The Operational Environment in Multi-Domain Operations

by Mr. Darryl Ward

Introduction

As an operational environment (OE) evaluator supporting the Army Quality Assurance Program, I have observed how Army centers and schools set conditions to prepare leaders for unified land operations. The Army institutional base is undergoing a major sea change in unified land operations as we transition from years of stability-centric operations to re-hone atrophied warfighting skills associated with large-scale combat operations. A key unified land operations aspect specified in ADP 3-0, *Operations,* is "across multiple domains to shape operational environments."[1] So how do Army institutions shape OEs? More importantly, how do these institutions replicate contested multiple domains that help shape OEs? It is the latter question I will address and offer some recommendations. Tackling this question, as the Army wrestles with educating leaders to operate in contested multi-domains, enables further understanding and shaping of future OEs.

History and Past Operations

To appreciate the context of multi-domain environments, it might help to go back and recapture some of the more significant events that altered our ways of planning and prosecuting warfare. My intent is not to present an all-inclusive history lesson but rather to make it like Mel Brooks's *History of the World: Part I.*[2] So for brevity, I left out several important events.

Through the centuries, warfare generally occurred in the domains of land and maritime environments. The tactics and geometries with which battles were fought on the fields and seas have certainly changed with the discovery of black powder in the 9th century and technological advancements such as optics in the early 17th century.[3] These achievements led to increased ranges, lethality, and improved situational awareness; however, for the most part, warfare remained a surface-level affair until the late 18th century.

In the 18th century, specifically in the 1780s and 1790s, French experiments with hot air balloons, and then hydrogen-filled balloons, led to manned observation platforms to achieve the ultimate high ground (so they thought) and signaled the beginning of a third domain (air) that would change warfare forever. Just over a century later, these crude aerial observation platforms progressed to rudimentary delivery means for strategic bombing during World War I. Roughly three decades later, during World War II, rapid technological advances in the air domain culminated with the aerial bombings of Hiroshima and Nagasaki and helped usher in the atomic age.

World War II did more than bring a new era to the world; it also initiated a fourth (space) domain with the V-2 rocket program. The V-2 was the world's first long-range ballistic missile that achieved an altitude anywhere between 55 and 120 miles, thus departing and reentering the Earth's atmosphere (more or less). No distinct separation exists between the Earth's atmospheric layers and outer space, but it is generally accepted to be at 62 miles altitude.[4] Much like its predecessors, the space domain was and still is marked with rapid technological advances. From earlier space exploration (Sputnik, Vostok, Mercury, Gemini, and Apollo) to where we are today, much of what we take for granted in telecommunications, navigation, weather forecasting, etc., was made possible through our current perception (Gene Roddenberry fans notwithstanding) of the ultimate high ground. Today, approximately 2,000 satellites orbit in the Earth's exosphere,[5] making such capabilities as positioning, cellular phones, and the Internet of Things seem routine.

Considering that the air and space domains are divided around the 60-mile mark, all domains have a physically distinct feature that separates them—except for one, the cyberspace domain. Cyberspace, or "cyber" for short, is the fifth domain that interconnects with the other four domains via the electromagnetic spectrum and thus serves

as an enabler for synchronizing, coordinating, processing, and storing information. Likewise, cyber is also a lucrative target because of the relatively low cost with regard to the resources needed to execute cyber warfare compared with high gains in terms of second-order effects to the other domains. Indeed, one can acquire insight into how potential threats perceive the importance of cyber in the following excerpt from *Unrestricted Warfare:* "To a very great extent, war is no longer even war but rather coming to grips on the internet, and matching the mass media, assault and defense in forward exchange transactions, along with other things which we had never viewed as war, now all possibly causing us to drop our eyeglasses. That is to say, the enemy will possibly not be the originally significant enemy, the weapons will possibly not be the original weapons, and the battlefield will also possibly not be the original battlefield."[6]

Multi-Domain Concepts and Doctrine

Operating in multiple domains is not new to the U.S. Army. Even the active defense doctrine from the mid-1970s, which segued to AirLand Battle 2000 in the 1980s and 1990s, contained domain aspects that orchestrated forces on land, sea, and air. In fact, AirLand Battle 2000 is where we begin to see military applications of space for reconnaissance, surveillance, and targeting. Both of these doctrines served their purpose for a defensive posture against a monolithic conventional threat. However, lessons learned from United States Army operations in Afghanistan and Iraq, which varied in conflict and operational theme, necessitated the 2008 publication of FM 3-0, *Operations*. A significant chapter in the manual is on *Information Superiority*.[7] It is here we first learn about the Army's informational tasks. Some of these tasks (for example, command and control warfare and information protection) and their associated capabilities evolved into the current cyberspace missions and actions we see in the 2017 FM 3-12, *Cyberspace and Electronic Warfare Operations*.[8] Therefore, while the term *multi-domain* introduced in TRADOC Pamphlet 525-3-1, *The U.S. Army in Multi-Domain Operations 2028,*[9] may sound new, the concept of operating in multiple domains against a near-peer or even a peer threat is not.

Guidance

From the National Defense Strategy to the Army Posture Statement, these important documents acknowledge the challenges the U.S. Army faces in an ever-competitive global security environment. The reemergence of Russia and China as pacing threats and the nuclear ambitions of rogue nations such as North Korea and Iran command our attention, and transregional terrorist groups remain a persistent threat. Given the multitude of capabilities associated with current and potential adversaries, the Army's challenge to prevail in unified land operations, as well as our institutional base to train and educate the next generation of Army leaders, has never been greater. Perhaps the best guidance I have read is in the *Fiscal Year 2020 Combined Arms Center Command Guidance*. It says, "Enable the Army to transition **the current [counterinsurgency] COIN-centric fielded force to a [multi-domain/large-scale combat operations] MD-LSCO force with the capability and capacity…**that can continuously **compete** and, when required, **prevail** in large scale combat against peer threats in multi-domain contested environments."[10] Army centers and schools need no more than this statement to realize why it is important to create conditions that replicate contested domains.

U.S. Army photo collage

For the past two years, the Army has initiated many changes to help modernize the force. Among those changes, Army Futures Command found a new home, Soldiers began receiving a new rifle, and the Army made strides to improve its hypersonic, networking, and artificial intelligence capabilities.

Future Operational Environment

We live in a world of more than 7 billion people. The National Intelligence Council estimates that by 2030 the global population will be more than 8 billion and the trend for people to

move to urban settings will increase, causing the urban population to climb to nearly 60 percent.[11] Think about what an extra billion means to already stressed infrastructures, increasing demands, limited global resources, and climatic changes that serve as a catalyst for reducing resources in some areas (desertification in Africa) while opening new areas in others (oil exploration in the Arctic). When you connect the dots, you see why pacing threats are modernizing their militaries.

Just as with our lessons learned, threats are studying the U.S. Army and drawing their own lessons. Threats understand that to counter a power projection capability such as the U.S. military, they must be able to separate forces in terms of time, space, and function. Threat antiaccess and area denial (A2AD) strategies will therefore include elements that attack multiple domains and fight in depth, beginning at the U.S. homeland. The earlier passage from *Unrestricted Warfare* provides a glimpse into the conceptual view of this fight to disrupt and disaggregate U.S. forces.[12]

A2AD strategies will target multiple domains. The following information is not all-inclusive but provides an idea of how threats are planning to disrupt, delay, and disaggregate. In the cyber domain, which affects all domains, information warfare elements such as computer warfare and information attacks performed via denial of service, malware emplacement, and network penetration may create abnormalities in mission command network performance, create erroneous information, and spoof end users. In the air, land, maritime, and space domains, electronic warfare through nonlethal and lethal directed-energy weapons (lasers, radio frequency) will also incapacitate or destroy mission command sensors and communication systems, jeopardize aircraft survivability, and limit performance of unmanned aircraft systems (UAS). In the not too distant future for air, land, maritime, and space domains, physical destruction through enhanced kinetic energy weapons (hypervelocity rail guns) will seek strategic high-payoff targets that might be continents away.[13] In the air, land, and maritime domains, special-purpose forces and proxies will target strategic air and seaports of embarkation/debarkation, power grids, communication, and transportation networks. Finally, I don't want to forget chemical, biological, radiological, and nuclear (CBRN) defense. I participate in a U.S. Army Forces Command countering weapons of mass destruction working group, which anticipates discussions about CBRN as a battlefield condition in future large-scale combat operations.

Multi-Domain Impacts on Unified Land Operations

ADP 3-0, *Operations,* defines unified land operations as, "simultaneous execution of offense, defense, stability, and defense support of civil authorities across **multiple domains** to shape operational environments, prevent conflict, prevail in large-scale ground combat, and consolidate gains as part of unified action."[14] I highlighted *multiple domains* because the question is, how do we replicate contested multiple domains?

We are a land component, yet we depend on multiple domains such as cyber and space. The Army relies on space to communicate; use positioning, navigation, and timing (PNT); protect; sustain; and enable intelligence. The Army's reliance on cyber (internet, telecommunication networks, computer systems, processors, and controllers) affects every domain, warfighting function, and individual. A typical brigade combat team has more than 2,500 PNT-enabled devices and over 250 satellite communications space-enabled devices.[15] An individual can easily have 13 or more cyber identifiers.[16] Think about those numbers. I believe you will agree that the Army relies on multiple domains such as cyber and space to help shape the OE in order to prevail in unified land operations. Threats plan to contest these domains; therefore, it is imperative that Army centers and schools create classroom and field conditions that are conducive to getting future leaders to think about operating in contested domains.

Classroom Conditions

Replicating contested multiple domains in the classroom for Army centers and schools is a greater challenge than

U.S. Army photo

Officers and noncommissioned officers within the Joint Force Headquarters-National Capital Region and the U.S. Army Military District of Washington participated in a week-long Company Commander/First Sergeant Course on Joint Base Myer-Henderson Hall, VA, 28 October to 1 November 2019.

replicating these domains at an Army combat training center. For starters, the outcomes are different. Leader development tasks at centers and schools focus on individual learning step activities, while combat training centers focus on collective training objectives. Centers and schools lack the dedicated ground opposing forces (OPFOR) that are at the combat training centers along with a World Class Cyber OPFOR that provides direct support to the combat training centers. Finally, leader development at centers and schools occurs primarily in classroom situations using constructive means via simulations rather than the live training provided at combat training centers (the Mission Command Training Program is the exception). However, centers and schools can still take steps to create rigorous conditions for learning outcomes and get leaders in the mindset that they are operating in contested domains.

My recommendations for the following training areas are described below:

- Analog planning and battle tracking.
- Personal devices.
- Air superiority.
- Creation of a degraded electromagnetic spectrum.
- Degraded precision-guided munition (PGM) effectiveness.
- Target acquisition.
- Battle drills.
- Camouflage, cover, and concealment.
- CBRN defense.

Analog Planning and Battle Tracking. Reliance on digital systems such as Command Post of the Future has led to atrophied analog skills. Force students to maintain backup paper maps and overlays during planning and execution that maintain the common operational picture. Get students to verify data and never to assume. As previously stated, threats to PNT systems will attempt to spoof, block, or create erroneous data. If a discrepancy exists between digital and analog systems, it might indicate a threat computer warfare and/or information attack.

Personal Devices. The threat is always in the reconnaissance phase. Here is a simple multi-domain condition the instructor can create during any lesson that places students in an operational planning or execution setting. Ask students whether they have their personal electronic devices (cell phone, smartwatch, Fitbit device, etc.) with them. These items are all targetable and exploitable by the threat. We must be constantly aware that the threat wants our digital signature, and it is our responsibility to make it as difficult as possible for them to achieve that goal. Get students used to the idea of not bringing personal digital devices into the classroom, just as they should not take these devices into an operational setting.

Air Superiority. Students must understand that when planning large-scale combat operations against a peer threat, they can no longer assume the luxury of friendly air superiority.

Creation of a Degraded Electromagnetic Spectrum. A threat will attempt to interdict communications through electronic warfare. The results could be a degraded electromagnetic spectrum that disrupts communications. Force students to plan for couriers to send and receive information, limit total asset visibility, and delay the classes of resupply. These are injects that can be scripted into an exercise and do not require replication by virtual or constructive means.

Degraded Precision-Guided Munition Effectiveness. Threat nonlethal and lethal attacks against PNT systems will affect PGM effects. Space-related weather (solar winds, flares) may also naturally generate electromagnetic interference. Reconstitute constructive OPFOR in simulations to replicate ineffective PGM strikes due to threat or electromagnetic interference-induced effects. Force students when building their attack guidance matrices to plan for additional sensors to assess PGM effects.

Target Acquisition. Threat attacks against PNT systems will also affect the acquisition of high-payoff targets for time-sensitive targeting. This should be accounted for during planning, specifically during wargaming, and rehearsed by the students to develop battle drills when high-payoff targets cannot be detected or unexpectedly appear.

Battle Drills. While on the subject of battle drills, disciplines learned in the classroom will carry over to operational assignments. A noted shortcoming of staffs during combat training center rotations was their lack of battle drills when under electronic attack (jamming) by the OPFOR.[17] Have students develop and rehearse battle drills such as primary, alternate, contingency, and emergency plans for responding to electronic attack and naturally occurring electromagnetic interference.

Camouflage, Cover, and Concealment. Assume others have the ability to observe us via satellites and UAS. More than 65 countries have satellites,[18] and those countries without satellites, including non-nation states, may acquire satellite imagery from open sources or pay those that have it. Students should get into the habit of sound force protection practices. This includes planning for camouflage, cover, and concealment of high-value targets to avoid detection from

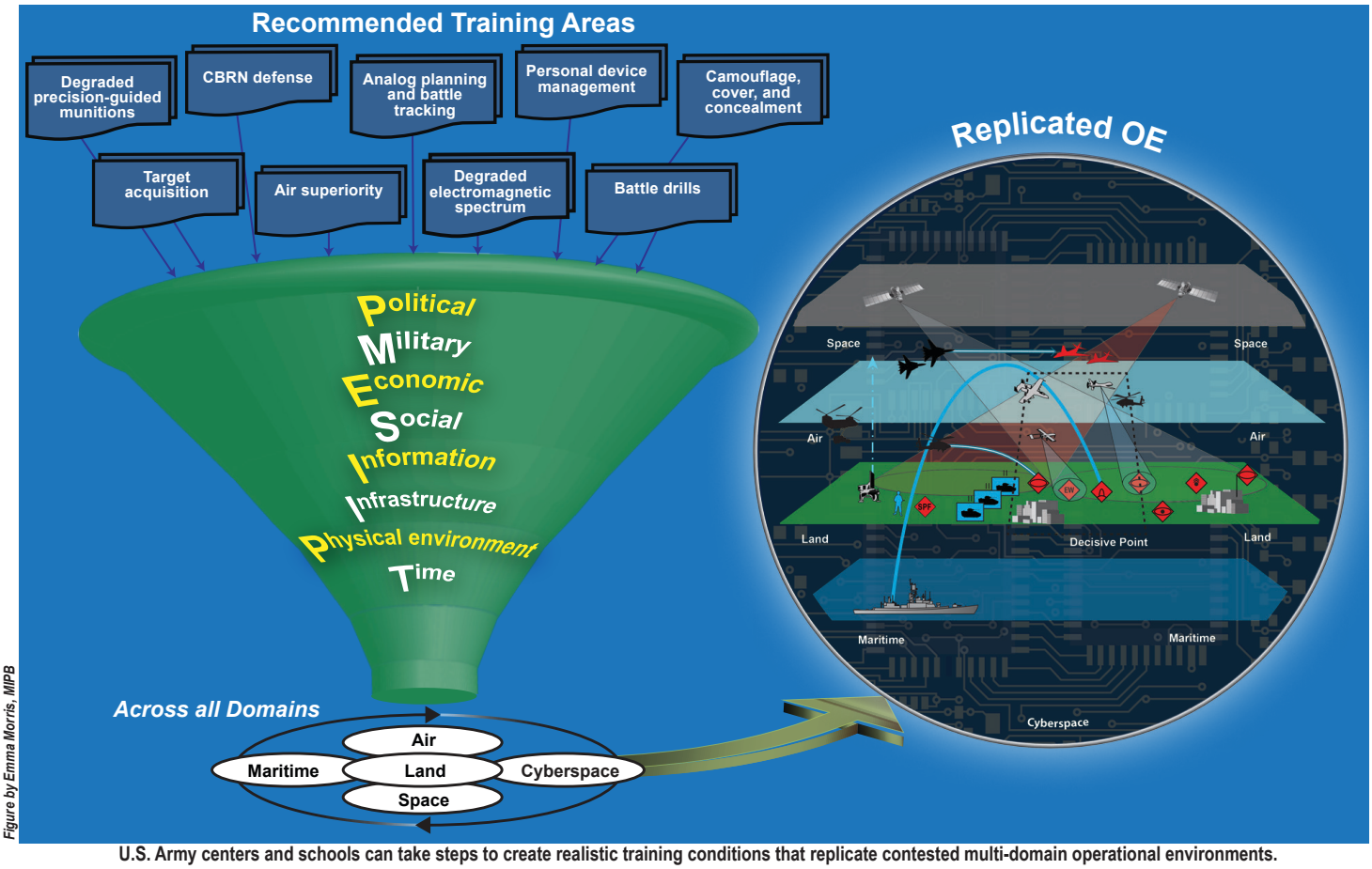

Figure by Emma Morris, MIPB

U.S. Army centers and schools can take steps to create realistic training conditions that replicate contested multi-domain operational environments.

satellites and UAS. Planning for observation from space and air domain capabilities is a good practice to implement both in classrooms and in field environments.

Chemical, Biological, Radiological, and Nuclear Defense. CBRN defense is an anticipated condition in the next large-scale combat operation. The threat will target troop concentrations, logistical centers, main supply lines, and key terrain to disaggregate/slow momentum. This will disrupt timelines for reception, staging, onward movement, and integration as well as classes of resupply. Students must account for threat CBRN capabilities during the planning process.

Conclusion

Finally, I will return to my original question: How do Army institutions replicate multiple domains that help shape OEs? I will leave you with my personal observation. The doctrinal operational variables of political, military, economic, social, information, infrastructure, physical environment, and time (PMESII–PT) do not do a particularly good job in specifying the domains. This might lead to an unintentional omission during planning of domain impacts on the OE. JP 3-0, *Joint Operations,* states, "[operational areas] OAs have physical dimensions composed of some combination of **air, land, maritime, and space domains.**"[19] ADP 3-0 further states, "The area of interest always encompasses aspects of the **air, cyberspace, and space domains.**"[20] So while PMESII–PT does not specify the five domains, if Army centers and schools get their students to think of air, cyber, land, maritime, and space as extensions of the physical environment when defining the OE, and create some of the conditions described in the classroom, this will go a long way in our ability to shape the OE.

Endnotes

1. Department of the Army, Army Doctrine Publication (ADP) 3-0, *Operations* (Washington, DC: U.S. Government Publishing Office [GPO], 31 July 2019), 3-1.

2. *History of the World: Part I* is a 1981 American sketch comedy film written, produced, and directed by Mel Brooks. Despite carrying the title *Part I*, there is no sequel; the title is a play on *The History of the World* by Sir Walter Raleigh who wrote the work while prisoner in the Tower of London. He intended to write a multivolume set but only managed to complete the first volume before being beheaded. Wikipedia, s.v. "History of the World, Part I," last modified 20 July 2020, 6:19, https://en.wikipedia.org/wiki/History_of_the_World,_Part_I.

3. Neil deGrasse Tyson and Avis Lang, *Accessory to War: The Unspoken Alliance Between Astrophysics and the Military* (New York: W.W. Norton & Company, 2018).

4. Brandon Specktor, "The Edge of Space Just Crept 12 Miles Closer to Earth," Live Science, July 25, 2018, https://www.livescience.com/63166-outer-space-border-karman-line.html.

5. Union of Concerned Scientists (UCS) Satellite Database, updated April 1, 2020, https://www.ucsusa.org/resources/satellite-database.

6. Qiao Liang and Wang Xiangsui, *Unrestricted Warfare: China's Master Plan to Destroy America* (Los Angeles: Pan American Publishing Company, 2002). Written by two colonels in the People's Liberation Army, the book was originally titled *Unrestricted Warfare*. In 1999, the Foreign Broadcast Information Service, an open-source intelligence component of the Central Intelligence Agency, made the English translation available. In 2002, the book was published in English, with the subtitle *China's Master Plan to Destroy America*. Wikipedia, s.v. "Unrestricted Warfare," last modified 25 July 2020, 17:35, https://en.wikipedia.org/wiki/Unrestricted_Warfare#cite_note-:1-1; and Wikipedia, s.v. "Foreign Broadcast Information Service," last modified 13 May 2020, 23:01, https://en.wikipedia.org/wiki/Foreign_Broadcast_Information_Service.

7. Department of the Army, Field Manual (FM) 3-0, *Operations* (Washington, DC: U.S. GPO, 27 February 2008 [obsolete]), 7-1–7-13.

8. Department of the Army, FM 3-12, *Cyberspace and Electronic Warfare Operations* (Washington, DC: U.S. GPO, 11 April 2017).

9. 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), GL-7.

10. Department of the Army, *Fiscal Year 2020 Combined Arms Center Command Guidance* (Fort Leavenworth, KS: U.S. Army Combined Arms Center, 2 August 2019), 1.

11. Office of the Director of National Intelligence, *Global Trends 2030: Alternative Worlds* (Washington, DC: National Intelligence Council, December 2012), 26.

12. Qiao and Wang, *Unrestricted Warfare*. An abridged version derived from a translation by the Foreign Broadcast Information Service is available at https://www.c4i.org/unrestricted.pdf.

13. Department of the Army, TRADOC Pamphlet 525-92, *The Operational Environment and the Changing Character of Warfare* (Fort Eustis, VA: TRADOC, 7 October 2019).

14. Department of the Army, ADP 3-0, *Operations,* 3-1 (emphasis added).

15. Department of the Army, FM 3-14, *Army Space Operations* (Washington, DC: U.S. GPO, 30 October 2019), 1-1.

16. Department of the Army, FM 3-12, *Cyberspace and Electronic Warfare Operations,* 1-14.

17. Department of the Army, Center for Army Lessons Learned Handbook No. 18-28, *Operating in a Denied, Degraded, and Disrupted Space Operational Environment* (Fort Leavenworth, KS: Center for Army Lessons Learned, June 2018).

18. UCS Satellite Database.

19. Office of the Chairman of the Joint Chiefs of Staff, Joint Publication 3-0, *Joint Operations* (Washington, DC: The Joint Staff, 17 January 2017), IV-9 (emphasis added). Change 1 was published on 22 October 2018.

20. Department of the Army, ADP 3-0, *Operations,* 4-3 (emphasis added).

Mr. Darryl Ward is retired from military service with the U.S. Army. He has 35 combined years of military intelligence experience in the Army and civil service and as a government contractor. He currently serves as a contractor in the U.S. Army Training and Doctrine Command G-27 Operational Environment/Opposing Force Program Validations Division supporting the U.S. Army Quality Assurance Program. He holds a bachelor of science in education from the University of Arkansas and a master of arts in health business administration from Webster University.