No. 22
November 2018

The Mitchell Forum

Access, Control, Exploit:
Defining Multi-Domain Operations

By Lt Col Cory S. Hollon, USAF

About the Forum

The Mitchell Forum exists to give an open venue to authors with ideas and thoughts on national defense and aerospace power. The series features topics and issues of broad interest and significant impact on current and emerging policy debates. The views expressed in this series are those of the author, and not necessarily those of the Mitchell Institute.

Abstract

The phrase "multi-domain operations" (known as MDOs) is now pervasive in current military writings and analysis. Unfortunately, most authors fail to define it, leading to confusion. Worse, it can seem as if people are discussing the same set of issues when they are not. This paper attempts to rectify the situation, examining each component word and then the phrase as a whole. Warfighting in a single domain is about gaining access to the domain in question, controlling the domain, and exploiting that control to create effects. However, multi-domain operations are more than operations in adjacent domains. To possess meaning as a distinct phrase, there must be some relationship in the access, control, and exploitation of the domains. Therefore, this paper argues that multi-domain operations are a set of tactical actions taken in one domain in order to enhance the access, control, or exploitation of one or more different domains. There are two types of multi-domain operations. First, a set of tactical actions that could exploit two or more domains to create effects on a target or objective simultaneously—convergence. Second, a multi-domain operation could gain access and control in one domain in order to create opportunities in a separate domain—establishing windows of domain superiority. True MDOs require a common language, integrated capabilities, packaging of these multi-domain capabilities, and the elimination of classification stovepipes.

Introduction

The phrase "multi-domain operations" (also known as an MDO or MDOs) has become a pervasive descriptor in current writing about US military operations. However, there is a great deal of confusion concerning what qualifies as "multi-domain."[1] If the reporting and commentary about this concept is to be believed, MDOs are:

- a "decisive asymmetric advantage"
- "an evolution in warfare"
- "both lethal and non-lethal" capabilities
- "interconnected from the strategic to the tactical level"
- and "seamless, dynamic and continuous integration of capabilities generating effects in all domains."[2,3,4,5,6]

This is quite the list of attributes and capabilities, but it does not address the issue of what qualifies as a multi-domain operation—and what does not. A true MDO requires creating a common language, eliminating classification stovepipes, integrating capabilities, and packaging together multi-domain capabilities.[7] Considering that "multi-domain" is approaching near-cliché buzzword status, adopting a clear definition about what is and what is not an MDO is essential to preempt future discussion and debate about operational approaches and required capabilities from degenerating into platitudes.

Warfighting in a single domain can be understood as a sequence of actions taken to access, control, and exploit that domain. A definition of an MDO should address the interaction between the access, control, and exploitation of two or more domains.

In order to arrive at a clearer definition of multi-domain operations, this paper will first examine the individual words in the phrase. The current use of the phrase hints that it is more than just the sum of its parts. For example, to understand what an MDO is, one must first extrapolate the meaning of a single-domain operation. Warfighting in a single domain can be understood as a sequence of actions taken to access, control, and exploit that domain. A definition of an MDO should address the interaction between the access, control, and exploitation of two or more domains. Better put, MDOs are a set of tactical actions in one subsection of the naturally occurring physical environment (also known as one of the classical "domains" of land, air, sea, space, and, more recently, cyberspace) taken to enhance the access, control, or exploitation of one or more different subsections of the naturally occurring physical environment. This paper explores this structure more fully, and concludes by examining the implications resulting from the adoption of this definition.

First, we need to review the concept of a domain. While MDOs are more than just a definition of their component parts, it is useful to examine what the individual words mean within current US military doctrine. Joint doctrine does not directly define an MDO, but does define each of the five warfighting domains: air, space, cyber, land, and sea. With the exception of cyberspace, these definitions have a common structure in that each is within a physical environment on or above the surface of the Earth. In contrast, the definition of cyberspace places it within the information environment and includes various networks of information technology and the data contained within them. Cyberspace fits awkwardly with these other domains because it is actually a subcategory (or environment) of a broader and naturally occurring physical domain: the electromagnetic spectrum. That domain subsumes cyberspace and includes capabilities such as electronic attack, directed energy weapons, and non-cyberspace communication tools and techniques.

Second, this paper needs to clearly define "operation." US Joint Staff doctrine

defines an operation as "a sequence of tactical actions with a common purpose or unifying theme."[8] The two key points to note here are that operations consist of a series of tactical actions, not just one, and these actions are all aligned with a common purpose. Therefore, a single tactical event, such as the takeoff and landing of an airplane, which technically incorporates two domains, is not a multi-domain operation. Furthermore, a series of related tactical events, such as the establishment of a beachhead, is an operation, but not a multi-domain one since the activity is limited to the maritime domain.

Military actions in a particular domain are iterative sequences of access, control, and exploitation. Initially, forces gain access to the domain. This could be as simple as connecting a computer to the internet or as complicated as launching a satellite into orbit. Once an actor gains domain access, they will attempt to control some portion of it. Military forces must establish control long enough to exploit the domain and achieve an effect. To be a MDO, this exploitation must have some sort of relationship with a different domain. MDOs, then, are sets of tactical actions in one subset of the naturally occurring physical environment in order to enhance the access, control, or exploitation of one or more different subsets of this environment.

After gaining access to a domain, the fighting begins—if it is possible. Access to a domain does not guarantee the freedom to act within it.

The First Step: Access

Access is the first step of battle within a domain. Denying individuals access to the land domain, for example, requires military forces to kill, physically remove, or place an obstacle to entry (such as land mines or fortifications) in front of them. In all other domains, however, there is already some technological barrier to access. In the maritime domain, for instance, combatants use ships or boats (even if they are unmanned) to project force. If an adversary can maintain some type of fleet, they can continue to access the domain even if their opponent can control most of it. Similarly, in the air domain, aircraft—specifically designed to operate in the air domain—are required for access. Without airborne weapons systems, there can be no access to the air domain. In space, there is a two-fold barrier: One is the technology to put a spacecraft or object into space, and the other is the technology required to communicate with it and control it through the electromagnetic spectrum. In the electromagnetic domain, military forces require computers and a connection to a network. The barrier to access of the electromagnetic domain is so low, as evidenced by the proliferation of computers and increasing skill of hackers, that it may be useless to develop an operational approach seeking to deny an adversary access to this actual domain. However, access to every domain is a prerequisite to being able to fight within it. Electromagnetic spectrum effects or kinetic capabilities that can destroy technology needed to operate within a domain can prevent an adversary force from entering it—holistically denying them the ability to project combat power in, from, or through the domain.

Securing the Freedom to Act: Control

After gaining access to a domain, the fighting begins—if it is possible. Access to a domain does not guarantee the freedom to act within it.[9] *Control* centers on the ability to act within a domain once a military force overcomes the physical or technological barrier to access. Each opponent seeks to control the domain to the extent required to perform operations essential to their military objectives. For example, land forces will seek to physically occupy certain terrain. If one

force cedes that area, then there will be no fight for control of the domain there. However, if that force seeks to defend the area, a battle will ensue for control over it. In the other domains, control is more broadly understood as a degree of dominance allowing one force to conduct operations without "prohibitive interference by the opposing force."[10] The need for control is not, however, equivalent to the need for permanent dominance in a domain. For example, if a naval convoy is able to project control of the maritime environment around it sufficiently to enable its movement from one location to another, then it does not matter if an enemy gains control in the vacated area or in an area that is not on the convoy's route. Similarly, control in the air is required, but only for the duration of and in the location necessary to enable the desired tactical action (the traditional definition of air superiority). Control follows from access and is required in order to produce desired effects.

…control is more broadly understood as a degree of dominance allowing one force to conduct operations without "prohibitive interference by the opposing force." The need for control is not, however, equivalent to the need for permanent dominance in a domain.

Achieving Objectives Through Effects: Exploit

The goal of all military action is to have some effect on the adversary parallel with the intent of achieving an objective. Military forces use access and control of a particular domain in order to *exploit* it to pursue tactical, operational, or strategic aims. Access and control of a particular portion of a domain does not achieve larger objectives on its own. In other words, an air force can shoot down all the enemy aircraft in the skies, but if the enemy tank commander is drinking in the squadron bar after the air force's main airfield has been overrun by adversary armored units, these pilots are likely to wind up on the losing side of the conflict. The exploitation of control of a domain is what truly matters in warfare. For example, if one belligerent state has control of a key piece of terrain, the presence of that state's forces could threaten certain actions and result in the loss of other territory. The control of one section of the domain is only meaningful in relation to its usefulness in achieving objectives.

Effects Across Domains: Deny

There are some operations, though, that do not fit neatly within the above paradigm. For example, a surface-to-air missile system (SAM) operates in the land domain (or maritime domain in some cases), but it prevents access to the air domain. Could it be posited that a sufficiently advanced SAM system could control the air in a segment of the air domain? If so, the "access-control-exploit" construct, as a somewhat sequential approach, would be a misunderstanding of military force application. However, a SAM does not really control the air as much as it denies its use to a given force or actor. Consider a case in which both sides in a conflict deploy highly capable SAM systems within operational range of each other. The threat rings of these weapon systems overlap such that their effects completely cover the space between them. Neither side would have control of the air, since neither side could access it to carry out exploitation. In this case, it follows, each force denies the domain to the other. SAMs work to deny the air domain through the exploitation of the land domain. Similarly, an electronic attack aircraft attempts to deny the use of the electromagnetic spectrum in a particular area. It does not seek to contest control of the domain, but to prevent its exploitation.

A good way to understand the actions vis-a-vis the access-control-exploit construct is as a branch from access—since access could result as a product of a domain's exploitation. For example, manipulating

the electromagnetic spectrum can disrupt navigation or control of a small remote piloted aircraft (RPA). On the other hand, access may be extraordinarily brief, such as when a SAM battery shoots a missile through the air at another aircraft. Further, using a kinetic kill mechanism against on-orbit systems may cause enough space debris to deny that portion of the domain to all orbital actors. Whatever the case, after gaining access to a domain, military forces can take actions to deny the adversary use of that domain. If one force can get to the point of such denial, that may be sufficient to achieve their political objectives. The bar to gaining victory is set lower for defensive forces: All they have to do is deny access or control of a domain in order to achieve their objectives. The offensive force, in contrast, must act to gain access and at least some degree of control to exploit a domain in the pursuit of said objectives.

Framing the definition of multi-domain operations through the lens of the access-control-exploit construct clearly divides what is and what is not an MDO. First, an MDO must include more than one tactical action in order to qualify. Second, an MDO will include the exploitation of two or more domains. As stated before, the point of military operations is to exploit the access and control of domains, so it follows that an MDO would require exploitation of more than one domain. However, this eliminates actions that originate in one domain and create effects in another. Aerial bombing, for example, should be classified as a cross-domain operation because it exploits the access and control of one domain to create effects in another. Finally, MDOs would include coordinated actions from two or more domains that affect a single target simultaneously or affect operations where actions in one domain enable access to and control of another domain, or convergence.

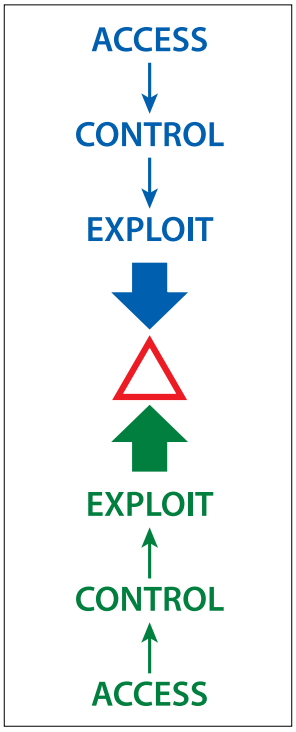

Figure 1: True multi-domain operations would utilize convergence—that is, coordinated actions from at least two or more domains that affect a single target at the same time.

Convergence is the simultaneous application of forces from two or more warfighting domains on a single target or objective. It presents the adversary with multiple dilemmas by which they can only defend against one attack at the cost of exposing themselves to increased vulnerability from another.

For example, consider a land force maneuvering against an enemy force while an air force attacks the enemy formation. Enemy systems and capabilities could only be optimized against one of these threats. In practical terms, it would prove cost-prohibitive to develop enough defensive systems to be able to defeat attacks from both vectors. The enemy will probably only be able to concentrate an effective defense against one of these two threats. Similarly, convergence could potentially overload the adversary's ability to respond by presenting several dilemmas across the range of warfighting domains. An electronic attack combined with kinetic effects from either land or air could quickly overwhelm an adversary's ability to understand—much less respond to—this multi-domain attack.

Convergence operations are inherently complex, and currently require extensive coordination and planning to bring capabilities from multiple domains to bear on a target at the same time. Executing such operations consistently, rapidly, and frequently requires detailed integration of capabilities from conception through training and employment. These operations, though, can create valuable windows of domain superiority to achieve military objectives and end states if executed correctly—the core goal of MDOs.

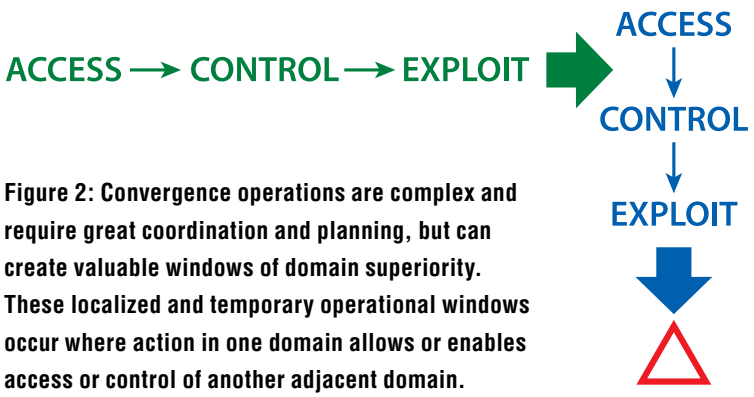

Figure 2: Convergence operations are complex and require great coordination and planning, but can create valuable windows of domain superiority. These localized and temporary operational windows occur where action in one domain allows or enables access or control of another adjacent domain.

Windows of domain superiority are temporary and localized instances where actions in one domain allow or enable access and control of an adjacent domain. Future combat operations will be contested in all domains, but operations must continue to exploit these domains despite adversary action.[11]

The key to success is the creation of windows of domain superiority by gaining temporary access and control of a domain while preventing significant interference from adversary actions. Additionally, military forces must be able to quickly and easily combine forces from multiple domains into a mission package, enabling a window of domain superiority, which in turn enables the exploitation of the other domain. For example, if land-based capabilities can suppress enemy air defenses, air forces should be prepared to integrate with them to take advantage of the opportunity.

Tangentially, the common language requirement for MDOs highlights the need for better and faster communications. Too often, classification stovepipes prevent adequate communication between US military service components and ele-ments of a potential operational solution.[12] As a result, leaders, planners, and operators are unaware of capabilities that could enhance access, control, or exploitation of a given domain. Alternatively, these same groups could be unaware of opportunities or vulnerabilities their own actions bring to bear in other domains. However, if each series of tactical actions were viewed through the prism of the access-control-exploit construct, their implications for other domains would be clearer. As such, this framework provides even more rationale for breaking down classification and organizational stovepipes.

To rapidly and frequently employ MDOs, the US military (and others) will require integration of forces operating in, from, and through all domains.[13] The time required to plan, coordinate, and create windows of domain superiority and converge forces on targets—and doing so often enough to be a military's fundamental operational approach—is currently prohibitive, and thus makes it difficult to institutionalize this construct as a fundamental operational approach. However, integration of capabilities from inception through development, fielding, and employment over time will enable MDOs on a larger scale, and at a more rapid pace.[14]

Capabilities that can be integrated are only one part of the solution to the challenges facing MDOs. In order for convergence to be effective, capabilities need to be packaged together to present an adversary with multiple dilemmas from multiple domains. The multi-domain packages, therefore, must

have capabilities that are complementary but independently lethal to the target or objective they are prosecuting. If not, the target can safely ignore one attack in order to defeat the other. By combining independently lethal effects that exploit the access and control of their individual domains, multi-domain packages will find significantly more success. Additionally, multi-domain packages enable rapid and frequent execution of MDOs. Because speed will be vital in future wars, packaging multi-domain capabilities is necessary to maintain this tempo.[15]

Multi-domain operation plans and packaging will necessitate changes to current command and control structures and relationships among the US military's forces. Currently, the US armed services and combatant commands are not optimized for the nature of these type of operations.

…military forces will need to protect themselves from offensive multi-domain operations. One option is developing layered defenses in different domains that can rapidly converge on attacking forces.

For example, new capabilities are extending the range that land forces can employ organic fires from. Future planners and commanders will need to integrate these forces with other long-range forces (specifically air and cyber forces) to provide effective convergence and prevent a scattershot effect that an enemy might be able to overcome. Current command relationships and the division of authorities among geographic and functional commanders are not adaptive, agile, or fast enough to prosecute this kind of warfare effectively. Future forces will have to develop effective means to integrate and employ with sufficient frequency, agility, and rapidity to fully implement a multi-domain approach. In the meantime, framing the problem set as one of complementary access, control, and exploitation should drive the composition and development of future capabilities.

Finally, military forces will need to protect themselves from offensive multi-domain operations. One option is developing layered defenses in different domains that can rapidly converge on attacking forces. Alternatively, some commanders may choose to limit their own operations in a domain in order to negate an adversary's advantage. For example, if one force is reliant on space-based communication, an adversary may decide that denying access to those assets through the electromagnetic spectrum may be sufficient to tip the balance of power in a specific area. The access-control-exploit framework allows commanders the flexibility to accept some degradation of their own power if and when it has more impact on their adversary. As a result, military conflict will become less about technological superiority in one domain and more about the ability to rapidly transition actions in between domains.

Defining multi-domain operations as a combination of their components is inadequate. Doctrinal definitions should shape what is termed an MDO, but that term should also have a more distinctive meaning. The combination of effects from multiple domains is only one part of an MDO. A better way of defining a multi-domain operation is to treat it as a phrase as opposed to a term. The relationship actions between discrete domains is essential in understanding how to develop and employ multi-domain capabilities and operations.

MDOs, as understood by convergence or windows of domain superiority, allow a military commander to place an enemy on the heels of multiple dilemmas. The challenge ahead is understanding what an MDO is, integrating and packaging capabilities to be able to execute it, and establishing organizations that can lead and direct it. Understanding an MDO through the lens of an access-control-exploit framework is the first step to developing sustainable multi-domain-capable military forces. ✪

Endnotes

1 Michael Spirtas, "Toward One Understanding of Multiple Domains," *C4ISRNET*, May 1, 2018, http://www.c4isrnet.com/opinion/2018/05/01/toward-one-understanding-of-multiple-domains (all links accessed October 2018).

2 Wilson Brissett, "Prioritizing Multi-Domain Command and Control," *Air Force Magazine*, June 19, 2017, http://www.airforcemag.com/Features/Pages/2017/June%202017/Prioritizing-Multi-Domain-Command-and-Control.aspx.

3 Jonathan Bott, "Outlining the Multi-Domain Operational Concept Part II: Evolution of an Idea," *OTH Journal*, June 21, 2017, https://othjournal.com/2017/06/21/outlining-the-multi-domain-operational-concept-part-ii-evolution-of-an-idea.

4 Thomas Aretz II, "Information Operations in a Multi-Domain Operations Battlespace," *Over the Horizon Journal*, March 28, 2018, https://othjournal.com/2018/03/28/information-operations-in-a-multi-domain-operations-battlespace.

5 Shmuel Shmuel. "Multi-Domain Battle: AirLand Battle, Once More, with Feeling," *War on the Rocks,* June 20, 2017, https://warontherocks.com/2017/06/multi-domain-battle-airland-battle-once-more-with-feeling.

6 B. Chance Saltzman, *Multi-Domain Command and Control*, Washington, DC: Headquarters US Air Force, March 14, 2017, https://technodocbox.com/Computer_Networking/76064621-Multi-domain-command-and-control.html.

7 Aaron Kiser and Jacob Hess, El Mostafa Bouhafa, and Shawn Williams, "The Combat Cloud: Enabling Multi-Domain Command and Control Across the Range of Military Operations," Master's thesis, Air Command and Staff College, 2017, http://www.dtic.mil/dtic/tr/fulltext/u2/1042210.pdf; Amy McCullough, "Lockheed Conducts Multi-Domain Command and Control Experiments," *Air Force Magazine*, February 27, 2018, http://www.airforcemag.com/Features/Pages/2018/February%202018/Lockheed-Conducts-Multi-Domain-Command-and-Control-Experiments.aspx; Robert Brown and David Perkins, "Multi-Domain Battle: Tonight, Tomorrow, and the Future Fight," *War on the Rocks*, August 18, 2017, https://warontherocks.com/2017/08/multi-domain-battle-tonight-tomorrow-and-the-future-fight.

8 Joint Chiefs of Staff, *Doctrine for the Armed Forces of the United States*, JP 1 Joint Chiefs of Staff, 2017, I-9, https://fas.org/irp/doddir/dod/jp1.pdf.

9 Julian Stafford Corbett, *Principles of Maritime Strategy* (Mineola, NY: Dover Publishing, 2004), 164.

10 Department of Defense, *Dictionary of Military and Associated Terms*, Vol. 1–02, Washington, DC: Department of Defense, 2010, 16.

11 Albert Palazzo and David P. McLain II, "Multi-Domain Battle: A New Concept for Land Forces," *War on the Rocks*, September 15, 2016, https://warontherocks.com/2016/09/multi-domain-battle-a-new-concept-for-land-forces.

12 "Multi-Domain Battle Requires Non-Stovepipe Solutions, Say Leaders," *Benning News* (official news blog), US Army Maneuver Center, May 25, 2017, https://benningnews.org/2017/05/25/multi-domain-battle-requires-non-stovepipe-solutions-say-leaders.

13 Mark Pomerleau. "How Industry's Helping the US Air Force with Multi-Domain Command and Control," *Defense News*, September 25, 2017, http://www.defensenews.com/c2-comms/2017/09/25/industry-pitches-in-to-help-air-force-with-multi-domain-command-and-control.

14 Aretz, "Information Operations in a Multi-Domain Operations Battlespace"; Marcus Featherston, "Multi-Domain Command and Control (MDC2): Changing the Face of Modern Warfare," *Aerospace and Defense Technology*, February 1, 2018, https://www.aerodefensetech.com/component/content/article/adt/features/articles/28395.

15 Robert Barnett, "VCSAF Highlights Speed, Innovation as Keys to Victory in Future War," US Air Force, Secretary of the Air Force Public Affairs, April 10, 2018, http://www.af.mil/News/Article-Display/Article/1489186/vcsaf-highlights-speed-innovation-as-keys-to-victory-in-future-war.

About The Mitchell Institute

The Mitchell Institute educates the general public about aerospace power's contribution to America's global interests, informs policy and budget deliberations, and cultivates the next generation of thought leaders to exploit the advantages of operating in air, space, and cyberspace.

About the Forum

The Mitchell Forum series is produced and edited by Marc V. Schanz, Mitchell Institute's director of publications. Copies may be reproduced for personal use. Single copies may be downloaded from the Mitchell Institute's website. For more information, author guidelines, and submission inquiries, contact Mr. Schanz at mschanz@afa.org or at (703) 247-5837.

About the Author

Lt Col Cory S. Hollon, USAF, is a student in the Grand Strategy Seminar at the Air War College at Maxwell AFB, Alabama. Prior to his current position, he was an airpower strategist for the futures and concepts division of the Air Force Warfighting Integration Center at the Pentagon.

From June 2016 until June 2017, Hollon was the commander of the 332nd Expeditionary Operations Support Squadron at an undisclosed location in the Middle East. He has flown more than 1,000 combat hours in the F-15E and was an instructor pilot at Seymour Johnson AFB, North Carolina; Mountain Home AFB, Idaho; RAF Lakenheath, United Kingdom; and Nellis AFB, Nevada. He has deployed seven times in support of Operations Iraqi Freedom, Enduring Freedom, Noble Eagle, Freedom's Sentinel, Resolute Support, and Inherent Resolve. During his time at Seymour Johnson's 4th Fighter Wing, he was the operations officer of the squadron that won the 2015 Air Force Association's David C. Shilling award for most outstanding flying unit.

Hollon holds a Bachelor of Arts degree in speech communications and religious studies from Western Kentucky University. He earned his commission from Officer Training School, Maxwell AFB, Alabama, and completed undergraduate navigator training at Naval Air Station Pensacola, Florida. Hollon has graduated from the USAF Weapons School, Squadron Officer School, Air Command and Staff College, and the School for Advanced Military Studies. He can also be found on Twitter—@cory_hollon. Readers should be prepared for a lot of *Star Wars* references.

The views expressed are those of the author and do not necessarily reflect the official policy or position of the US Air Force or the Department of Defense.