identify and consider.

Observing and Orienting for MDO

If the multidomain context is, as described above, characterized by increased complexity and speed then, to out-maneuver adversaries, there will be far greater emphasis on warfighters' ability to first out-observe and out-orient them. Further, this calls for a corresponding change in the *way* war fighters observe and orient themselves to the battlespace. As William Dries, an Air Staff strategist working on MDO, notes, "the ability to understand an enemy's activities. . . in multiple domains with speed and agility is the key to all of this."[24] The following sections outline the enduring foundations of observing and orienting, as well as the new requirements and implications placed on both to create an advantage in a fast and complex context.

Foundations of Observing and Orienting

Observation is the ability to perceive things and activities that have potential significance. According to Boyd, observation is fed and influenced by unfolding circumstances, outside information, interaction with the environment, and iterative interaction with the orient-decide-act components of the OODA Loop.[25] Observation, in turn, feeds the war fighter the information necessary to orient: the interactive process of cross-referencing projections, empathies, correlations, and rejections that is shaped by and shapes the understanding of the battlespace.[26] Orienting is, as

Boyd describes, the most important part of the OODA Loop, the Schwerpunkt that "shapes the way we interact with the environment," as well as "the way we observe, the way we decide, and the way we act."[27] Without it, "there is no command and control worthy of the name."[28]

Enduring ISR principles further build this foundation. While many experts and organizations have developed exhaustive lists of important principles that apply to ISR, a set of core and enduring principles can be distilled for utility in the MDO discussion. Primary among these are:

1. Perspective—the ability to see and understand the competition and battlespace from others' perspectives, including partners, nonplayers, and the adversary,
2. Objectivity—recognizing and counteracting biases to remain intellectually transparent and honest,
3. Integration—information where and when it is needed,
4. Context—aggressive collection and sourcing of information to provide multiple vantage points, enabling the analysis and cross-referencing required to increase breadth and depth of understanding.[29]

In turning this toward practical application, the Core ISR Tenets described in *ISR 2023* provide an additional useful piece of this foundation.

1. ISR is indivisible—effects depend on ISR synchronization and integration.
2. ISR is domain-neutral—focused on capabilities and effects, not platforms.
3. ISR is operations—not solely support to operations.[30]

Requirements for Multidomain Observing and Orienting

Examining the emerging multidomain context through the lens of the foundation provided above, requirements for future observe and orient activities start to become discernible. Aggressively sourced information that provides perspective and objectivity, integrated at the right time and place must now flex to: feed opportunistic cross-domain maneuver via pockets of domain superiority created and exploited at all echelons, at speeds that outpace adversaries' ability to build awareness and respond. To meet these demands, ISR forces must be able to identify cross-domain opportunities and vulnerabilities, leverage increasingly vast amounts of data to provide clarity in complexity, and provide broader awareness to a more diverse set of actors.

Identify Cross-Domain Opportunities and Vulnerabilities

To feed multidomain maneuver, ISR must be able to identify cross-domain opportunities and vulnerabilities, recognizing and correlating capabilities, connections, and patterns in a more complex and interconnected operational environment. This means observing the battlespace in greater depth and breadth to have enough puzzle pieces to configure and reconfigure to create opportunity or discover vulnerability. If, as the JCEO describes, future forces will need to "employ opportunistic, unpredictable maneuver, in and across multiple domains," then their OO functions must be able to identify these fleeting cross-domain gaps and opportunities faster than the adversary can discover and close them.[31]

Sense-making in Complexity and Among Voluminous Data

Observing and orienting for success in MDO will require the ability to make sense of a more complex battlespace with vastly growing volume and variety of data. This places an even greater emphasis on orienting in particular and the ability to fully translate increasingly vast data into insight relevant to commanders' vision, intent, and objectives. The JOAC's call for the joint force to be able to "collect, fuse, and share accurate, timely, and detailed intelligence across all domains," barely scratches the surface on the depth of what this requirement really means.[32] It is a demand for a far more sophisticated ability to, as Boyd described, analyze and synthesize "across a variety of domains" to "evolve new repertoires to deal with unfamiliar phenomena or unforeseen change."[33] This means that to create the "mental. . . patterns that match with activity of the world" in this new multidomain context, OO functions must be able to make sense of increased complexity and data volume.[34]

Broaden Awareness at All Decision Levels

To create cross-domain synergy at increased speed and at lower echelons, broader awareness of activities, risks, and opportunities in and between domains becomes a necessity from the joint force commander (JFC) down through components and tactical forces. To maneuver in multiple domains, war fighters must be more fully aware of the interconnected domain space their forces operate in and the opportunities that present themselves or can be created. This awareness needs to be available at the same speeds and fidelity as higher echelons to afford forces the ability to disperse to avoid A2/AD threats and then re-concentrate rapidly to exploit opportunity.[35] With this sort of breadth and depth of access to facilitate multidomain OO, actors at all levels will be able to, as Boyd describes, "exploit lower-level initiative yet realize higher-level intent."[36]

Implications for the ISR Enterprise

The evolving battlespace demands and OO requirements outlined above build toward an inflection point for the ISR enterprise. New multidomain challenges and opportunities are beginning to present themselves, but existing ISR tools, organizations, and concepts are not postured to engage them. The positive news is that new and developing ideas within industry and the ISR community provide a useful foundation to build from. Many of these ideas and tools emerging in pockets of innovation can be refocused and tied together to begin to meet the MDO challenge. Just as early aircraft changed how military forces observed their battlespace, providing awareness far beyond the perspectives of ground and naval forces, these new concepts and capabilities are putting an ISR paradigm shift in sight, one that can provide a more holistic understanding of the complex multidomain battlespace.[37] It is a paradigm shift with, as the Air Force lead for intelligence analysis highlighted, broad implications for "what we collect, how we process it, how we analyze it, and how we connect to the operators, platforms and staffs that need that information."[38]

Rethink the Battlespace

First, it is essential to rethink the battlespace itself, re-conceptualizing it as a layered and interconnected multidomain maneuver-space. This interconnected continuum of domains contains innumerable new maneuver options that are not sufficiently captured through traditional, often stovepipe OO constructs. Within modern military operations exists a tight interdependence between individual domain functions. Being able to discern and visualize the layers, interconnection points, and dependencies will provide the sort of battlespace understanding that enables multidomain action.

Rethink Actors and Activities

To achieve success in a multidomain competition, ISR professionals must also rethink their conception of activities and actors within the battlespace. Instead of focusing on one dimensional targets with narrow activity sets, ISR must hunt targets as multidomain systems with exploitable interconnected surface area. Further, it must have a broad baseline understanding of the multidomain environment to detect anomalies and be able to observe and orient off the series of interconnected activities that relate to a particular behavior or actor. Most current ISR constructs stovepipe their questions and focus, narrowing collection and analysis, resulting in missed opportunities and vulnerabilities.[39]

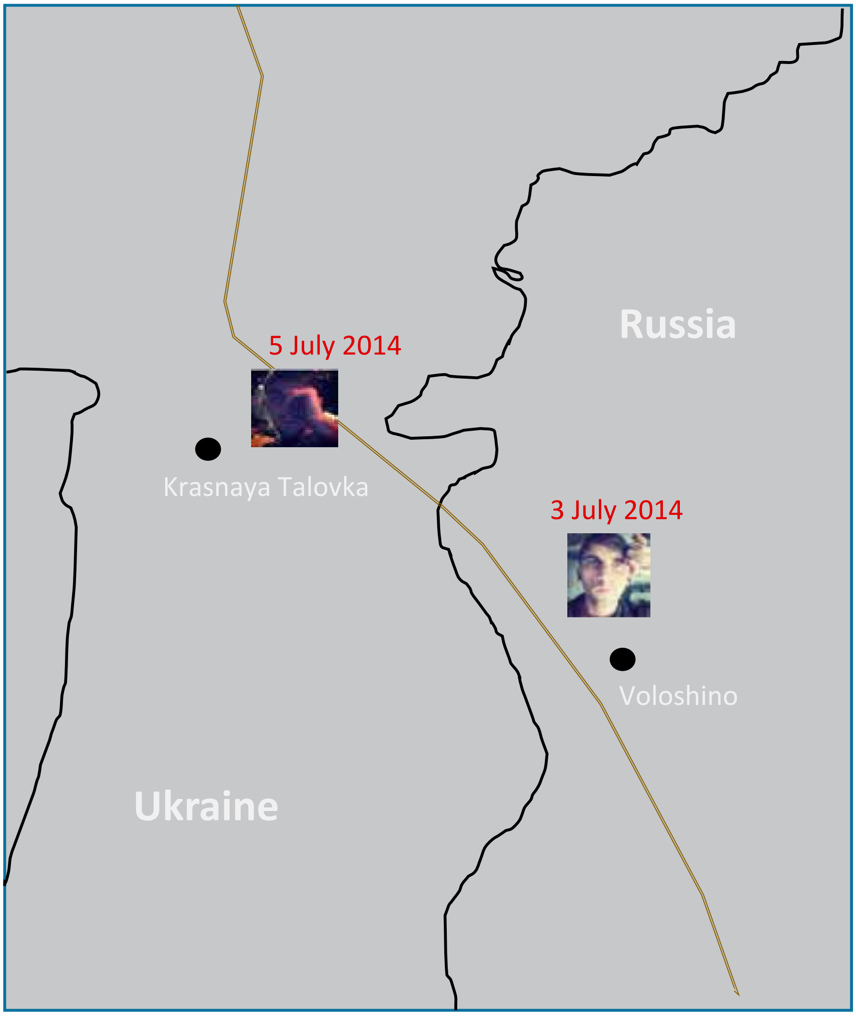
Recent developments in ISR methods and technology provide the practical foundation to realize this necessary perspective shift. The advancement of object-based intelligence (OBI) and activity-based intelligence (ABI) concepts, in which intelligence work is organized around the person, place, or thing being studied along with its associated activities vice any particular organization or collection system, enables the more holistic OO that MDO requires.[40] Instead of interpreting a snapshot image to discern a narrow amount of information, an MDO ABI approach would focus on understanding what is happening with the person, place, or thing studied and how that activity and its interconnected elements and environment change over time.[41] The ISR paradigm shifts from simply identifying enemy capabilities and estimating motivations, to assessing a changing battlespace and its impact on operations.[42]

Change How We Observe the Battlespace

Decisions that drive MDO demand new information and awareness that necessitate a corresponding change in how we observe the battlespace. In order to quickly identify and leverage opportunity for cross-domain maneuver and effects, future

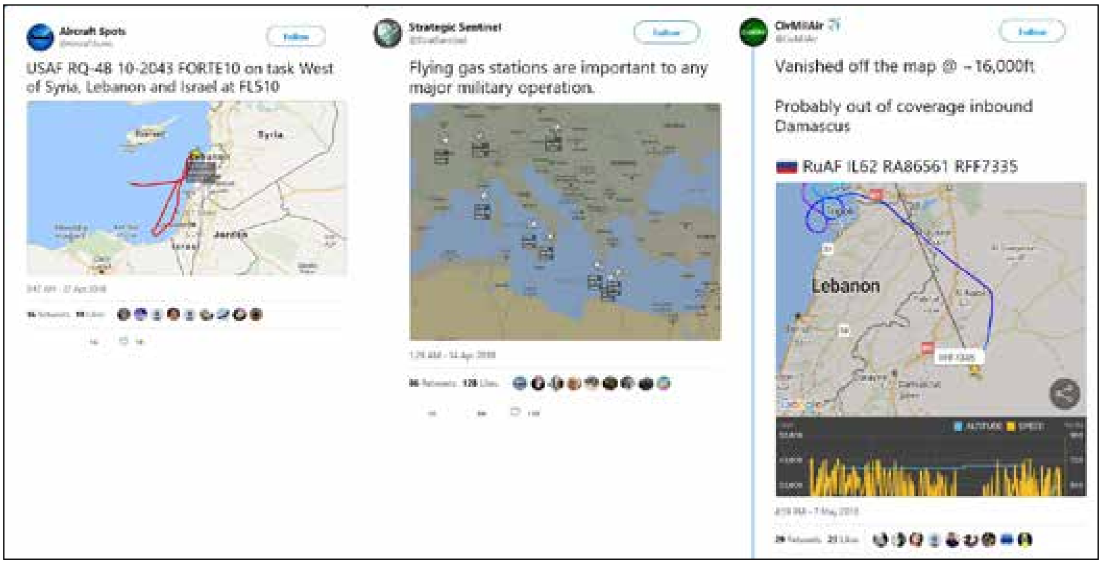
ISR operations should involve collecting broader information across all domains. More specifically, MDO requires greater data volume, variety, and velocity derived from more sources.

Increased interconnectivity between domains means actors and activities in one domain are more likely to appear with exploitable surface area in others. For example, during the 2014 Russian seizure of Crimea, the lack of traditional telltale signs of invasion surprised intelligence analysts.[43] While Russian soldiers obfuscated their traditional visual and EMS signatures, where ISR was postured to look, they interestingly began showing up prominently in cyberspace on social media sites including Twitter, Instagram, and the Russian version of Facebook.



Russian soldier Alexander Sotkin's Instagram posts revealing clandestine movement into Ukraine

Of course, this kind of exposure is not limited to Russians in Crimea. Private citizens are publishing volumes of information revealing military activities, from spy ship tracking to missile launch details.[44]



Aircraft Spots

USAF RQ-4B 10-2043 FORTE10 on task West of Syria, Lebanon and Israel at FL510

Strategic Sentinel

Flying gas stations are important to any major military operation.

CivMilAir

Vanished off the map @ ~16,000ft

Probably out of coverage inbound Damascus

RuAF IL62 RA86561 RFF7335

Twitter feeds publishing locational data on military assets and activities

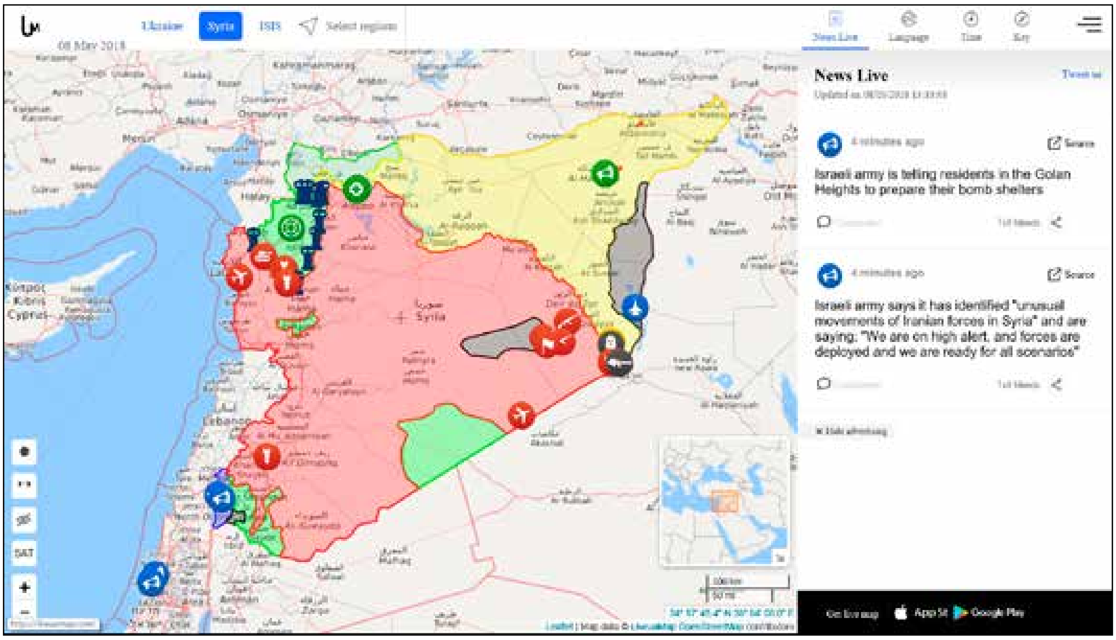
The power of these sources was demonstrated recently when amateur analysts published a minute-by-minute account of the combined US–UK–French strike on Syrian chemical weapons facilities as it was occurring. The details released via Twitter updates included tanker support tracking, strike aircraft routes, and ISR aircraft positions.[45]

Further, developing the kind of awareness that enables quick multidomain action requires continuous collection that not only feeds characterization of actors and activities but of the multiple environments that make up the multidomain battlespace as well. Continuous sensing across domains enables quicker identification of multifaceted patterns and anomalies that lead to speedier identification of opportunities to exploit and vulnerabilities to address. Additionally, increasing data sources and types provide analysts the ability to correlate and cross-verify, ensuring increased veracity of conclusions. It also enables big data reliant methods such as OBI/ABI to perform better with increased volume and variety. As noted in the *JOAC*, this requirement of broader and continuous collection has implications for "steady state sizing, systemic capacity, and analytic technologies of intelligence forces."[46]

To accomplish this, the type of sensors employed and even what constitutes an ISR platform must fundamentally change. In contrast to ISR platforms equipped with narrowly focused sensor suites, observing for MDO requires sensor systems capable of collecting broader types of data. It also demands shifting to an "everything a sensor" model in which every asset, regardless of primary purpose, can simultaneously act as sensor platforms. Every friendly point of presence is also an access point into the battlespace that can be leveraged for collection and, if needed, as a pivot point for potential multidomain maneuver. As Gen Carlton Everhart highlighted during a discussion on air mobility assets, "we need our aircraft to be sensor platforms that can gather and securely communicate information."[47]

This does not mean scrapping the charge to develop ISR sensors and systems designed to penetrate and survive in high-threat areas.[48] These are still critical to acquiring data that would be otherwise impossible to reach. The end result will look similar to a multidomain crowd-sensing effort similar to commercial products like Waze. Every platform and point of presence should be an ISR contributor, an element of a larger intelligence collection network composed of interlinked sensors across all domains.

Further, this approach to collection demands a more prominent role for open-source data. As Col Sean Larkin noted in *Foreign Affairs*, "over the next decade, the market-driven explosion of surveillance sensors and data analytics will bring an unprecedented level of transparency to global affairs. . . offering inexpensive and automated reports on everything from crop yields to military activity."[49] Dr. Jon Kimminau describes how "the foundation of knowledge we need. . . can come from Open Source," freeing more exquisite sensors to collect less accessible data.[50]



News Live

4 minutes ago Source

Israeli army is telling residents in the Golan Heights to prepare their bomb shelters

4 minutes ago Source

Israeli army says it has identified "unusual movements of Iranian forces in Syria" and are saying: "We are on high alert, and forces are deployed and we are ready for all scenarios"

The openly available LiveUAmap's coverage of conflicts in Syria and Crimea produced information that often rivaled classified sources and methods. (Reprinted from image of map of Syria to illustrate unknown aircraft in News Live, accessed 14 May 2018, *https://syria.liveuamap.com*.)

Change how we derive understanding from observation

With new demands to understand more detail on more aspects of the battlespace and activities within it, the challenge then becomes deriving understanding from observation that produces vastly increased data velocity, variety, and volume. This challenge is at the heart of multidomain orienting and requires a significant shift in analysis to produce decision-level understanding without proliferating a multitude of systems that only bury users in data.[51] Fortunately, this is another area where intelligence professionals can adapt recent initiatives in data analysis tools, technologies, and concepts.

First, the current DOD and broader intelligence community efforts to adopt a big-data approach must be redoubled and steered to facilitate multi-domain awareness. Shifting to a big-data construct is ideally suited to the MDO challenge in that it is designed to derive deeper understanding in greater interconnected complexity with vast data volumes and types. As Dr. Kimminau again highlights, increasing data types and volumes should enable cross-domain thinking.[52] In fact, even with "dirty" or raw unprocessed data, a common concern of many ISR professionals regarding big data, these new analytic approaches are proving able to better discern activities or opportunities that analysts did not know to look for in the first place.[53]

Second, artificial intelligence (AI) and machine learning must be further invested in and integrated to provide the speed of analysis in complex interconnected environments to out-orient adversaries at the operational and tactical levels. The multidomain battlespace will increasingly overwhelm existing analytic approaches that primarily rely on human and "brute force" computer analysis. At the same time, advances in commercially developed AI, such as IBM's Watson, are capable of leveraging vast data to learn and develop, as James R. Clapper described, "a beautiful intuition" that can identify and even predict the sort of opportunities and vulnerabilities that enable MDO.[54]

Additionally, AI can further accelerate analysis by quickly translating raw or unstructured data into a more useable form.[55] For instance, AI is proving increasingly proficient in deriving data within raw data, structuring it to become useable by follow-on analytics. A recent example that highlights the utility of these advances is found in a Google team's research on Convolutional Neural Networks' ability to learn, identify, and catalogue objects or activities in video and audio data.[56] Quickly deriving and structuring useful data embedded within other data is critical to maximizing the possibility of finding multidomain opportunities and vulnerabilities, enabling tighter and truer orienting. As the previous Deputy Secretary of Defense noted, "the Department of Defense must integrate artificial intelligence and machine learning more effectively across operations to maintain advantages over increasingly capable adversaries and competitions."[57]

Change How Users Interact with the Observe and Orient System

Changing the OO paradigm and supporting system to enable MDO creates new opportunities for decision makers at all levels in how they engage that system. In particular, the technologically and conceptually complex system described above requires a new approach to crafting and translating critical intelligence requirements to drive collection and analysis. Further, decision makers at all levels will add to and shape the system in real-time as participants, not just receivers.

For this new system to perform, the ISR enterprise must build the connective tissue between decision makers' information needs and the complex analytic system that supports them. This connective layer must perform dynamic mission data science (DMDS) to translate information requirements into analytic models and algorithms that can adapt to meet the demands of an evolving battlespace, enabling true multidomain awareness and prediction. To achieve this higher-order predictive analysis that tightens the OODA loop in multidomain complexity, there must be people in place who understand the requirements and how to dynamically craft the analytic tools to get there.[58]

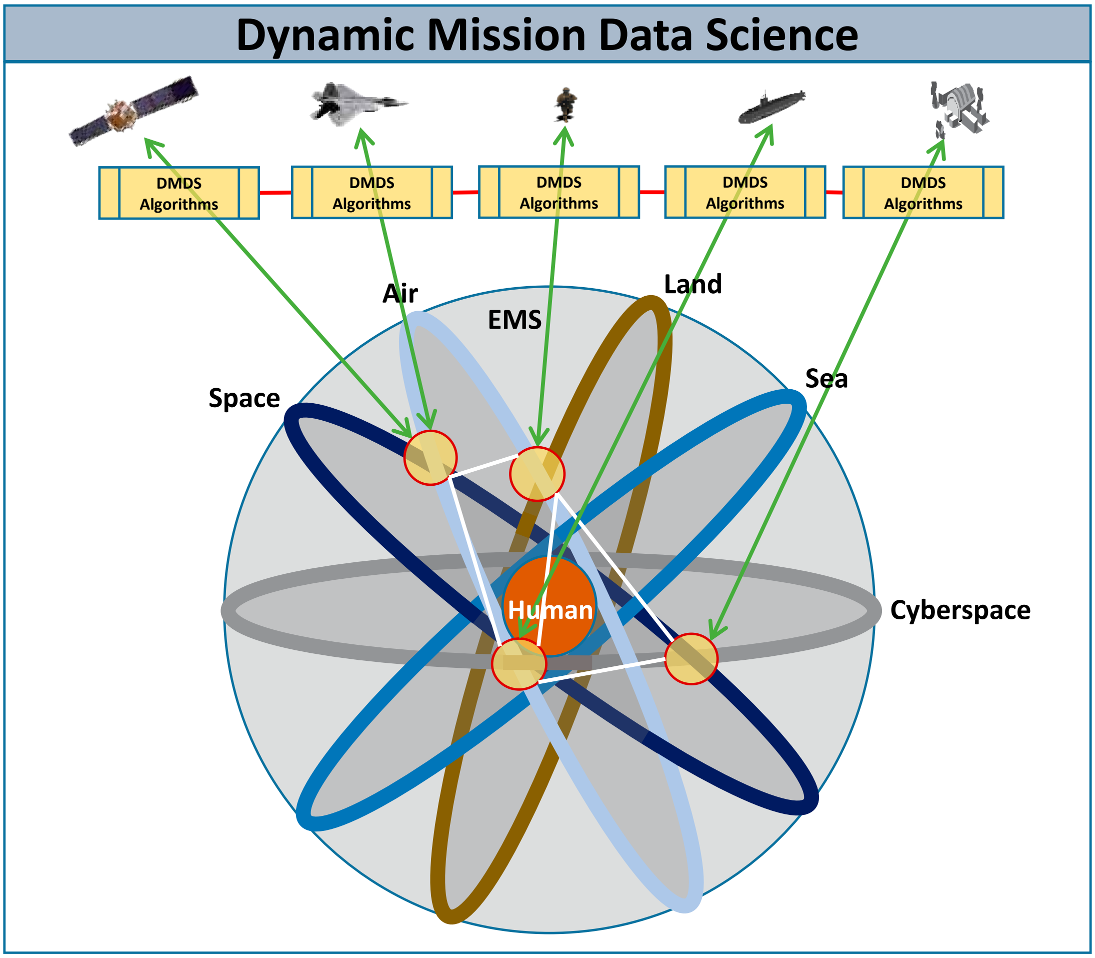
Further, the DMDS function must exist broadly across the operational force to enable multidomain action at all levels of decision and execution. The same data and analytic expertise that provides operational-level insight to JFCs can be leveraged to quickly identify or predict opportunities and vulnerabilities at the tactical level. Different algorithms can be crafted and run on the same data to serve different perspectives and needs. As Vice Adm Jan Tighe notes, it is critical to "more rapidly update, modernize, and customize our applications inside their actual environment with the end-user community fully embedded in that journey."[59] To achieve OODA advantage across a continuum of domains at each level, ISR data science functions must be embedded with each of these end user perspectives.

In addition to connecting with the OO system through a DMDS layer, decision makers and operators will also interact directly with the system to further orient and sharpen collection and analysis. In its simplest form, it is similar to how companies like Amazon leverage consumer interaction with their system to generate more data to analyze and determine how to shape what it produces to best fit the user's needs. In this construct, decision makers are more than users of information, they are participants in the data analytics.[60]

Change How We Architect and Evolve the ISR System

The system that begins to take shape in the descriptions above points toward a change in how the ISR enterprise is designed and, probably more importantly, how it is quickly evolved. The shift toward MDO is largely technology driven and, as such, advantage can be lost just as easily as it is won when adversaries integrate the next technological development that provides it an edge. Because the majority of information technology development is led by private industry, the US must reshape its acquisition model to enable broader and faster partnership with industry. The current infrastructure model and acquisition processes do not allow for the speed required to consistently evolve ahead of threats.

The future ISR infrastructure must be an open architecture system that maximizes interoperability between services and partners, as well as the ability to quickly integrate new capabilities from across industry. It must be based on the same common industry standards that allow the quick evolution and integration of new and disruptive technology in the commercial world. In a battlespace where speed and broad interoperability translate to significant advantage, proprietary developments by a handful of defense contractors is increasingly a national security liability.



Leveraging Dynamic Mission Data Science to conduct multi-domain maneuver, enabling asymmetric advantage that outpaces adversary observe, orient, decide, and act capabilities

An open architecture platform makes it simple to agilely adapt and leverage new sensor or analytic advances as soon as the industry develops them, keeping the ISR enterprise on the technological edge at less cost. A competitive advantage in a complex multidomain battlespace will be achieved by whomever can first leverage developments that drive faster, more capable OO operations: machine learning, cloud analytics, human-machine teaming interfaces, supporting information infrastructure, and so forth.

Further, an open architecture makes possible the degree of interoperability required for interservice and interpartner effectiveness in a multidomain environment. The current architecture, built over decades of individual service initiatives that created proprietary products, hinders or precludes interoperability between domain operators, and thus the true Joint operational flexibility required for multidomain advantage. As a recent *C4ISR* article describes, "the idea behind an open-systems architecture is to create opportunities where you don't have stovepiped, proprietary systems that don't allow for things to plug in."[61] An open architecture system ensures not only that the ISR enterprise can iterate with industry faster, but that it will more easily interconnect across all domain operators and international partners.

Success in a multidomain environment also depends on the ISR enterprise's ability to eliminate stovepipes. At the very heart of the MDO concept is the need for quick maneuver or action between domains. The supporting OO system cannot have barriers in place that prevent or slow the identification of multidomain opportunities or vulnerabilities. The effectiveness of a big-data approach, for example, relies on its ability to leverage disparate multidomain data to correlate opportunities and build a more holistic awareness.

At the information infrastructure level, this means breaking down stovepipes between services and agencies, as well as the types of collection (signals, human, imagery, open source, and so forth). Currently, every type of intelligence is stovepiped, often with separate information environments, and even within each there exist sub-stovepipes of more specific types of collection.[62] Breaking down these stovepipes is critical to transitioning to become data-focused and will require a reexamination of current classification, access, and data sharing protocols.[63]

Change How We Organize to Orient

This re-examination also calls for a change in how the analytic force is organized, moving further toward a sensor agnostic, collaborative, and data science focused force. The goal is to move away from stovepiping thought or data access in a way that limits analysts' ability to identify multidomain opportunity and vulnerability. For the DMDS layer described above to operate effectively, teams composed of analysts, data scientists, and programmers are required at each of the decision-making levels and perspectives. DMDS teams must be present at the unit level to develop and dynamically modify models and tools that feed tactical decisions for ground, air, space, cyber, and maritime operators. These teams must also be present at the JTF and component levels to develop and dynamically modify the models and tools that feed operational decision making. Further, this analytic force arrayed at various levels and perspectives should not be hindered by organizational boundaries to collaborate, enabling an adaptive approach based on a more open organizational construct.[64]

Fortunately, if a cloud-based infrastructure that eliminates stovepipes and enables a true multidomain big-data approach is meaningfully implemented, there will not be a need to expand the ISR workforce. Currently, a majority of the ISR workforce is engaged in time-consuming data-processing functions. Leveraging AI and big-data analytics to increasingly conduct data processing functions potentially liberates thousands of minds to work on analytics.[65] As Vice Admiral Tighe again points out, the Navy's migration to cloud-based architectures, both ashore and afloat, will "enable analytic environments and battle management decision aids that reduce the dependency on our people for tasks that can be automated and free up our analysts to go further, faster in a human-machine teamed environment."[66]

Conclusion

The development and proliferation of advanced technology are once again changing the battlespace and shifting the character of conflict away from what the US military has prepared for. Still in development, the MDO concept proposes a better integration of capabilities across all maneuver domains to overcome challenges that increasingly defy current operational concepts. Although MDO is not a new idea, its emerging shape places new demands on the joint force that have fundamental implications for how it observes and orients itself. MDO will require re-conceptualizing the battlespace, how we derive understanding, reshaping approaches to constructing and organizing ISR, and new ways of using and interacting with the ISR enterprise.

More than 30 years ago, Boyd expressed the need to simultaneously "generate many different possibilities as well as rapidly implement and shift among them" to outmatch adversaries.[67] The MDO concept is built on the idea that these possibilities are exponentially increasing in number as interconnectivity between domains, both physical and virtual, continues to grow. Without the ability to observe and orient to these new combinations of possibilities, however, MDO will remain out of reach. Just as ISR shapes and drives decisions and actions, ISR professionals are now in a position to develop a multidomain OO construct that shapes and drives multidomain warfare from concept to practice. ✪

Notes

1. DOD, *Joint Operational Access Concept*, 7 January 2012, https://www.defense.gov/Portals/1/Documents/pubs/JOAC_Jan%202012_Signed.pdf; and US Army, *Multi-Domain Battle: Evolution of Combined Arms for the 21st Century 2025–2040*, December 2017, http://www.arcic.army.mil/App_Documents/Multi-Domain-Battle-Evolution-of-Combined-Arms.pdf.

2. United Kingdom Ministry of Defence, Joint Doctrine Publication (JDP) 2-00: *Understanding and Intelligence Support to Joint Operations*, 3rd ed. (London, UK: UK Assistant Chief of the Defence Staff, August 2011), 1–4; and Bill Dries et al., "Securing Operational Access: Evolving the Air-Sea Battle Concept," *The National Interest*, 11 February 2015, http://nationalinterest.org/feature/securing-operational-access-evolving-the-air-sea-battle-12219.

3. Jeffrey M. Reilly, "Multidomain Operations: A Subtle but Significant Transition in Military Thought," *Air & Space Power Journal* 30, no. 1 (Spring 2016), 61, http://www.airuniversity.af.mil/Portals/10/ASPJ/journals/Volume-30_Issue-1/V-Reilly.pdf.

4. George M. Gross, "The New Generation of Operational Concepts," *Small Wars Journal,* 8 January 2016, http://smallwarsjournal.com/jrnl/art/the-new-generation-of-operational-concepts.

5. DOD, *Department of Defense Strategy for Operating in Cyberspace*, July 2011, https://csrc.nist.gov/CSRC/media/Projects/ISPAB/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf.

[6] Sydney J. Freedberg, "VCJCS Mulls Newest Domain: Electromagnetic Spectrum," *Breaking Defense*, 22 April 2016, http://breakingdefense.com/2016/04/vcjcs-mulls-newest-domain-electromagnetic-spectrum/.

[7] Max Boot, *War Made New: Technology, Warfare, and the Course of History* (New York: Penguin Books, 2006).

[8] Reilly, "Multidomain Operations," 61.

[9] Joint Chiefs of Staff (JCS), *Joint Concept for Entry Operations*, 7 April 2014, vi, http://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/jceo.pdf?ver=2017-12-28-162000-837.

[10] Reilly, "Multidomain Operations," 67.

[11] Ibid., 71.

[12] DOD, *Joint Operational Access Concept*, 14.

[13] Jeffrey M. Reilly, "Over the Horizon: The Multi-Domain Operational Strategist (MDOS)," *Over the Horizon: Multi-Domain Operations and Strategy*, 13 January 2017, https://overthehorizonmdos.com/2017/01/13/oth-mdos-reilly/.

[14] Marc Van de Mieroop, *A History of Ancient Egypt* (New Jersey: Wiley-Blackwell, 2010), 240–57; Margaret Bunson, *The Encyclopedia of Ancient Egypt* (New York: Gramercy Books, 1999), 111; and Arther Ferrill, *The Origins of War* (London: Westview Press, 1985), 86–87.

[15] Reilly, "Multidomain Operations," 63.

[16] JCS, *Joint Concept for Entry Operations,* 19.

[17] DOD, *Joint Operational Access Concept*, iii; and Dries et al., "Securing Operational Access."

[18] Mark Pomerleau, "Generals Describe Challenges, Characteristics of a Multi-Domain Battle," *C4ISRNET*, 14 March 2017, https://www.c4isrnet.com/show-reporter/global-force-symposium/2017/03/14/generals-describe-challenges-characteristics-of-a-multi-domain-battle/.

[19] Dries et al., "Securing Operational Access."

[20] Reilly, "Multidomain Operations," 71.

[21] Gen David L. Goldfein, "AUSA 2016: Multi-Domain Battle Ensuring Joint Force Freedom of Action in Future War," 4 October 2016, https://www.dvidshub.net/video/485976/ausa-2016-multi-domain-battle-ensuring-joint-force-freedom-action-future-war.

[22] Dries et al., "Securing Operational Access."

[23] Reilly, "Multidomain Operations," 61.

[24] William Dries, "Some New, Some Old, All Necessary: The Multi-Domain Imperative," *War on the Rocks*, 27 March 2017, https://warontherocks.com/2017/03/some-new-some-old-all-necessary-the-multi-domain-imperative/.

[25] John R. Boyd, "The Essence of Winning and Losing" (lecture, Defense and the National Interest [DNI]), Washington, DC, 28 January 1995), https://danford.net/boyd/essence1.htm.

[26] John R. Boyd, "Organic Design for Command and Control," (lecture, DNI, Washington, DC, May 1987) http://www.iohai.com/iohai-resources/organic-design-c-and c_files/frame.htm.

[27] Ibid.

[28] Ibid.

[29] Adapted from Joint Doctrine Publication 2-00, *Understanding and Intelligence Support*.

[30] Air University, *Air Force ISR 2023: Delivering Decision Advantage* (Washington, DC: US Air Force 2012), 7, http://www.airuniversity.af.mil/Portals/10/Research/ISR/Rotator/documents/AF-ISR_2023.pdf.

[31] JCS, *Joint Concept for Entry Operations*, vi.

[32] DOD, *Joint Operational Access Concept*, 29.

[33] Boyd, "The Essence of Winning and Losing."

[34] Boyd, "Organic Design for Command and Control."

[35] JCS, *Joint Concept for Entry Operations*, 20.

[36] Boyd, "Organic Design for Command and Control."

[37] JCS, *Intelligence, Surveillance, and Reconnaissance: Joint Force 2020 White Paper* (Washington, DC: JCS, June 2014), 1, http://www.airuniversity.af.mil/Portals/10/Research/ISR/Rotator/documents/Joint_Force_White_Paper.pdf.

[38] Sean Atkins, "Finding Clarity in Complexity: Interview with Dr. Jon Kimminau [Part I]," *Over the Horizon*, 24 January 2017, https://othjournal.com/2017/01/24/interview-kimminau-part-1/.

39. Sean Atkins, "Clarity from Complexity Part III: An Interview with Dr. Jon Kimminau on Big Data and Activity Based Intelligence," *Over the Horizon*, 30 January 2017, https://overthehorizonmdos.com/2017/02/07/interview-kimminau-part-3/.

40. James R. Clapper (address, 2016 GEOINT Symposium, Orlando, FL, 17 May 2016), http://usgif.org/events/geoint-symposia.

41. Ibid.

42. Benjamin Jensen and Ryan Kendall, "WAZE for War: How the Army Can Integrate Artificial Intelligence," *War on the Rocks*, 2 September 2016, https://warontherocks.com/2016/09/waze-for-war-how-the-army-can-integrate-artificial-intelligence/.

43. Adam Entous, et al., "U.S. Scurries to Shore Up Spying on Russia," *Wall Street Journal*, 24 March 2014, https://www.wsj.com/articles/u-s-scurries-to-shore-up-spying-on-russia-1395625416.

44. Ben Sullivan, "Twitter's the Only Tool You Need for Tracking the Military," *Vice*, 24 April 2017, https://motherboard.vice.com/en_us/article/twitters-the-only-tool-you-need-for-tracking-the-military.

45. David Cenciotti, "Everything We Know [and No one has Said] about the First Waves of Air Strikes on Syria," 14 April 2018, https://theaviationist.com/2018/04/14/everything-we-know-and-no-one-has-said-so-far-about-the-first-waves-of-air-strikes-on-syria/.

46. DOD, *Joint Operational Access Concept*, 29.

47. Gen Carlton D. Everhart III, "Air Mobility, Multi-Domain Operations, and the MAF's Future: An Interview with General Everhart," *Over the Horizon*, 15 May 2017, https://overthehorizonmdos.com/2017/05/15/air-mobility-c2-interview-geneverhart/.

48. *Joint Force 2020 White Paper*, 2.

49. Sean P. Larkin, "The Age of Transparency: International Relations Without Secrets," *Foreign Affairs* 95, no. 3 (May–June 2016), https://www.foreignaffairs.com/articles/world/2016-04-18/age-transparency.

50. Sean Atkins, "Clarity from Complexity Part II: An Interview with Dr. Jon Kimminau on Big Data and Activity Based Intelligence," *Over the Horizon*, 30 January 2017, https://othjournal.com/2017/01/30/interview-kimminau-part-2/.

51. *Joint Force 2020 White Paper*, 1.

52. Atkins, "Clarity from Complexity Part III."

53. Ibid.

54. Clapper, GEOINT Symposium.

55. Atkins, "Clarity from Complexity Part II."

56. Shawn Hershe et al., "CNN Architectures for Large-Scale Audio Classification," Google Inc., 10 January 2017, https://arxiv.org/pdf/1609.09430.pdf.

57. Bob Work, "Establishment of an Algorithmic Warfare Cross-Functional Team (Project Maven)," DOD Memorandum, https://www.scribd.com/mobile/document/346681336/Establishment-of-the-AWCFT-Project-Maven?skip_app_promo=true.

58. Atkins, "Clarity from Complexity Part II."

59. Sean Atkins, "On the Precipice: The Future of Cyber and Intelligence with Vice Admiral Jan Tighe," *Over the Horizon*, 27 February 2017, https://overthehorizonmdos.com/2017/02/27/inteview-vice-admiral-jan-tighe/.

60. Atkins, "Clarity in Complexity," Part I.

61. Mark Pomerlau, "AUSA: Open Architecture and Multi-Domain Battle," *C4ISRNET*, 15 March 2017, http://www.c4isrnet.com/articles/ausa-open-architecture-and-multi-domain-battle.

62. Atkins, "Clarity from Complexity Part II."

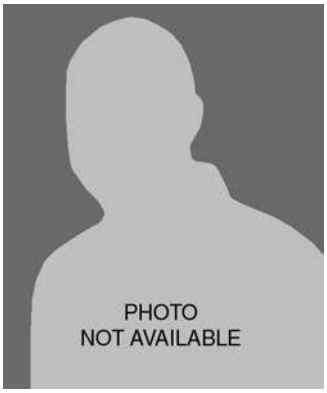
63. DOD, *Joint Operational Access Concept*, 29; and Atkins, "Clarity from Complexity," Part I.

64. JDP 2-00, *Understanding and Intelligence Support*, 1–6.

65. Sean Atkins, "Clarity in Complexity," Part I.

66. Atkins, "On the Precipice."

67. John Boyd, "Patterns of Conflict" (briefing presentation, December 1986), http://www.dnipogo.org/boyd/pdf/poc.pdf (site discontinued).



Maj Sean A. Atkins, USAF

Major Atkins is a doctoral student in the Security Studies Program at the Massachusetts Institute of Technology. Previously, he was the deputy director of future warfare concepts and an instructor in the Air Command and Staff College's multidomain operations and strategy program. Major Atkins has served in a range of assignments from forward operating bases in Iraq to the Office of the Secretary of Defense. He is also the founding editor of *Over the Horizon*, a Chief of Staff of the Air Force Reading List online professional journal that brings together diverse perspectives to advance the conversation on future security.