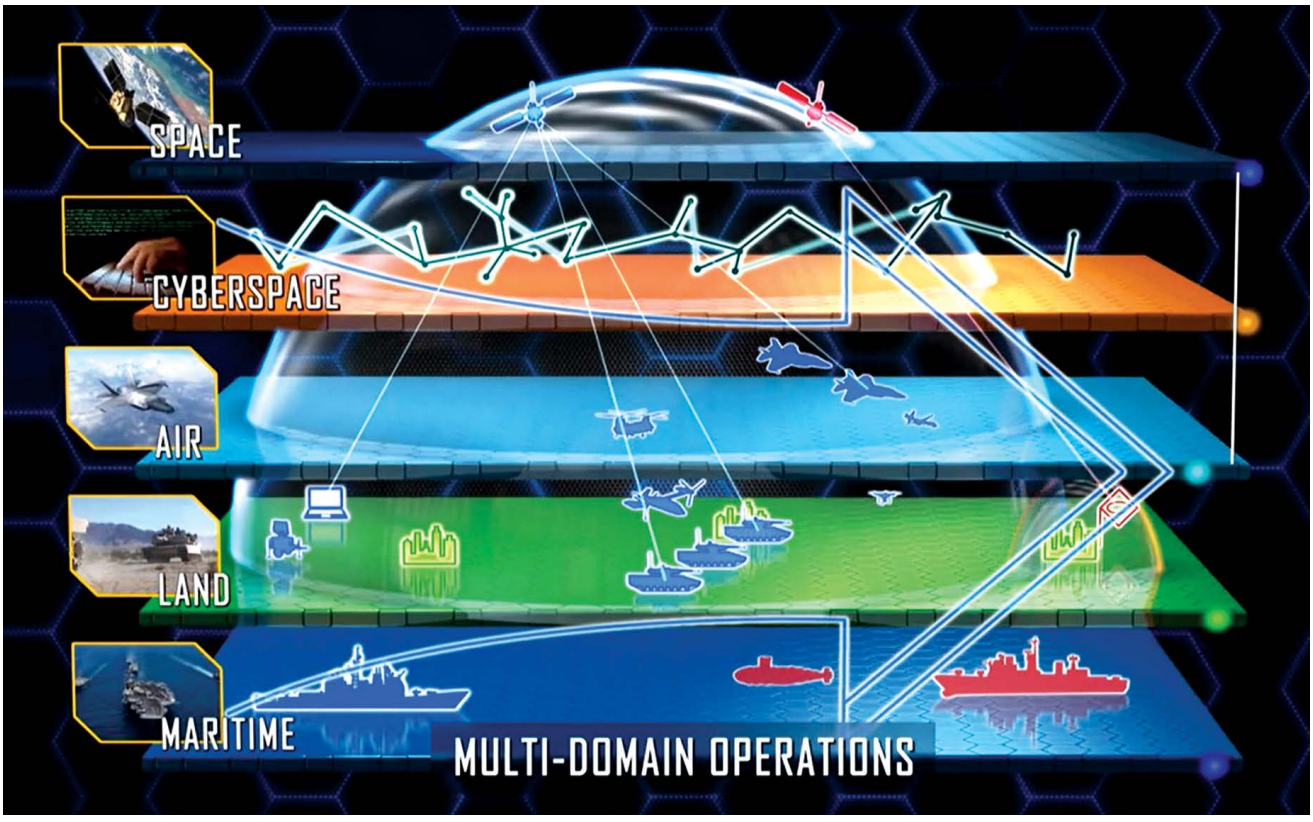
Domain Awareness Superiority Is the Future of Military Intelligence

Chief Warrant Officer 4 Robert M. Ryder, U.S. Army Reserve

Not long after the turn of the century, powers in Europe fought each other in a great world war using dreadfully archaic tactics and formations against rapidly evolving technology. Predictably, casualties were appallingly unspeakable on all sides, with tens of thousands of victims per day of major combat operations. Somewhat unexpectedly, battlefield lethality had increased tenfold over previous conflicts waged just a few years earlier due to rapid improvements in newly automated, quick-fire, highly accurate weapons, massed effects and fires, and machines developed during a rushed technological revolution in industry, information, and communications. Decision cycles became increasingly compressed as decisive points approached at extraordinary speeds, equating to nearly impossible reaction time requirements that shocked leaders and demoralized troops. Likewise, the world recoiled in horror at the lethal devastation unleashed upon its unprepared armies through this disruption in military affairs. The year was 2028.

This photo shows the urban area surrounding the medieval *Kölner Dom*, or Cologne Cathedral, 24 April 1945 in Cologne, Germany, after it had been completely devastated by intense bombing and shelling during high-intensity conventional fighting for control of the city near the end of World War II. Due to the greatly enhanced destructiveness of modern conventional weapons, future large-scale combat operations would likely result in similar if not greater damage to urban areas. (Photo courtesy of the U.S. Department of Defense)



(Screenshot of motion graphic by William Norris, U.S. Army Training Support Center)

Figure 1. U.S. Army in Multi-Domain Operations 2028

> Through the coming Revolution in Intelligence Affairs, machines will become more than just tools for information collection and analysis. They will become intelligence consumers, decision-makers, and even targets of other machine intelligence operations.[1]

Why Is Domain Awareness Not Already a Doctrinal Term?

Surprisingly, the term "domain awareness" is not formally known in Department of Defense organizations, doctrine, or lexicon, nor is it clearly defined in a wider sense, despite its creeping, informal acceptance into modern vernacular.[2] Its defining and subsequent adoption by the intelligence community, however, would solve a significant doctrinal gap in developing multi-domain operations (MDO) and joint all-domain operations (JADO) concepts. This doctrinal gap was created when two unstoppable forces—the information revolution and the nascent revolution in intelligence affairs—not only created the cyber domain (and artificial intelligence possibilities) but also created a domain which now crosses into all others, making a domain awareness concept increasingly relevant.

There are four physical domains (sea, air, land, space) and one functional domain (cyber and the electromagnetic spectrum [EMS]) encompassed in the MDO/JADO concept, which are collectively known as the five operational or warfighting domains (see figure 1). The desire for the rapid convergence of massed effects simultaneously (and at times continually) across several domains at decisive moments in a global, complex operating environment equally necessitates an exceptional, omniscient-like awareness.[3]

There is no unifying terminology for the type of intelligence support now required to meet multi-domain operational needs. The idea of "domain awareness superiority" logically follows; this intelligence-specific concept bridges the 2018 *National Defense Strategy*

reference to "information superiority" and the 2020 joint warfighting concept of "information advantage," which ostensibly leads to operational "decision dominance" (see figure 2).[4]

Current U.S. Army MDO doctrine is based primarily on two documents, U.S. Army Training and Doctrine Command Pamphlet (TP) 525-3-1, *The U.S. Army in Multi-Domain Operations 2028*, and Chief of Staff Paper #1, *Army Multi-Domain Transformation: Ready to Win in Competition and Conflict*, and the relatively new concept of combined joint all-domain command and control (CJADC2) in U.S. Army parlance (or joint all-domain command and control [JADC2] in U.S. Air Force's).[5]

Air Force JADC2 planning doctrine emphasizes the "tension" of balancing between the exploitation of knowledge a decision maker already has versus exploring new knowledge, or the same tension between intelligence (explore) and operations (exploit). While more possible in the long competition phase preceding crisis and conflict, I argue this idea of balance is impossible in a hyperactive battlespace experiencing persistent contact and which will necessitate the near-real time intelligence collection and instantaneous analysis and targeting across all domains.[6] As the Chief of Staff Paper #1 warned in March 2021, "In competition and conflict, joint operations will experience continuous disruption of command and control (C2) from the electromagnetic spectrum (EMS), space, and cyber domains."[7]

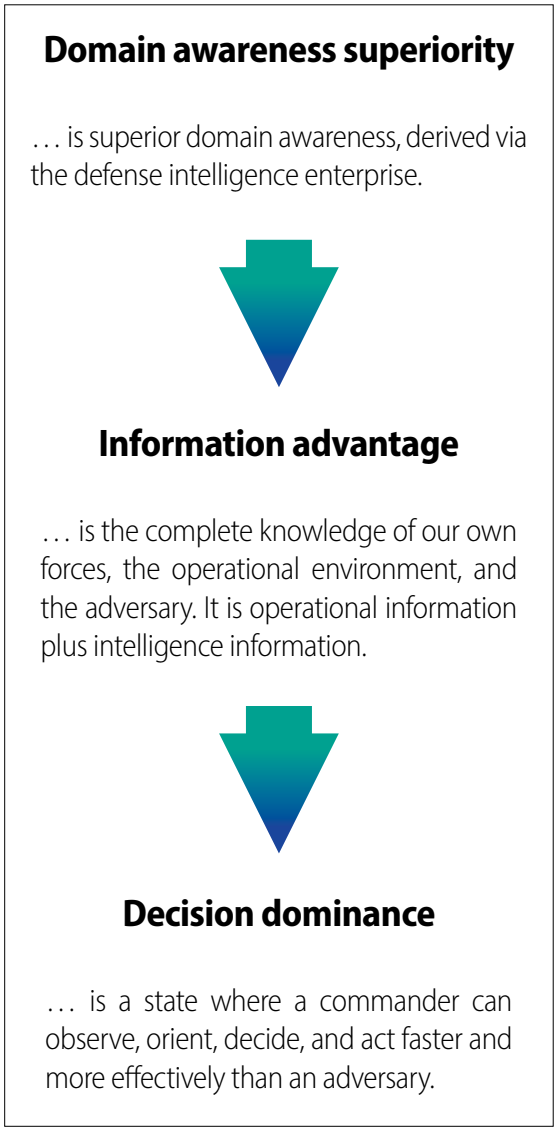
Historically, the terms "common operating picture" or commander's "situational awareness" have been used to portray a simpler semblance of domain awareness when there were just three primary domains. These older concepts, however, are too generalized and do not accurately describe a commander's information needs and future warfare, which will necessarily be highly automated, networked, and roboticized—a frenetic, hyperlethal battlespace distributed across all domains.

In July 2020, the emerging joint warfare concept included a working definition of information advantage, which was "the [operational] ability to integrate the information capabilities of space, cyber, the EMS, and cognitive activities to increase the commander's awareness and understand faster than RED [the opposing force], while inhibiting RED's ability to so the same."[8]

Domain awareness and domain awareness superiority are the intelligence-related concepts supporting information advantage that include kinetic and nonkinetic targeting of our adversary's ability to also achieve domain awareness superiority.

The June 2019 *Capstone Concept for Joint Operations* explains in an unclassified section: "The Joint Force will enable Information Advantage through knowledge of itself, its opponents, and the environment in which it fights. This advantage allows the Joint Force to moderate tempo against technologically peered adversaries."[9] Knowledge of "itself," or the joint force, is "enterprise domain awareness," as described later in this article.

Commanders must know of which domains they do not have sufficient awareness to properly task intelligence warfighting systems. They will need to close these intelligence gaps to enable their operational elements to converge on targets in one or more



(Figure by author)

Figure 2. Domain Awareness Is the Unifying Concept Between Intelligence and Operations

(Graphic courtesy of Lockheed Martin)

domains rapidly, simultaneously, and at times, continually. Domain awareness is key to JADO, whereas situational awareness is a lesser concept that more accurately refers to the interplay of battlespace effects on the joint force and the joint force's effects on the battlespace in near real time. Domain awareness creates situational awareness, while the converse may not necessarily be true.

TP 525-3-1 acknowledges the joint force has two major technical shortfalls in achieving convergence: the lack of a joint visualization and decision support tool (i.e., common operational picture), and the lack of joint sensor-to-shooter synchronization capabilities that enable any joint shooter to see all intelligence, surveillance, and reconnaissance (ISR) and targeting data. Again, domain awareness is the key to help solve both problems.[10] But first, we need to define it.

Defining Domain Awareness

"Domain awareness" is a compound construction of two nouns, "domain" and "awareness," where domain functions as an adjective to describe awareness. What a domain is depends on context. Relevant modern definitions include a field, realm, sphere, or a range of knowledge, activity, influence, responsibility, or a physical region characterized by specific features.[11]

Awareness is simpler; it is the quality or state of realization, perception, knowledge, or understanding that something is (or is not) happening or exists (or does not exist).[12] By taking key elements of all of the preceding definitions and concepts, the proposed definition follows:

> Domain Awareness is having operational knowledge of a particular sphere of concern, and understanding its interactions with other domains in a given environment. By extending Domain Awareness across all domains, the Intelligence Community Enterprise and organic, joint ISR and operational sensors enables superior Domain Awareness through the timely creation and sharing of multidisciplined intelligence data at all classification levels through directed or automated dissemination mechanisms in near real time.[13]

Operational warfighting domains are not the only domains that fall under the overall domain awareness concept. Other domains may include functional or conceptual domains like medical, financial, political, human, legal, executive, and more. Some domains, like the five operational domains, are external to an organization, whereas the functional domains can be internal factors affecting an organization, or are external domains to manage. For example, policy and legal (i.e., statutory authorities or intelligence oversight governance) domains often play an outsized, fundamental role in an intelligence organization's operations, and play into a definition of enterprise domain awareness. Know yourself, in other words. As Sun Tzu might have said if he was alive today,

> It is widely said that if you have Domain Awareness Superiority and also Enterprise Domain Awareness you will not be defeated in a hundred battles; if you do not have Domain Awareness Superiority but do have Enterprise Domain Awareness, you will win one and lose one; if you do not have Domain Awareness Superiority nor Enterprise Domain Awareness, you will be imperiled in every single battle.

The Army is a system of systems and is a large enterprise with a combat mission delegated by various statutes that authorize policies that govern the enterprise's operations. There is a system of budgeting, execution, and regulatory oversight that directly affects the enterprise capabilities and the employment of those capabilities. In essence, these internal domains affect the operational environment during competition in peace and conflict in war (i.e., always). The proposed definition of enterprise domain awareness for an intelligence entity is having institutional knowledge of all the operational domains on which an organization has intelligence data and knowing how internal domains of policy, capabilities, operations, and others influence the organization's ability to generate operational domain awareness.[14]

Goodbye Situation Awareness, Hello Domain Awareness Superiority

Artificial intelligence (AI) and its subdiscipline machine learning are emerging and future technologies that will enable the realization of domain awareness. These technologies will process, exploit, and disseminate the torrent of sensor and intelligence information collecting against information requirements in all operational domains in near-real time. A National Geospatial Intelligence Agency director estimated that the agency will need the equivalent of eight million imagery analysts by 2037 to process and make sense of the volume of imagery information that will be available by then.[15] When ultimately paired with augmented cognition, human intermediaries will play a crucial role in managing domain awareness and domain awareness superiority processes, including sensor-to-shooter interactions. These humans-in-the-loop will ultimately need to be enabled through cyberware and brain-computer interfaces.

In June 2020, the Office of the Director of National Intelligence released the first framework for the intelligence community's ethical use of AI and machine learning, which followed on from the January 2019 release of its augmented intelligence using machines strategy initiative.[16] The U.S. House Armed Services Committee released their *Future of Defense Task Force Report* in September 2020. This somewhat dire report argues for a "Manhattan Project" in defense-related AI, mandated Department of Defense spending on AI systems, and for the United States to lead international efforts on the practical and ethical uses of AI for defense purposes.[17]

The incorporation of AI into the military and national security realms will fundamentally change the way wars are fought and won. Whichever nation triumphs in the AI race will hold a critical, and perhaps insurmountable, military and economic advantage.

—Future of Defense Task Force Report 2020[18]

The key to focus the military intelligence enterprise as we progress—and as our competitors and adversaries likewise pursue these technologies—is the goal of superior domain awareness. This goal is the raison d'être of why and what we are trying to accomplish in military intelligence support to MDO; we are moving far beyond just the creation of situational

Chief Warrant Officer 4 Robert M. Ryder is a U.S. Army Reservist with thirty years of service in the intelligence community, mostly at strategic-level echelons, including mobilizations to the Joint Staff J-2 and the U.S. Forces-Iraq J-2. He holds a Master of Science in strategic intelligence from National Intelligence University and is an adjunct instructor of analytical methodologies at a Department of Defense agency where he is primarily employed as a strategic-level intelligence analyst.

awareness for human decision-makers. We are moving into all-domain awareness leading to information advantage and decision dominance.

Long-term technological or informational overmatch on peer or near-peer adversaries is likely to be an unrealistic goal, but the potential for superior domain awareness will be achievable under at least some conditions. One condition where it may not be, however, is if our adversaries develop faster computing and smarter AI, though enemy domain awareness capabilities can be degraded and deceived through cyber effects or attacks in the EMS or against ISR—as well as against ours. Domain awareness superiority could be an intermittent phenomenon, with both sides grasping it momentarily before the other side takes it back through automated attacks and integrated all-domain effects.

Domain awareness will be key when employing increasingly robotized, automated forces that necessarily rely on high-fidelity information on all domains. The systems that produce domain awareness capability must be high fidelity, redundant systems generating and providing highly accurate information to sensors and shooters. Otherwise, unresolved ethical considerations involving the use of lethal autonomous weapons will prohibit our developing them, let alone our destroying them on the battlefield. Further, expect the proliferation of small, low-Earth-orbit satellite sensors to enable friendly and adversarial domain awareness and imagine a multipronged, robust antisatellite capability to automatically destroy them and satellites in all orbits at the onset of hostilities.[19] Defeating intelligence collection systems that enable adversarial domain awareness and domain awareness superiority will be a top priority on the way to decision dominance.

On Bias

Within any given decision cycle in a hyperactive engagement, the side with domain awareness superiority should win most battles, even when disadvantaged in a correlation of forces. One key to achieving domain awareness superiority is going to be ongoing, objective assessments of "consciousness"—of how one's domain awareness exists across a qualitative or semiquantitative spectrum.[20] We must develop and emplace quality assurance systems that attempt to objectively discover blind spots in ISR coverage, data, and intelligence gaps, military deception, and various other undesired biases and confounding variables. The ultimate risk is assuming domain awareness superiority exists, when it may just exist as a form of incomplete situational awareness.

> We need a common focal point to keep us on track developing the systems and processes to allow us to keep pace with the onrushing future: domain awareness superiority.

One significant obstacle of true domain awareness is the concept of data bias, where AI algorithms focus only on data that is easily collected, accessible, favored, or particularly suitable to automation (i.e., electronic intelligence, measurement and signature intelligence, geospatial intelligence, or signals intelligence metadata).[21] For instance, human intelligence is not particularly suitable for automation (in either collection or analysis), and similarly, neither is communications intelligence—yet. The promise of AI suggests the ability to parse this type of unstructured intelligence will occur, however, along with the correlation of publicly available and open-source, intelligence-derived data and information. Nonetheless, data bias will continue to be a vast problem that is difficult to solve.

There may also be bias in measurement information (e.g., accuracy or precision due to calibration error, spoofing, or resolution), legacy database field mismatch, legacy database entry errors, and others such as data and target revalidation. Deception is another pitfall. Only AI and an unbiased domain awareness baseline will enable the detection of sophisticated and cheap swarms of AI-facilitated denial and deception operations.

> Using the Manhattan Project as a model, the United States must undertake and win the artificial intelligence race by leading in the invention and deployment of AI while establishing the standards for its public and

private use. Although the Department of Defense has increased investment in AI and established the Joint Artificial Intelligence Center to assist with the transition and deployment of AI capabilities, cultural resistance to its wider adoption remains. Congress and the Department of Defense must take additional action to overcome these barriers.[22]

The Future All over Again, but Much Sooner Than We Expect

We are rapidly headed toward algorithmic warfare whether we like it or not, and we must learn the lessons of the impacts of the Industrial Revolution had on large-scale combat operations in the two world wars; the impacts from the information revolution will almost certainly be the same. Recall the advancements in both information and space technologies over the past fifteen years and similarly project forward to imagine 2035. Assume a realized breakthrough in quantum computing somewhere in that time frame, and the future will be on us. Accordingly, we need a common focal point to keep us on track developing the systems and processes to allow us to keep pace with the onrushing future: domain awareness superiority.

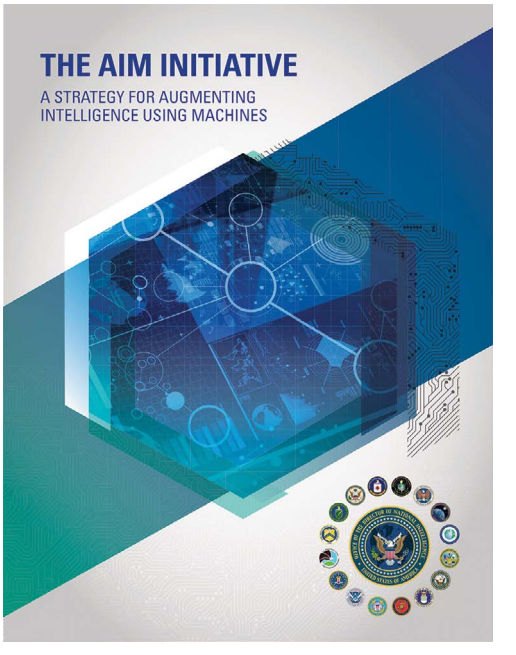
True domain awareness superiority is predictive, not just descriptive (which it fundamentally needs to do well). It will predict enemy courses of action and be able to preemptively queue ISR at automatically generated named areas of interest designed to confirm or deny the most likely actions, as well as warn joint targeteers to prepare for associated fires or effects missions and feed them the required domain awareness information. Domain awareness superiority is joint and will naturally feed information to all sensor-to-shooter systems so the transition to more automated targeting is realized. Defining the domain awareness superiority concept and incorporating it into doctrine will help focus the Army intelligence enterprise to meet the Army's 2035 MDO AimPoint Force objectives and drive change across the entire Department of Defense for JADO. ■

Notes

1. Anthony Vinci, "The Coming Revolution in Intelligence Affairs: How Artificial Intelligence and Autonomous Systems Will Transform Espionage," *Foreign Affairs* (website), 31 August 2020, accessed 16 June 2021, https://www.foreignaffairs.com/articles/north-america/2020-08-31/coming-revolution-intelligence-affairs.

2. Maritime Security Policy Coordinating Committee, *National Plan to Achieve Maritime Domain Awareness for the National Strategy for Maritime Security* (Washington, DC: U.S. Department of Homeland Security, December 2013), iv. The phrase "maritime domain awareness" has been in common use

For those readers interested in supplemental information including detailed explanations and analysis of evolving concepts related to multi-domain operations and domain awareness dominance, see Army Futures Command Pamphlet 71-20-1, *The Army Futures Command Concept for Maneuver in Multi-Domain Operations 2028,* at https://api.army.mil/e2/c/downloads/2021/01/20/2fbeccee/20200707-afc-71-20-1-maneuver-in-mdo-final-v16-dec-20.pdf.



To view *The Aim Initiative: A Strategy for Augmenting Intelligence Using Machines*, visit https://www.dni.gov/index.php/newsroom/reports-publications/item/1940-the-aim-initiative-a-strategy-for-augmenting-intelligence-using-machines.

for decades, and is used in national security contexts, such as the 2013 *National Maritime Domain Awareness Plan for the National Strategy for Maritime Security*. In this context, maritime domain awareness is "the effective understanding of anything associated with the maritime domain that could impact the security, safety, economy, or environment of the United States."

3. U.S. Army Training and Doctrine Command (TRADOC) Pamphlet (TP) 525-3-1, *The U.S. Army in Multi-Domain Operations 2028* (Fort Eustis, VA: TRADOC, December 2018), 20. The joint all-domain operations tenet of convergence is "the rapid and continuous integration of capabilities in all domains that optimizes effects to overmatch the enemy through cross-domain synergy and multiple forms of attack, all enabled by mission command and disciplined initiative."

4. Merrick E. Krause, "Decision Dominance: Exploiting Transformational Asymmetries," *Defense Horizons* No. 23 (Washington, DC: Center for Technology and National Security Policy, National Defense University, February 2003), accessed 22 June 2021, https://ndupress.ndu.edu/Portals/68/Documents/defensehorizon/DH-023.pdf. "Decision dominance" is a still-emerging term that has drifted from how it was first described by Krause in February 2003, as a state where a commander can deny an adversary decisional options while maintaining his own; Sydney J. Freedberg Jr., "Army's New Aim Is 'Decision Dominance,'" Breaking Defense, 17 March 2021, accessed 16 June 2021, https://breakingdefense.com/2021/03/armys-new-aim-is-decision-dominance/. As of March 2021, Army Futures Command Gen. Mark Murray describes it as "the ability for a commander to sense, understand, decide, act, and assess faster and more effectively than any adversary."

5. *Army Multi-Domain Transformation: Ready to Win in Competition and Conflict*, Chief of Staff Paper #1 (Arlington, VA: Headquarters, Department of the Army, 16 March 2021) (hereinafter CSA March 2021).

6. Air Force Doctrine Publication 3-99, *Department of the Air Force Role in Joint All Domain Operations* (Maxwell Air Force Base, AL: Curtis E. Lemay Center for Doctrine Development and Education, 8 October 2020).

7. CSA March 2021.

8. Joint Staff J-5 representative, personal communication with author, July 2020. "RED" refers to the opposing force.

9. Ibid.

10. The word "awareness" appears just three times in TP 525-3-1, *The U.S. Army in Multi-Domain Operations 2028*, all in appendix D on dense urban terrain, twice in the form of situational awareness, and once in State Department awareness.

11. *Oxford English Dictionary Online*, s.v. "situational," accessed 1 July 2021, https://www.lexico.com/en/definition/situational.

12. *Oxford English Dictionary Online*, s.v. "awareness," accessed 1 July 2021, https://www.lexico.com/en/definition/awareness.

13. Joint Publication 3-0, *Joint Operations* (Washington, DC: U.S. Government Publishing Office, 22 October 2018). By "operational knowledge," the author intends to convey flexibility within a limited conceptual range. Generally, operational knowledge is that knowledge, which when operationalized, enables tactical force employment to achieve strategic objectives. It encompasses the entire spectrum of knowledge management: the deliberate discovery, capture, storage, sharing, utilization, monitoring, and (re)creation of knowledge; or, in other words, having the knowledge required to conduct successful operations. See Giulio Valente and Alessandro Rigallo, "An Innovative Approach for Managing Competence: An Operational Knowledge Management Framework," in *Knowledge-Based Information and Engineering Systems: 7th International Conference, KES 2003, Oxford, UK, September 2003, Proceedings, Part I*, ed. Vasile Palade, Robert J. Howlett, and Lakhmi Jain (Berlin: Springer, 2003), accessed 16 June 2021, https://link.springer.com/chapter/10.1007/978-3-540-45224-9_136.

14. CSA March 2021. The Army Continuum Analysis (ACA) is a form of Enterprise Domain Awareness. The ACA is the term given to the iterative process of using wargames, scenarios, and data analysis to drive deep future doctrine development in conjunction with developing capabilities and force generation.

15. Robert Cardillo, "Small Satellites—Big Data" (remarks, Utah State University, Logan, UT, 7 August 2017), accessed 16 June 2021, https://www.nga.mil/news/Small_Satellites_-_Big_Data.html.

16. Patrick Tucker, "New Intelligence-Community AI Principles Seek to Make Tools Useful—and Law-Abiding," Defense One, 23 July 2020, accessed 16 June 2021, https://www.defenseone.com/technology/2020/07/new-intelligence-community-ai-principles-seek-make-tools-useful-and-law-abiding/167163/; "Artificial Intelligence Ethics Framework for the Intelligence Community, v. 1.0 as of June 2020" (Washington, DC: Office of the Director of National Intelligence [ODNI], June 2020), accessed 16 June 2021, https://www.dni.gov/files/ODNI/documents/AI_Ethics_Framework_for_the_Intelligence_Community_10.pdf; *The Aim Initiative: A Strategy for Augmenting Intelligence Using Machines* (Washington, DC: ODNI, 16 January 2019), accessed 16 June 2021, https://www.dni.gov/index.php/newsroom/reports-publications/item/1940-the-aim-initiative-a-strategy-for-augmenting-intelligence-using-machines.

17. U.S. House Armed Services Committee, *Future of Defense Task Force Report 2020* (Washington, DC: U.S. House Armed Services Committee, 23 September 2020), accessed 16 June 2021, https://armedservices.house.gov/_cache/files/2/6/26129500-d208-47ba-a9f7-25a8f82828b0/6D5C75605DE8DDF0013712923B4388D7.future-of-defense-task-force-report.pdf.

18. Ibid.

19. Defense Intelligence Agency, *Challenges to Security in Space* (Washington, DC: Defense Intelligence Agency, January 2019), accessed 16 June 2021, https://www.dia.mil/Portals/27/Documents/News/Military%20Power%20Publications/Space_Threat_V14_020119_sm.pdf.

20. Such as no awareness, low awareness, partial awareness, moderate awareness, etc., or a percentage-based estimate.

21. Mike Mullane, "Eliminating Data Bias from Machine Learning Systems," Medium, 13 November 2018, accessed 16 June 2021, https://medium.com/e-tech/the-impact-of-data-bias-on-machine-learning-4875498b9f84.

22. U.S. House Armed Services Committee, *Future of Defense Task Force Report.*