REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
03/21/2019	Master's of Military Studies	SEP 2018 - APR 2019

4. TITLE AND SUBTITLE
In the beginning: The multi-domain Joint Force and the future of domain thinking

5a. CONTRACT NUMBER
N/A

5b. GRANT NUMBER
N/A

5c. PROGRAM ELEMENT NUMBER
N/A

6. AUTHOR(S)
Hertenstein, Geoffrey, FA, CPT, USA

5d. PROJECT NUMBER
N/A

5e. TASK NUMBER
N/A

5f. WORK UNIT NUMBER
N/A

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
USMC Command and Staff College
Marine Corps University
2076 South Street
Quantico, VA 22134-5068

8. PERFORMING ORGANIZATION REPORT NUMBER
N/A

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR'S ACRONYM(S)
MMS Mentor's Name

11. SPONSOR/MONITOR'S REPORT NUMBER(S)
N/A

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited.

13. SUPPLEMENTARY NOTES

14. ABSTRACT
For the concept of multi-domain operations to be successful, there needs to be a common language amongst the joint force, and the concept must not abandon single domain dominance at the expense of maneuvering through an existing domain or through creation of a new one. Not all problems need a rigid doctrine to overcome and multi-domain operations requires ambiguity in order to maximize its potential. To act otherwise risks rigidity in concept that frustrates the concept's utility.

15. SUBJECT TERMS
Multi-domain operations, multi-domain battle, domains, ambiguity

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			USMC Command and Staff College
					19b. TELEPHONE NUMBER *(Include area code)*
Unclass	Unclass	Unclass	UU	42	(703) 784-3330 (Admin Office)

United States Marine Corps
Command and Staff College
Marine Corps University
2076 South Street
Marine Corps Combat Development Command
Quantico, Virginia 22134-5068

MASTER OF MILITARY STUDIES

In the beginning: The multi-domain Joint Force and the future of domain thinking

SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR THE DEGREE OF
MASTER OF MILITARY STUDIES

CPT GEOFFREY HERTENSTEIN, USA

AY 2018-19

Mentor and Oral Defense Committee Member: MATTHEW FLYNN
Approved: _____
Date: 3/21/19

Oral Defense Committee Member: PAUL ARMSTRONG
Approved: _____
Date: 3/21/19

Table of Contents

Executive Summary

Title: In the beginning: The multi-domain Joint Force and the future of domain thinking

Author: CPT Geoffrey Hertenstein, United States Army

Thesis: For the concept of multi-domain operations to be successful, there needs to be a common language amongst the joint force, and the concept must not abandon single domain dominance at the expense of maneuvering through an existing domain or through creation of a new one. Not all problems need a rigid doctrine to overcome and multi-domain operations requires ambiguity in order to maximize its potential. To act otherwise risks rigidity in concept that frustrates the concept's utility.

Discussion: There has been recent momentum within the US Army and the Joint Force regarding implementing multi-domain solutions to overcome emerging strategic and tactical challenges. The overarching mechanism to address these challenges is to frame doctrine by which services acknowledge and provide cross-domain effects in support of one another. This endeavor has so far been met with challenges, as the Joint Force has definition challenges and must eventually acquiesce to developing capability that will support other services at the expense of their own capability in a zero sum resource environment. This task is challenging at best, unachievable at worst. Additionally, generating a solution inherently increases complexity associated with execution. However, significant doctrinal overhaul is not necessary and the beneficial effects of multi-domain cooperation are best manifested through inherent ambiguity.

Conclusion: A drastic doctrinal solution for multi-domain operations is both unachievable and thankfully unnecessary. Allowing for ambiguity in thought? provides opportunity by enabling services to maintain primary domain dominance which is necessary for multi-domain cooperation and then success across the domains. It also allows for solutions to be developed relevant to the specific situation, leveraging creativity without the risk of resource competition in a zero sum resource environment. Synchronization between services can be overcome through more focused and consistent language and through the use of existing infrastructure to implement change without significant turbulence, leaving the US military advantage intact and capable of ensuring continued US global projection of power.

DISCLAIMER

THE OPINIONS AND CONCLUSIONS EXPRESSED HEREIN ARE THOSE OF THE INDIVIDUAL STUDENT AUTHOR AND DO NOT NECESSARILY REPRESENT THE VIEWS OF EITHER THE MARINE CORPS COMMAND AND STAFF COLLEGE OR ANY OTHER GOVERNMENTAL AGENCY. REFERENCES TO THIS STUDY SHOULD INCLUDE THE FOREGOING STATEMENT.

Preface

Multi-domain operations is a developing military concept that has frustrated me due to the flexible use of the term defying definition. After researching its merits, this flexibility, more ambiguity, presents itself as the solution, and attempting to over codify its meaning and its execution brings up more questions than answers. By allowing creativity, accepting ambiguity paradoxically suggests that the concept becomes more clear as the detail is scaled back, as one might expect when taking a broader view of an issue. In this case, over complication is a result of over prescription. That being said, I am not a pessimist, and I am excited for the potential combat power enabled by a synchronized joint force.

I would like to thank everyone who supported me during this project: my wife Krystal for her patience and for enduring unsolicited discussions about the merits of domains and domain thinking, Dr. Flynn my advisor for weathering the sometimes constant email exchange, particularly about God, the meaning of life, and Napoleon, and for the staff at the USMC Command and Staff College for the work put into an exceptional Professional Military Education program. I am blessed to have the opportunity to attend this course and to represent the US Army as a student.

INTRODUCTION

For the concept of multi-domain US military operations to be successful, there needs to be a common language amongst the joint force, and the concept must not abandon single domain dominance. The concepts that multi-domain operations are rooted in are well-documented; the indirect approach, seeking vulnerability, and operating in ambiguity. The concept at its core is not flawed, but flawed domain thinking on its periphery can lead to imprecise implementation and eventually exhaustive analysis that is of limited value. If the evolution of warfighting concepts is to simply expand the scope of the battlespace, domain analysis dilutes practical application in proportion to the expansion and further defocuses the much sought military innovation that will set up the United States and our allies for success in the "next war." Not all problems need a rigid doctrine to overcome, and multi-domain operations requires ambiguity in order to maximize its potential; the converse risks rigidity in concept that frustrates the concept's potential. When this calibration is made, the US military can look forward to ensuring a continued ability to advance US national security interests.

Thinking about domains for military professionals went from merely registering the reality of fighting on land, sea, and air, and at times in space, to a necessity of weighing all possible points of contact at once. Arguably, the passing of time has added more domains and therefore more complexity to visualizing warfighting in the near term and long term. How far thinking about domains and their intersection takes us is the key issue. Services explore joint solutions to problems in their primary domains, while the US Army seeks to evolve existing structure to fully multi-domain formations which are able to engage across all domains at echelon independent of the joint force. Domain thinking requires creative solutions to problems, but codifying lock-step solutions either in the joint community or within individual services

stovepipes solutions and places single domain dominance at risk while enabling effects reduncancy. That relationship threatens to undo the very sought-after gain from multi-domain integration. So, while that thinking must be addressed, there must be an accepted lack of resolution when assessing all of the domains at once. This lack of clarity will better serve the US military going forward to win the next war than any assumed and erroneously declared harmony across all domains. As is always the case, a flexibility of thinking and action will enable victory in the coming war more so than any proclaimed doctrine promising success but more likely limiting adaptivity in time of crisis. A conceptual baseline and language across the joint community is better than a rigid solution.

A few examples can illustrate this need and intention. If a nuclear missile is launched from a submarine at a land target, traveling through air and space, assumedly guided by some network enabled software or hardware, the whole mission has now encompassed all five of the current recognized domains – land, sea, air, space, cyber.[1] It also transcends a possibly infinite number of yet to be discovered domains. As humans have created the cyber domain, the creation of new domains is theoretically limitless, and a missile moves through them without our discovery or definition. Regardless of the number of domains, the result is the same: a nuclear explosion on the receiving end and no one more the wiser of the inter-domain path it took to get there.

Nuclear attack is a dramatic illustration, but the point remains: multi-domain operations have become a selectively malleable concept, that through attempting to narrow a focus has convoluted it into a catch-all elastic clause. Recent conceptualization describes a system and seeks to analyze an ever increasingly complex network of interrelated possibility, finding gaps that may create maneuver opportunity across existing domains or what humans may yet create.[2]

Effects take the form of what is there and what cannot be seen, understanding that assets get stripped off of the battlefield beyond tangible awareness, be it from a supersonic missile at ever increasing range, a bomb from an aircraft far from sight, a cyber incursion that drops "the network." As possibilities of what can be seen or not, what exists and is undiscovered, or what may be invented and leveraged are endless, resources and time are not. The Joint Force, not guided by common language, risks extending itself to infinity in search of possibility, and is unable to adequately compete asymmetrically, ceding overmatch across old domains while in search of new ones.

This problem with optimizing jointness inherent to multidomain operations is not new. Looking back to before the nuclear age, World War II offers some key insight into thinking about domains. Control of multiple domains was the decisive factor in the American victory over Japanese forces at Guadalcanal, an eight-month campaign that helped turn the tide of war in the Pacific. The Americans made multi-domain operations work by fusing joint capability together to overcome asymmetry in a single domain, notably sea.[3] However, each service fought for control within their primary domain first before affecting other domains. Multi-domain cooperation focused on maintaining the sea and air lines of communication to sustain the land fight, supported by primary domain dominance by the land, air, and sea components, were crucial to American success.[4] Losing in one domain would have spelled doom for another, particularly for the 1st Marine Division, ashore and dependent on the interservice partners to deliver much needed war fighting men and material.

Without a responsible party for each domain, the joint force is vulnerable. Guadalcanal illustrates this as does the Pacific theater as a whole. During the struggle over Guadalcanal, the Marines ran the land fight, the Navy ran the sea, and the air component supported both via

aircraft carriers and the Cactus Air Force out of the famed Henderson Field. The Marine Division ashore was not concerned with how they could support the Navy's fight, but was concerned with surviving hostile naval bombardment and maintaining an open sea line of communication. The Navy was not worried about the land campaign beyond providing supplies, and though able to occasionally support with naval gunfire, the sum of the efforts to the land campaign was minimal. General Vandegrift, in command of 1st Marine Division, and the series of Navy commanders during the campaign, had relatively equal and opposite forces working against them. The real "multi-domain" opportunity came because of the distance and early warning interior lines for the Cactus Air Force, which allowed it to have its effects within a defensive bubble around Guadalcanal. If senior American leadership in the Pacific had decided to attack Rabaul before deciding on the Guadalcanal landing, it may have gone the opposite direction ending in catastrophe given the ability of the Japanese to benefit from ground air in the midst of a struggle to control the sea. The risk in multi-domain thinking comes in the hypothetical scenario that the Marines could somehow support the Navy with shore-based artillery or other assets. This pulls forces in the tactical sense and funding in the strategic sense away from generating parity and overmatch within the services or component's parent domain that was crucial to success. The effects would have benefited the force as a whole, but force capability and capacity is zero sum. To provide a cross-domain effect comes at the expense of something else within a service, thus rigid dictation of capability may come at the expense of a creative solution that balances requirements in a primary domain and across domains.

This theory is present today in multi-domain operations conversations. Winning in service or component parent domains first is crucial. Much can be said of the heroic contributions of the Cactus Air Force and its multi domain effects throughout the campaign.

However, those effects were limited by distance, weather, and plane availability. One prominent author covering the campaign, James Hornfischer, suggests that the Navy had to win at sea at the second battle of Savo island and in other cases before the joint force could be fully employed together, and had to do it on its own because of the limited availability of the Cactus Air Force.[5] Vandegrift had to hold off significant night assaults at Tenaru and Edson's ridge without the help of air power for the same reasons.[6] The professed gaps and maneuver space consistent with multi-domain thinking today may not be there unless forces do what they are designed to do: win in their respective domains first. The capability to exploit enemy gaps is a distinct advantage that is captured in multi-domain thinking. However, the essence of successful multi-domain cooperation is to not only provide effects into other domains, but also not to become a burden to those respective component commands. The first and most important cross-domain effect that a component must achieve is to not lose and thus create a gap in its own domain that could be exploited by the enemy.

To act otherwise draws time and resources away from the ability of a force to maintain positive asymmetry. In this instance, if Edson's ridge had fallen when that small unit faced the second major Japanese offensive on the island, or if the Navy had been unable to score crucial victories when facing key elements of the Japanese fleet, the aggregate joint force combat power is impotent in the region with obvious negative consequences for the US defense of the island. Mutual support starts with domain dominance; conversely, a failure in a domain invites a mutual vulnerability across all domains. The true challenge of multi-domain operations is not ceding capability, or at a minimum symmetry which an enemy cannot bypass, while attempting to seek advantage from operating in another domain. The key to success in multi-domain cooperation is

to protect the other domains through single domain dominance, thereby enabling cross-domain maneuver and effects.

More context can be found in cultural analysis at least ostensibly divorced from a warzone. The Judeo-Christian influence on Western perceptions of order is evident, impacting the military's division of the world into compartmentalized war fighting environments.[7] The point of departure of existence mirrors that of war, war is simply that; a shapeless struggle like the faceless voice in the void. That space was all encompassing and dark, until God created light and with it the dichotomy that pits us against them, or a perception of good against evil, thus generating a moral imperative for victory and an imperative to pursue different methods of achieving it. Order out of chaos, understanding out of the fog of war, this was the first step.

Domains take shape as God distinguishes heaven from the void, the first step in separating and characterizing divisions of reality, whereby actions in one may influence results in another. The fall of man, this departure also indicates a divorce from utopia, where on Earth the struggle for peace is unattainable, and thus the nature of current perceptions of war are a constant and enduring act. There is no perfect solution in one domain or across many. The search for the perfect opportunity, the ideal synchronization of capability comes up short and serves primarily to distract humanity from both its sin and its redemption. This was the second step, domains marking the progression toward the end of utopia, its impossibility but for the divine creator providing a path to eternal salvation. God was both purveyor of unholy domain integration and its ability to perform this very sacred act – if one could get to perfection. Since humanity could not enjoy that state of being, domains remained both a God-send and curse.

The struggle over imperfection continues. The land and the sea appear simultaneously, though God first names the land, followed by the sea, so the first two domains. Having already

been split from heaven, the air necessarily followed. Within this, God orders the earth to produce seed, and with it the first forms of life. Though the sea and air also exist, the essential component of our understanding is the ground, whereby all effects are most important, where the seeds are grown. This was the third step, a ranking of domains but also clear distinctions among them.

The act of creation continued with the light in the sky, both during day and during night, another gift of binary existence suggesting a need to find harmony as a measure of time. Thus both day and night are inevitable. God places the sun and the moon to correspond to day and night, and the stars to guide the seasons and give purpose to the rigid divide of light and dark. The celestial reminders of light in darkness suggest an enduring existence of advantage despite the night. Darkness is never fully realized if one knows where to look. Not only does God's fourth step parallel the discovery of the fourth domain, it also reflects on an enduring overhead presence of good, much as a satellite provides navigation and communications, or presents the possibility of persistent observance from space. This was the fourth step, space as a measure beyond air but still short of heaven, where influence can be projected but decisiveness is yet to be achieved.

The fifth day showed the creation of living beings on the land, sea, and those same beings trafficking air, introduces interconnectedness and networks that transcend traditional domains. Not all creatures feed on creatures within their domain; birds eat fish, mammals eat birds, and the cycle continues. This network, much like a cyber network, is global in reach, weaving between domains, seemingly unaffected by the characteristics of that domain but understanding a need to feed on such domains where possible.

Much as humanity must wrestle with the interaction of domains now, so too was the case with the sixth step. Continuing with the analogy, God creates man on the sixth day, the most

complex creature entrusted with care over the networks that effortlessly interface through the land, the sea, and the air. Confusion breeds attempted unity, a task bound to remain unclear in purpose and effect. Moreover, greater complexity presents opportunity, not inherent resolution, an idea only possible after the fall from grace in Eden.[8] Paradoxically, with the fall from grace, perfection became impossible and with it the full potential of opportunity. The blessing of ambiguity, manifested in free-will, is the only mechanism to overcome complexity interwoven with light and dark. Choice is the route which may realize salvation.[9]

It is unknown what the next domain will be, but the comparison of the creation story and the mandated domains of today suggests that that discovery awaits and the span of domains will again increase, exposing the need to somehow leverage the physical elements within the previously existing domains. An important reminder is man is an imperfect image of God, suggesting that the militarization of and the conflict within the next domain is inevitable. Absolute harmony is reserved for the divine, and is thus not achievable causing conflict. Benevolence was always a soul-searching gift much as the need to seek cross-domain integration to secure military advantage. The realization of benevolence comes from choice inherent in existence. Expecting perfection is dangerous and evil, with those seeking it challenged God and were cast out of Heaven.[10] However, pursuing harmony represented by God and His creation best positions imperfect humanity for salvation. Humans cannot expect to create as God has, but must understand the harmony within his creation; the interaction of domains, of light and dark, and the ability to choose a path within that design.

Assessing the Judeo-Christian influence on today's domain thinking in terms of military analysis is not intended to reaffirm humanity's place as divine, but rather to illustrate that the fundamental beliefs that have shaped Western thought continue to subconsciously influence

perception of domains. Should that seemingly inevitable link be a comfort of eternal life, so much the better. However, the more practical end of accepting that the discovery and militarization of domains tend to parallel the creation story is that the capability within a domain mimics the characteristics of God's design, and keeping with the analogy, that view comes up short. At the end of creation, the world is the world as it is, with increasing complexity. Without the God-created building blocks of land, sea, and air, the greater complexities cease to matter as the conditions for their existence are not there. In this way, cross domain conflict fails if the complexities of space or cyber do not have a tangible effect on the land, sea, or air, all of which have proven to shape outcome by force before the understanding and leveraging of the two newest domains. We are not God, and therefore inherently imperfect. Mastery of what has been placed in front of us is possible, but artificial creation of a new domain of decisive military utility is questionable at best.

Multi-domain operations: Is it new and does it matter?

Saluting the possibility of cross domain success and acknowledging how this success does not compromise single domain dominance leads one to weigh that relationship today. Duplicating that success clearly has merit, if one can get there. Given the need to consider more domains once adding space and cyberspace to the measure of domain dominance, makes this effort not only necessary but challenging.

Growing competitor capability, particularly robust Anti-Access and Area-Denial (A2AD) capability, face US forces, challenges which have been absent in US and allied combat operations over the past twenty years or more.[11] Specifically, US policy considers China and Russia top competitors whose A2AD capability must be overcome for successful military operations.[12] This capability contests the joint force in all domains, a deviation from previous

doctrinal thinking where authors of multi-domain operations suggest that America has enjoyed supremacy in the recent past.[13] Additionally, cyber capability has expanded the range and scale of potential military effects to virtually anywhere there is an internet connection, thus redefining the physical scope of what is to be considered the modern battlefield.[14] This expansion simultaneously compresses accepted understandings of the tactical, operational, and strategic levels of war, whereby a tactical action is espoused to more likely have a strategic impact, even at the lowest level, and strategic decisions and systems are able to influence directly a tactical action.[15] Other factors such as urbanization, littoralization, and resource scarcity, add to the complexity of the potential battlefield and create scenarios unfavorable for US military operations. These emerging trends risk tactical and strategic failure if not properly prepared for.[16]

The Army has proposed a three tenet solution to conducting multi-domain operations and thus overcoming the A2AD challenge and preparing forces for the complex future environment: maintain a calibrated force posture, develop and implement multi-domain formations, and premise operations on convergence.[17] The goal is to have the correct formations with sufficient capability and authority in the right place to compete in peace, set conditions for war if necessary, and conduct combat operations in a crisis or open conflict. Important to the concept is that it transcends peace and war, attempting to counter ongoing adversary military operations that amount to something less than war in addition to preparing for fighting in the traditional sense of the use of kinetic force on force. While the enemy becomes more capable and the operating environment more challenging, both friendly and enemy forces find themselves with a mix of capabilities at their disposal. This mix is the center of multi-domain battle, whereby forces attempt to outmaneuver one another through advantages gained by asymmetry within one

or more domains, potentially with limited time windows, capitalizing on vulnerabilities within denied areas.[18]

The concept has drawn criticism as being unoriginal, drawing much of its core concept from previous doctrine such as AirLand Battle, Army After Next, Capstone Concept for Joint Operations, the Army Operating Concept (2014), and the Marine Corps Operating Concept.[19] Arguably, the multi-domain operations concept does share notable similarities in principle with AirLand Battle of the 1980s. Concepts such as maneuver and combined arms effects to overcome a numerically superior enemy operating in one domain speak to both theories. AirLand battle sought superior position, exploiting weakness to gain temporary advantage through maneuver while the Air Force provided attrition to deep forces supported by joint suppression of enemy air defense (SEAD) from surface-based field artillery. Multi-domain operations seek superior positioning through maneuvering through different domains, exploiting vulnerability at a point of weakness across a spectrum of physical and constructed possibility.[20] AirLand Battle doctrine conceded that victory can come in one domain, land, but integration across the land and air domains was necessary to overcome a superior Soviet ground forces.

By recognizing the land combat power disparity, the Army acknowledged that defeat can come at the hands of a single domain force, but convergence can overcome the disparity. This insight has two important foundational implications for multi-domain battle. First, it is clear that multi-domain thinking is indeed not new. The theory is old, but the scope is new. The discussion today is a reaffirmation of the interdependence of the joint force at scale.[21] Second, the new thinking undermines the conceptualization of the joint force being unconcerned with contested operations that have allegedly been ignored, as suggested by proponents of multi-domain operations that attempt to portray the new concept as different from previous doctrine.[22] The

interdependence of effects such as joint SEAD and deep air to ground attack acknowledge that both forces are threatened within their own domains. Enjoying domain supremacy during extended counter-insurgency operations in Iraq and Afghanistan does not mean that contests in air and sea domains were ignored.

Although US forces have not been significantly challenged since the end of the Cold War,[23] doctrine still exists that accounts for cross-domain solutions to problems, acknowledging that doctrinal thinkers have not abandoned the idea of clashes across all domains. For example, Operation Desert Storm was largely inspired by AirLand Battle doctrine.[24] Additionally, with land forces heavily involved in counter insurgency in Afghanistan, the Air Force and Navy developed AirSea battle, whereby the services sought to combat parity in the sea and air domains by establishing a multi-service doctrine where Air Force and Navy assets were mutually supporting.[25] This mutually supporting doctrine sought to address many issues such as the A2AD challenge that multi-domain operations engage, acknowledging that both the air and sea domain proponents recognized that their domains were in fact contested despite the main effort being counterinsurgency. A lack of parity on recent battlefields does not mean that the joint force assumed supremacy as its core thinking. The premise of establishing a multi-domain doctrine is then inherently flawed. Services have always been aware of cross-domain threats and have a precedent of seeking multi-domain cooperation in order to overcome them without requiring a wholescale joint force intervention. The fact that multi-domain cooperation was occurring to overcome contested domains during long duration counter-insurgency operations suggests that the joint force never fully accepts the luxury of domain supremacy.

A theme underlying multi-domain operations is ambiguity. Ambiguity is characteristic of the changing battlefield, always present but perhaps more so now than in the past. Hybrid

warfare, population growth, the internet, and mega-cities all present new far reaching challenges to the joint force in potential combat operations by increasing complexity, premising multi-domain operations as a concept.[26] However, accepting ambiguity as inevitable in combat is not a new concept to the military. The Marine Corps describes ambiguity as "acting in such a way that the enemy does not know what to expect.[27]" In one of its capstone doctrine publications, *Operations,* the Army discusses the use of mission command as a means to overcome uncertainty and ambiguity.[28] In the case of ambiguity, the Marine Corps and the Army both see ambiguity as a risk and an opportunity. Those able to best accept it and leverage it have an advantage in an increasingly complex operating environment. The challenge with ambiguity within the military is that there is arguably a culture that does not facilitate leveraging it as an advantage. The dichotomy of professed mission command on the battlefield and an increasingly bureaucratic garrison system institutionally stifles the military's ability to deal with uncertainty and be proficient in an ambiguous environment, whereby leaders err on the side of caution and are less apt to make decisions.[29] This culture denies ambiguity and directly contrasts with the professed foundational tenets of multi-domain operations. Accepting doctrine as a common point of departure for operations and not as a lock step solution to a problem is critical to successfully leveraging ambiguity and managing uncertainty.

Stephen Frühling analyzes difficulty in overcoming uncertainty in strategy through a framework that intersects sources of uncertainty with uncertainty in the theory of victory.[30] Revolutions in military affairs (RMAs) are described by Frühling as a factor of uncertainty which can render obsolete one or more core competencies of an opponent, or generate new core competencies.[31] Core competencies are foundational to the way a military conducts war, and Frühling specifically cites combined arms warfare as an example.[32] As is, multi-domain

operations is admittedly an extension of combined arms operations, influencing operations in one domain with effects from others while adding complexity to the core competency.[33] Injecting complexity into a core competency is self-inflicted uncertainty, not an RMA as defined by Frühling, adding uncertainty while not addressing uncertainty through progress.

The good news for the joint force regarding multi-domain operations is that the disruptive effects of complexity should not be significantly detrimental, as the concepts are not new. The bad news is that increasing desynchronization and potential over-prescription of a core competency institutionally sidelines warfighters' ability to manage ambiguity that may already be a source of strength. Seeking to order complexity is important, particularly when leveraging the collective effects of the US Joint Force, making domains a useful framework. However, balancing ordering principles with conceptual impact while taking care to understand the doctrinal relationships to core competencies may be the difference between over prescription and creative liberty to leverage ambiguity.

Whether or not the concept is new matters in acknowledging the evolution of the modern battlefield. Just as multi-domain operations may not be revolutionary, the current and future operating environments are not the result of a sudden and figurative "Big Bang" either. This need to identify a new break in norms cages doctrinal thinking. Already cyber impacts are being compared to the previous impacts of air on other wars and battlefields.[34] The doctrinal trend is to seek ways around the enemy through different domains, which in theory may or may not already exist or have been discovered, but may now operate with different physical rules. Ultimately, that solution is possible as mainly an incomplete one.

Definition Challenges

A chief issue with multi-domain operations doctrine is that there is no clear consensus defining what it actually is. The joint force has piece-meal committed to an imperative of cross-service and cross-domain support within acquisition efforts while the US Army seeks autonomous multi-domain formations independent of the joint force. This discrepancy has seen historical challenges with joint force coordination, while the Army's efforts risk reduncancy within the joint construct. Until the joint force can establish a common vision for multi-domain operations, its implementation will at best be non-complementary across services, and at worst will be counter-productive. Though common vision may not ever be fully realized, common language can begin to facilitate understanding and ease concerns over integration concerns across the Joint Force.

A key starting point for definition challenges is JP 1-02, which lacks a definition of what constitutes a domain, though it has independent descriptions for the air, land, sea, cyber, and space domains.[35] To get this clarity, one can turn to William Dries, a retired Air Force pilot and civilian consultant to the Army and Marine Corps on multi-domain operations, who describes a domain as a "region distinctively marked by some physical or virtual features."[36] Domains have different rules, advantages, and limitations that must be negotiated in order to conduct operations within them.[37] By this definition, physical limitations such as gravity and terrain are things that cannot be changed, and are natural to the planet. However, virtual features, such as those characteristic of the cyber realm, are human made, and therefore can be defined in whatever image a creator may shape them. Though seemingly of little consequence, this difference between natural and manmade characteristics leaves everything available for discussion into establishment as a domain, which defocuses the concept.

A further illustration of the implications of manmade domains are found in US Army publications. The US Army's TRADOC Pamphlet 525-3-1 from December 2018, informed previously by the 2017 TRADOC White Paper titled "Multi-domain battle: Evolution of combined arms for the 21st Century, 2025-2040," describes the five domains as land, sea, air, space, and cyber. What is most interesting about the more recent document is that it describes conflict across all domains, and includes the electromagnetic spectrum and the information environment in addition to the regular five.[38] Coming short of overtly defining the electromagnetic spectrum and the information environment as domains, this view suggests the existence of seven domains, or at least two separate entities deserving the same attention as the five currently recognized. This deviation further speaks to the infinite nature of domains which is currently circulating through doctrine and professional literature. If each service can define domains or equivalent effects however it chooses as the Army has done, the joint effort is inherently undermined, frustrating implementation of mutually supporting effects. Differing views of multi-domain operations are already emerging across the joint force; defining other concepts such as the electromagnetic spectrum and information operations in the same structure as domains at the Army service level highlights a lack of synchronization.

Multi-domain operations and domain thinking are gaining interservice traction, though different services have different views of how the concept materializes. Both the Army and Marine Corps have emphasized multi-domain operations enabling joint and service maneuver. The Navy is committed to exploring how land forces can project power into the sea. The Air Force welcomes multi-domain operations and see them as no departure from how it has always conducted itself, but has introduced the idea of primary domains that need to be mastered in conjunction with coordinating for cross-domain effects with other formations or services.[39]

Admiral Harry Harris, former INDOPACOM commander, presented the case that land forces need to develop capability to influence the sea domains such as land based fires that could attack naval targets, as well as foster further air defense capability.[40] Additionally, General Robert Brown, the ARFORPAC commander, has presented similar concepts, emphasizing the interdependency of joint force capability to project mutually supporting effects into different domains.[41] INDOPACOM's interest in mutually supporting effects is evident from the nature of the operating environment. Operating across mostly water, and encompassing China's anti-access area denial (A2AD) system, it is reasonable to request all available assets to support the maritime effort.[42] However, this does not speak to why different services need to maintain cross domain effects, nor how the projects will be funded. Joint interoperability may exhaust itself at the hands of competitive budgets, which are focused on primary domain domination within the respective services. Because of the inherent resource competition and unclear joint guidance, even in its infancy, multi-domain operations also find drastically different definitions and application elsewhere across the services that seek to independently maximize effects within the new framework.

Most notably different from other services is the US Army's vision. General Perkins, the former Army TRADOC commander and one of the strongest voices for the implementation of multi-domain battle, describes multiple concepts. Besides designing forces and capability to provide cross-domain fires, the Army must reorganize into multi-domain task forces and formations, develop individual soldier lethality, and improve upon existing equipment and mission command systems.[43] This departs from the joint perspective because it describes multi-domain operations in both a cross-domain context as well as an improvement to existing Army systems that operate in a multi-domain dynamic independent of the joint force. This thinking

layers meaning onto the concept, convoluting clear understanding of what multi-domain operations actually encompass.

This convolution is evident given the differing opinions within the Army and professional military literature regarding what a multi-domain force is and what it is responsible for. TRADOC PAM 525-3-1 describes multi-domain formations in a broad sense. Formations at all echelons are multi-domain capable and provide converging effects for the Joint Force Commander.[44] The lowest echelon where multi-domain capability terminates is not overtly described throughout the document.[45] Similarly, the concept of convergence of capability seems at odds with the concept of the all encompassing multi-domain formation. At some level, a multi-domain force is inherently the convergence of multi-domain capability. It is unclear if the goal is the convergence of multiple multi-domain formations, the inherent convergence of multi-domain capability within any formation, or the eventual convergence of joint fires.[46] Converging joint or theater level assets does not seem to suggest that a formation is inclusively multi-domain, rather it is just seeking external support for requirements that may develop to secure the initiative on the battlefield.

Despite the document outlining conceptual responsibilities from the theater to the brigade level, the extent of multi-domain capability at echelon is not clear due to acknowledgement that higher echelons are needed to coordinate various effects.[47] Multi-domain capability for the sake of potential autonomous operations requirements should dictate that at all echelons the capability would need to be the same, maintaining capability until the formation can be reformed at echelon without a degradation of multi-domain options for the commander. By dictating tasks at echelon, the concept appears a little departure from current operations.

Professional Army literature has revealed other ideas of multi-domain formations and multi-domain operations, further broadening the definition and understanding. Concepts include functionally aligned divisions that can manage different areas of the battlefield,[48] and bolstering multi-domain capability in the cavalry and reconnaissance formations in order to enable high speed reconnaissance and maneuver.[49] This literature expands the scope, including in multi-domain formations special operations forces, engineers, and joint-fires capability, and tailored subordinate brigades and battalions able to execute specific tasks associated with their prescribed mission set.[50] This complexity is an important deviation from the Army understanding, as it dictates functionality beyond the domains, adding a dimension to the concept. Also, it focuses solely on the Army's ability to operate within multiple domains, not the Army's contribution to the joint force; valid considerations, but a departure from the joint understanding of the Army's contribution. The Army's initiative for independent multi-domain capability is redundant of a truly integrated joint force.[51]

The impact of the various multi-domain understandings is frustrated implementation across the joint force. Traditionally effects projection and protection efforts have been maintained in the services, focusing on the service's primary domain. Acknowledging that cross-domain solutions may speed action and increase the overall lethality of the mutually supporting joint force, each service's vision of multi-domain operations tend to predictably favor the joint force's contribution to operations within the respective service's primary domains.[52] This is both beneficial and challenging. Services are rightly concerned about maintaining dominance in their primary domains as a contribution to the joint force. However, resources are zero sum, creating a decision point by which services may potentially sacrifice single domain effects in favor of multi-domain coordination. This is facilitated by cross-service discussions to improve

understanding, but the problem has been acknowledged by senior service-members within at least the Army and the Air Force.[53] Other initial coordination has been made between the Army and the Marine Corps, both services co-authoring the original multi-domain operations white paper.[54] Conspicuously absent from the initial conceptualization is the Navy, until recently.[55] The Navy's relationship with the Marine Corps, which can project power across multiple domains, potentially dilutes the novelty of the concept to the service, while the Marine Corps' inherent multi-domain mindset potentially accounts for the enthusiasm. In this sense, one could say the Navy already has multi-domain thinking accounted for.

Further, the multi-domain operating environment inherently involves complex interdependence not only amongst the joint force, but also amongst coalition partners and allies.[56] This magnifies the impact of both theater focus and language. Partners in Europe potentially facing Russia have different capability than partners in the Pacific potentially facing China. Also, if the joint force has difficulty defining and agreeing on what multi-domain operations are, partners and allies that do not share a common language and have varying requirements significantly complicate matters.

Regardless, there is no joint authority dictating the concept and thus directing implementation, which can continue to dull the synergy of the concept adding skepticism to the initial coordination and implementation discussions. Multi-domain operations face the challenge that the concept is focused on domains, not an adversary. Nor does the idea own a four star general officer in charge of concept development and experimentation, all the while having to overcome cultural differences between services so as to benefit the joint force.[57] After implementing AirLand Battle, the Army and the Air Force initially enjoyed a mutually supporting doctrine, followed by a divergence of cooperation as both forces gained capability

that transcended the need for multi-service integration.[58] The Army has made it clear that its organic multi-domain capability needs to be grown in order to meet future challenges and contribute to the joint force. The paradox of increasing service capability and joint force integration is at play in multi-domain operations. If a service strives for less capability, it risks facing overmatch or of having a critical gap. However, if it strives for more capability, the inherent joint cooperation and integration that is at the center of multi-domain operations is at risk, as ever more independent services depart the joint effort at the first signs of inter-service friction.

Does it fit the problem(s)?

Multi-domain operations attempt to solve a variety of problems for the joint force and for individual services. Magnifying the challenges exposed in defining the concept, operationally it faces challenges of focus, scale, and scope. Presented as a turn-key operating concept at all echelons across all domains, multi-domain operations requires refinement based on a variety of technical and tactical problems. It also brings into question theoretical conceptions of how cross-domain effects interact.

First, multi-domain operations attempts to present a turn-key solution to multiple problems which are in reality very different, challenging the focus. Despite the acknowledgement that China and Russia are both threats and therefore the target of multi-domain operations due to having similar A2AD strategy,[59] the two countries and problems are not the same and should not be treated as such. Clarity starts with specificity, and doctrine should solve a specific problem. The coordination involved in AirLand Battle was successful because the Army and Air Force had a specific enemy in a specific place, and agreed upon specific

technical and tactical requirements for each other to address in mutual support.[60] This becomes challenging today, as potential adversaries vary in scale and scope.

Not only are Russia and China in two different theaters, but the service focuses are different. The Marine Corps and Navy are acutely focused on China, while the Army is arguably focused more on Russia and Europe, with different focuses in the Pacific such as North Korea.[61] Not only are the threats and geography different requiring specific solutions to each, but the interservice support is different offering yet another dimension of complexity to the situation.[62] Doctrine and operating concepts do not substitute for strategy. The assertion that Russia and China are similar enough to conceptualize an all-encompassing solution is one-dimensional and fails when digging deeper beyond threat force strategy. Presumably this disparity becomes worse as China manufactures more of its own defensive equipment, requiring increasingly different technological responses than what is required to counter Russian forces and equipment.[63] Multi-domain operations correctly hedges this problem by discussing calibrated force posture.[64] However, the joint force and the Army in particular should be wary of conceptually applying solutions from one adversary to the other as the concept continues to take shape.

Second, multi-domain operations at echelon present mission command and integration challenges that can undermine convergence. Integrating required multi-domain and combined arms effects requires significant staff effort. Manning issues, particularly at the tactical level, has notable impacts to multi-domain planning and execution, as the smaller staffs have limited bandwidth to adequately address integrated effects.[65] This challenge is magnified when attempting to integrate the kinetic and non-kinetic environment, as the data required to successfully understand and integrate multi-domain effects overwhelms staffs that are limited by both resources and time.[66] Developing an adequate multi-domain plan and executing it requires

expanded command and control capability that grows in proportion to the expectation of cross-domain effects. AirLand Battle acknowledged this and described corps as the level at which joint integration can best happen. It further delineated that battalions can take ground but do not have the organic ability to integrate joint fires for more than small durations and for mainly force protection type actions.[67] This is somewhat consistent with the Army's vision, describing corps as the formation that converges large amounts of joint fires.[68] However, the Army has also described the requirement for all formations to be multi-domain capable. The lower the echelon, the less capable it is to converge effects.

Integrating a Marine Air Ground Task Force (MAGTF) into a Joint Task Force provides insight into challenges of multi-domain formations at different echelons. The MAGTF is a inherently multi-domain formation, incorporating ground and air assets. The formation's integrity is of particular value to the Marines and to its overall effectiveness, which is at risk when the MAGTF is subordinate to another multi-domain task force such as a Joint Task Force. The MAGTF can operate effectively independently, but the sum of its parts can become a part of the larger force, and have significant effects across the broader battlefield.[69]

Similar to how the MAGTF risks its disaggregation to prevent reduncancy of effort and to unify joint effects, a multi-domain formation with organic cyber or space capability experiences the potential of being incorporated into the next higher multi-domain formation. The Marines through a series of agreements have codified resource commitment to a higher multi-domain formation, whereby the higher headquarters gets priority tasking of MAGTF assets for specific missions, and anything not tasked to directly support the MAGTF becomes available for the higher joint force commander.[70] This decreases the amount of idle assets that could support

the wider joint force, while ensuring that the MAGTF composition is sufficient to achieve its objectives.

Third, operating in all domains may be impossible for most formations, particularly in the cyber and space domains. Army cyber teams are being integrated at brigade and lower echelons at training exercises, providing network defense, while disrupting enemy mission command and communications, and disabling enemy social media networks used for propaganda distribution.[71] It is difficult to understand the requirement that cyber is executed from the front lines. To truly disrupt networked systems, cyber effects must overcome significant technical sophistication or other security measures that are within that country's digital terrain.[72] The complication of accessing highly secured networks that a sufficiently sophisticated adversary relies on to manage a portion of its military is hard enough from an office even for the best hackers,[73] and is surely more difficult under fire. If the internet is available from anywhere there is a computer and a connection, and physical proximity has nothing to do with the ability to find a specific network to have an effect, including offensive cyber capability in a forward multi-domain formation has minimal potential impact. Requesting cyber at lower echelons for the sake of multi-domain capability demonstrates a lack of understanding of the cyber domain and exposes the network to greater risk. Proximity access can be achieved by accessing a shared wireless of Bluetooth network, but this risks retaliation across the same access method.[74] Any offensive cyber operation can have an equal and opposite effect that should be considered carefully in formations that are heavily reliant on networked command and control[75] that is consequently vulnerable to cyber-attack.

The benefits of operating in domains beyond land, sea, and air are force multipliers, but also come with risks. A force chooses to be vulnerable by operating within these domains and

must weigh the cost benefit as they develop. Many tactical capabilities come from space, via satellites communicating with ground stations through cyber links.[76] While land, sea, and air communications and navigation have benefited greatly across the joint force due to the space and cyber domain, that connectivity has also presented a critically vulnerable reliance in a domain which did not have to be occupied. By creating and choosing the cyber domain by which to manage joint force operations, operations are intentionally placed at risk. The benefit can outweigh the risk, but it does not change the fact that in human created domains, humans have a choice to operate within them or not. This is different from land, sea, and air, as effects can physically cross between them. If a force is not on a cyber network, it cannot be affected by the cyber domain. Admittedly being forced off of the cyber domain is an effect itself. However, if the risk ever becomes greater than the benefit, theoretically a force can unplug and no longer be subject to the first order effects that concerned it.

Theoretical understanding of domains and cross-domain effects are currently questionable. Central to domain thinking is the concept of symmetry and asymmetry. The dawn of man and the dichotomy of good and evil necessitating choice allows for endless permutation and interaction. It is here that domain thinking develops, with limitless definition, attempting to invent reality or codify interactions that benefit one over another. When analyzing domains in the context of surfaces and gaps, inventing a gap is not the same as leveraging an existing one.[77] Participation in a manmade domain is voluntary. Asymmetry on land, sea, or air yields a clear advantage or disadvantage, and can equal victory or defeat. Asymmetry can be augmented by capability in the same domain or potentially from an effect from another domain. Cyber and space both provide capability, but the sum of the impact can still come up short of the aggregate firepower of the enemy. Moreover, if the enemy should choose not to be in the cyber domain and

still has greater overall combat power, cyber has proven to be indecisive, and the enemy is not vulnerable to attack within it. This illustrates the weakness of human creation within a cultural context. By leaving open the definition of domains, and using domains as a means of locating theoretical surfaces and gaps, we create an illusion that a vulnerability can be generated from human invention. Capability facilitates overmatch, not the advent of a decisive fighting environment.

Domain thinking risks becoming regressive as it is currently understood. Domain thinking simultaneously oversimplifies and overcomplicates. Compartmentalizing operations into a domain inherently ignores the aggregate effects and influence of the environment, suggested by systems theory in doctrine.[78] At the same time, by describing human made networks such as cyber as a domain, there is no limit to the possibilities of what can qualify, and therefore must be addressed. It assumes that physical domains and human-manufactured domains operate similarly. This allows for planners to wonder what domains may exist that have not been discovered or created, and exhaust resources and time attempting to find a means by which to outmaneuver an enemy that may or may not actually materialize. Manufactured domains inherently require participation. If the enemy is not in a domain, can they be affected there? Perhaps a manufactured domain can magnify effects in others, but effects from it cannot directly influence the physical existence of someone who has chosen not to be there.

What is the alternative?

Despite challenges with the current multi-domain operations paradigm, and with the associated domain thinking, doing nothing regarding this concept to then advance the country's warfighting capability is not an option. But one must tread carefully. Wholesale overhaul of doctrine and equipment risks undermining the ability of individual services to seek solutions within their imagination and budget that may not actually complement the joint force and risk what

dominance has been established in the primary domains. The joint force can forward multi-domain operations by leveraging existing force structure to focus and test the concept, gaining understanding of the existence of gaps in the current structure and applicability in proposed structure. This ensures that solutions work and do not cede capability across the majority of the joint force, preserving parent domain dominance. The aggregate of domain dominance augmented by multi-domain cooperation is enhanced capability and lethality. In combat, the side that bests understands this formula and is able to execute and apply it in stride, has a decided advantage. However, dealing with domains through lock-step solutions is not only impractical but also, thankfully, not necessary. Convoluted vision and competing requirements across the joint force defeat the notion of a perfect solution, but inherent ambiguity supported by minor synchronization efforts allows the joint force the ability to converge and maximize its effects.

Existing concepts that are relatable across the joint force are similar to principles of multi-domain operations and can be used to create a common language. Combined arms, maneuver warfare, single battle, and mission command are all familiar terms which frame multi-domain operations and streamline understanding.[79] However, within these concepts there is further misunderstanding. Army authors focus both on what the Army can provide to the joint force by having systems that have cross-domain effects, and what Army-pure multi-domain formations can achieve autonomously, independent of the joint force.[80] The Army in particular seeks multi-domain solutions through the depth of its formations, while Navy and Air Force authors have described the interrelated effects provided by the joint force. This demonstrates the difference between interpretation of the single battle concept.[81] Though single battle applies in both interpretations, the concept is at risk if the sum of the parts interfere with each other or go idle in supporting the aggregate joint force. The joint force requires a discussion about what

cross-domain capabilities are required by each service to support a broader operating concept. It also requires an honest discussion about what single-service capabilities should not be pursued that could undermine the overall operating concept. Currently these concepts are divergent, have created multiple meanings of multi-domain operations, and can hinder progress.

Decreased buying power compared to high operational costs over the past decade has frustrated modernization, a problem that has partly contributed to the shrinking overmatch enjoyed by the United States.[82] With the trajectory of conflict, it appears unlikely that modernization will be possible without competing with current operations, and therefore it can be assumed that immediate wholescale change and concrete cross-domain integration is not possible. Additionally, strategic mobility is at a shortage for force deployment and projection, a symptom of a significantly lower proportion of forward deployed US forces than the past.[83] This adds yet another level of complication to multi-domain operations, where the joint force, already competing for overmatch within the parent domains and being asked to provide cross-domain effects to support other service efforts is now required to synchronize mass troop movement at a scale that it is not prepared for.

Current structure exists to facilitate successful implementation of multi-domain operations, balancing the resource and time constraints of managing both a new operating concept and maintaining readiness in the existing force. The concept of calibrated force posture can be immediately leveraged. The Army forward deploys armored brigade combat teams in various theaters around the world on a rotational basis, currently Europe, Korea, and Kuwait. By making these permanent fixtures and adjusting the formations to be threat specific to the theater and adding multi-domain capability, the Army can mesh operations with innovation while maintaining fighting capability focused on the land domain across the rest of the available force.

These multi-domain strike groups, with increasing capability require that a general officer commands the formation, thereby addressing some authority issues that may be present regarding effects.[84] These formations with sufficient capability and survivability are placed in the contact layer and are capable of fighting immediately as the blunt force as described by the National Defense Strategy should a crisis break out.[85] When the surge force arrives, the calibrated multi-domain strike group has established required infrastructure, and is able to merge capability into the higher joint task force to prevent reduncancy. By providing specific forward deployed, calibrated multi-domain strike groups, the remainder of the Army can focus on land dominance, thereby linking the Army with the joint force, leveraging effects across domains, and continuing to seek focused dominance in its primary domain. Embracing the inherent ambiguity in the operating environment and the military's existing ability to manage it may provide targeted implementation of multi-domain operations that does not undermine jointness or effects coordination at scale. The solutions are already built in to structure and strategy requiring only minor adjustments. Multi-domain thinking is thus accounted for in the current military disposition.

The US military needs not be in awe of the complexity of the modern battlefield, but also needs to not add to it. The battlefield is changing, but our conceptualization can remain consistent in many ways. Fearing approaching parity on land, sea, and air, the joint force is correct in finding ways to magnify existing combat power. However, not using a common language and ignoring existing structure risks the potential effects of massing the aggregate joint force capability. Further, poor domain thinking is inherently risky. Assuming that parity or negative overmatch in one domain can be overcome by capability from another is limited by compartmentalization, or unnecessary redundancy. Domain thinking can also overstate the

decisiveness of inherently limited human created domains. Though potentially improving joint operations, if an adversary chooses to not be in a human created domain such as cyber, that domain cannot directly affect them. All of the advantages of domains such as GPS from space, or networking from cyber, can, in theory, be overcome from well-placed ordnance from a trained and able foe on the land, sea, or air. Guadalcanal highlights the generated fighting power and mutual reliance of multi-domain operations. It also shows that a force must be successful in winning in each domain, possibly independently. As demonstrated at Guadalcanal, the biggest favor one service can do for another is to not lose in its primary domain. Just as this responsibility was a requirement in the past, modern planners must also account for it while searching for application of effects in multi-domain coordination.

Accepting ambiguity is foundational in American understanding of war and consequently military doctrine. In order to manage ambiguity, concepts such as mission command are fostered in doctrine in order to enable low-level initiative and decision making via creativity. The US military's response to the current environment has done the opposite. The ambiguity of potential overmatch from competitors has compartmentalized solutions, whereby a threat is overcome by an asset in another domain like a game of rock paper scissors. Creativity within ambiguity is overshadowed by a lock-step solution from another domain and is convoluted by differences in understanding jointness.

Current domain thinking allows for infinite invention, and this is the good news. The bad news is that seeking to define a decisive solution through discovering or inventing a new domain may be impossible. The current understanding of multi-domain operations across the Army and how it fits into the joint force is thankfully ambiguous. There is a difference between natural ambiguity and a lack of synchronization. Current synchronization gaps can be overcome by joint

discourse, which may demonstrate that there is much ado about increasing multi-domain operations when the joint force is already there. The sum of the joint force combat power already enables multi-domain effects, leveraging creativity despite the concept of multi-domain operations not being overtly described in doctrine previously. Ambiguity breeds creativity and that state of mind wins wars. The current stress of domain thinking is a good example of the inability to get past the ambiguity of domains, but also the need to think about how to do so. The end-product of that effort breeds creative means of warfighting and leads to battlefield success.

Endnotes

[1] The current domains formally recognized are Land, Air, Sea, Space, and Cyber. See Headquarters, US Army Training and Doctrine Command. *The US Army in Multi-Domain Operations 2028*, TRADOC PAM 525-3-1, December 6, 2018. The pamphlet does not specifically define each or lay this out, but continuously references the "five domains." Additionally, this publication is the latest approved US Army vision of multi-domain battle, and therefore a key to understanding what is recognized as a domain.
[2] Elements sense and maneuver through convergence of capability across all domains. The document also cites cognitive isolation in addition to physical and virtual, suggesting effects beyond currently recognized domains. See Headquarters, US Army Training and Doctrine Command, 2018, ix.
[3]Chris Rein, "Guadalcanal: A case study for multi-domain battle," *Military Review*, 98, No. 3 (May/June 2018): 94.
[4]Rein, p. 102. Sea lines of communication and air lines of communication sustainability does not speak to the interoperability of domains. It speaks to dependency across domains in this specific case.
[5]James D. Hornfischer, *Neptune's Inferno: the U.S. Navy at Guadalcanal* (New York, NY: Bantam Books, 2011), 7.
[6]Two of the decisive land battles at Guadalcanal exemplify this: Tenaru and Edson's ridge. See Richard Frank, *Guadalcanal: The Definitive Account of the Landmark Battle* (New York, NY: Penguin Books, 1992), 153-155, 240. He describes the fight at Tenaru and USMC aircraft getting involved around 0630; he then describes Edson's ridge and how, despite night fighting, dawn was when aircraft was launched in support of ground combat.
[7]For the creation story, see Genesis 1, New King James Version Bible (NKJV), (Nashville, TN: Thomas Nelson, 1982).
[8]Genesis 3, NKJV.
[9] Free will appears most notably in the Gospels. Jesus after baptism endures 40 days in the wilderness resisting temptation. The free will by which Jesus overcomes temptation is archetypal of the imperative of choice between good and evil, and the foundation of faith. See Mark 1:12-13, Matthew 4:1-16 and Luke 4:1-14, NKJV.
[10]For discussion on the casting out from heaven, see Isaiah 14:12-15, NKJV. For implications regarding choice, see John 3:19, NKJV.
[11]Headquarters, US Army Training and Doctrine Command, 2018, 6.
[12]Ibid., 7.
[13]Headquarters, US Army Training and Doctrine Command. *Multi-Domain Battle: Evolution of Combined Arms for the 21st Century 2025-2040 v. 1.0*, TRADOC White Paper, October 2017, 1.
[14]Ibid., 5-7.
[15]Ibid., 7.
[16]Ibid., 2017, 7.
[17]Headquarters, US Army Training and Doctrine Command, 2018, 18-20.
[18]Headquarters, US Army Training and Doctrine Command, 2017, 8.
[19]Kelly McCoy, "The Road to Multi-domain Battle: An Origins Story." *Modern War Institute at West Point*, (October 2017), https://mwi.usma.edu/road-multi-domain-battle-origin-story/.
[20]AirLand Battle acknowledged the numerical and firepower deficiency of NATO forces against Soviet land forces. Seeking to overcome the discrepancy, moments of opportunity against parts of the Soviet force could be exploited. This is an inherent similarity between multi-domain operations and AirLand Battle. See D. W. Skinner, *Airland Battle Doctrine* (Washington, DC: Center For Naval Analyses, 1988), 3-10.
[21]Dries offers that interagency is also a part of the joint mentality required by multi-domain operations. This is a departure in scope from previous doctrine. See William Dries, "Some New, some Old, all Necessary," *Fires* (May/June 2017): 18.
[22]Foundational to the justification for a new framework is the professed lack of competition in air and sea in recent history for the US Military. See Headquarters, US Army Training and Doctrine Command, 2017, 1.
[23]Headquarters, US Army Training and Doctrine Command, 2017, 1.
[24]Richard Hart Sinnreich, "Multi-Domain Battle: Old Wine in a New Bottle?" *Army*, 67, no. 2, (2017): 14.
[25]AirSea Battle was written during the Global War on Terror. Despite being heavily involved in counter-insurgency operations, services were already seeking to address emerging parity with other potential adversaries. See Sinnerech, 14.
[26]Chief of Staff of the Army Strategic Studies Group, Cohort IV, *The character of warfare 2030- 2050: Technological change, the international system, and the state*, US Army Future Studies Group, 2015, 87. Also see

Headquarters, US Army Training and Doctrine Command, 2017, 1, for how the modern battlefield is a requirement for change.

[27]Headquarters US Marine Corps, *Warfighting,* MCDP 1, Washington, DC: Headquarters US Marine Corps, June 20, 1997, 44.

[28]Headquarters, Department of the Army. *Operations.* ADRP 3-0. Washington, DC: Headquarters, Department of the Army, November, 2016, 3-10.

[29]David Barno and Nora Bensahel, "Three things the Army chief of staff wants you to know," *War on the Rocks, Special Series-Strategic Outpost* (May 23, 2017), paragraphs 10-14.

[30]Uncertainty is inherent to strategy and is driven by four sources of uncertainty: aleatory uncertainty, complex systems, human limitations, and the enemy. These intersect with five factors of uncertainty in the theory of victory: international system, intelligence, friction, strategic interaction, and revolutions in military affairs. This framework demonstrates how factors interact to generate uncertainty in successful strategy. See Stephan Frühling, "Uncertainty, Forecasting and the Difficulty of Strategy," *Comparative Strategy*, 25, no. 1 (2006): 24.

[31]Ibid, 27.

[32]Ibid.

[33]Multi-domain operations is heralded as an evolution of combined arms by focusing on the convergence of effects across a broader spectrum. However, this is little departure from the intent of combined arms operations where effects were converged across domains already. See Headquarters, US Army Training and Doctrine Command, 2017, 3.

[34]Austin G. Commons, "Cyber is the New Air: Domain Superiority in the Megacity," *Military Review*, 98, no. 1 (January/February 2018): 120.

[35]The construct of the land, air, and sea domain definitions are similar, and the space and cyber definitions are structured differently. This may speak to the vision of domains and domain thinking, where there are three original and two additional. See Headquarters, US Department of Defense, *Department of Defense Dictionary of Military and Associated Terms*, Joint Publication 1-02, February 15, 2016, 6, 11, 58, 137, 146, and 220.

[36]This definition does not appear in joint or service terms dictionaries, nor does it appear in the Army's multi-domain operations papers previously referenced. It is a useful definition, though its source is unclear. See Dries, 16.

[37]Dries, 16.

[38]Headquarters, US Army Training and Doctrine Command, 2018, p. vi. This usage is found throughout the document.

[39]The idea of primary domains is prevalent throughout the document relating to the tactical level of war. Cross-applied to other concepts, the author suggests that tactical proficiency is inherent within one primary domain. See Albert Harris, "Preparing for Multidomain Warfare: Lessons from Space/Cyber Operations." *Air & Space Power Journal*, 32, no. 3 (Fall 2018): 47.

[40]Sea access and air superiority or supremacy are crucial to the Navy in the Pacific. Note the author is a former Navy Flag Officer and INDOPACOM commander. This position could hold heavy weight in the capability and doctrine discussions for the Navy and thus may reflect a trend of understanding for multi-domain operations. See Harry B. Harris Jr., "Role of Land Forces In Ensuring Access to Shared Domains" (speech, Association of the United States Army Institute of Land Warfare LANPAC Symposium, Honolulu, HI, 25 May 2016).

[41]Robert B. Brown, "The Indo-Asia Pacific and the Multi-Domain Battle Concept," *Military Review*, 97, no. 5 (2017): 18.

[42]GEN Brown comments on the complexity of INDOPACOM, suggesting that one force is not tailored to fit all situations. EUCOM, for example, would offer a different flavor of complexity. See Brown, 2017, 15-16.

[43]GEN Perkins was the Army TRADOC commander through much of the development of multi-domain battle. This article emphasizes the duality of the Army's vision: develop lethality within the Army through leveraging domains, and less on how it aids the overall joint force. See David G. Perkins, "Multi-Domain Battle: The Advent of Twenty-First Century War," *Military Review*, 97, no. 6 (2017): 12.

[44]Headquarters, US Army Training and Doctrine Command, 2018 x.

[45]TRADOC PAM 525-3-1 does not define the lowest echelon, but context suggests that Brigades are the lowest echelon. The fact that it is not overt adds to the confusion. See Headquarters, US Army Training and Doctrine Command, 2018, 23.

[46]Headquarters, US Army Training and Doctrine Command, 2018, 23.

[47]Ibid, 23.

[48]Nathan A. Jennings, "Realign the Army for Multi-Domain Battle," *Army Magazine,* 67, no. 4 (2017): p. 45.

[49]Nathan A. Jennings, Amos C. Fox, Adam L. Taliaferro, David W. Griffith, and Kyle T. Trottier, "The Return of Cavalry: A Multi-Domain Battle Study," *Cavalry & Armor Journal*, 8, no. 3 (2017): 24.
[50]Jennings, 2017, 45.
[51]Dries, 18.
[52]This source article is co-authored by both senior Army and Air Force General Officers responsible for doctrine. This is an indication that the coordination has at least taken place initially despite the acknowledged difference of opinions regarding multi-domain operations within the text. See David D. Perkins and James M. Holmes, "Multi-Domain Battle: Converging concepts toward a joint solution," *Joint Force Quarterly*, 88 (January 2018), 56.
[53]Perkins and Holmes, 2018, 54.
[54]GEN Perkins outlines the cooperation between the Army, USMC, and Air Force, but makes no further mention of the Navy in this article. See Perkins, 2017, 12-13.
[55] Stephen J. Townsend, "Accelerating Multi-Domain Operations: Evolution of an Idea," *Military Review*, 98, no. 5 (2018): 6.
[56]Anthony M. Clas, EdD, "Commanding in Multi- Domain Formations," *Military Review*, 98, no. 2 (2018): 95.
[57]David E. Johnson, Shared Problems: The Lessons of AirLand Battle and the 31 Initiatives for Multi-Domain Battle: *RAND Corporation* (August 2018), 5.
[58]Johnson, 2018, 3. Capability such as ATACMS and long range ground fires increased ranges and impeded Air Force efforts in the Deep Area, and Air Force air to ground target identification capability surpassed the need for many ground sensors.
[59]Headquarters, US Army Training and Doctrine Command, 2018, 6.
[60]Johnson, 6.
[61]Ibid., 6.
[62]Though there are similarities between China and Russia as explained by TRADOC PAM 525-3-1, differences are great enough to not make one solution sufficient to address both. Ibid., 6.
[63]The multi-domain operations publication admits to China and Russia being two distinct threats but assesses them to be sufficiently similar to apply the concepts equally. Russia is identified as the Army's pacing threat. See Headquarters, US Army Training and Doctrine Command, 2018, vi.
[64]Headquarters, US Army Training and Doctrine Command, 2018, 17.
[65]James E. Zanol and Brian M. Pierce PhD, "Overcoming the Challenges in Implementing Emerging Maneuver Concepts," *Military Review*, 98, no. 3 (2018): 87.
[66]Zanol and Pierce, 88.
[67]Skinner, 12.
[68]Headquarters, US Army Training and Doctrine Command, 2018, p. 23.
[69]Andrew F. Mazzara, "Integrating MAGTF into Joint Operations," *Marine Corps Gazette*, 78, no. 7 (1994): p. 65.
[70]Michael R. Kennedy, "MAGTF Area of Operations: Turf War Or Doctrinal Necessity?" *Joint Force Quarterly*, 32 (2002): 95.
[71]Sandra Jontz, "Taking Cyber War to the Front Lines," *Signal*, 71, no. 2 (October 2016): 23.
[72]Martin C. Libicki, "Cyberspace is Not a Warfighting Domain," *I/S: A Journal of Law and Policy*, 8, no. 2 (2012), 329.
[73]As challenging as hacking is, it becomes nearly impossible when adequately secured. See Libicki, 332.
[74]Michael Klipstein and Michael Senft. "Cyber Support to Corps and Below: Digital Panacea or Pandora's Box?" *Small Wars Journal*, http://smallwarsjournal.com/jrnl/art/cyber-support-to-corps-and-below-digital-panacea-or-pandora%E2%80%99s-box, accessed November 8, 2018.
[75]TRADOC PAM 525-3-1 describes the network as crucial to command and control, and references the Army Network throughout the document. See Headquarters, US Army Training and Doctrine Command, 2018, 12, 19, 47.
[76]Albert Harris, 51.
[77]MCDP 1, 92.
[78]All actions perceived or not on the battlefield have interconnected effects. See Headquarters US Marine Corps, *Command and Control*. MCDP 6, Washington, DC: Headquarters US Marine Corps, October 4, 1996, 47.
[79]C. T. Reese, "Between Buzzwords and Big Ideas," *Army*, 67, no. 1 (2017): 12.
[80]Perkins, 11. GEN Perkins and other authors suggests that the Army should have an impact to the joint force and that lies on multidomain capability. However, GEN Perkins article describes capability advancements that seem to only enhance the Army's combat power.
[81]Single Battle Concept: "Operations or events in one part of the battlespace often have profound and consequent effects on other areas and events; therefore, a commander must always view the battlespace as an indivisible entity.

Commanders prepare for a single battle effort during planning primarily through their intent, which provides the larger context for subordinate units so they can exercise judgment and initiative when the unforeseen occurs while remaining consistent with larger aims." See Headquarters US Marine Corps. *Marine Corps Planning Process,* MCWP 5-10, Washington, DC: Headquarters US Marine Corps, May 2, 2016, 1-6.

[82]Carter F. Ham, "The Great War Echoes Today: Army Faces Similar Challenges a Century Later," *Army Magazine*, 67, no. 10 (October 2017): 8.

[83] Ham, 8.

[84]Douglas Macgregor, "Strategic Means: Building an Army for an Era of Uncertainty," in *American Grand Strategy and the Future of U.S. Landpower*, Carlisle, PA: U.S. Army War College Press, December 2014. Macgregor's Light Reconnaissance Strike Group formation suggests a formation of similar size as an Army Brigade Combat Team (BCT) with more cross-domain capability and survivability. Though developed before the "multi domain battle" concept, the formation provides insight into the span of control issues of a cross domain formation. The author suggests a Brigadier General should command such a formation, further implying that the complexities of multi-domain battle exist at echelon. Having a commander more senior to the multi-warfighting function BCTs suggests that it will be difficult to produce multi-domain effects below the brigade level or higher.

[85]James N. Mattis, *Summary of the 2018 National Defense of the United States of America: Sharpening the American Military's Competitive Edge*, Arlington, VA: Office of the Secretary of Defense, 2018, 7.

Bibliography

Barno, David, and Nora Bensahel. “Three things the Army chief of staff wants you to know.” *War on the Rocks, Special Series-Strategic Outpost* (May 23, 2017).

Brown, Robert B. “The Indo-Asia Pacific and the Multi-Domain Battle Concept.” *Military Review*, 97, no. 5 (September/October 2017): 14–20.

Chief of Staff of the Army Strategic Studies Group, Cohort IV. *The character of warfare 2030-2050: Technological change, the international system, and the state.* US Army Future Studies Group, 2015.

Clas, Anthony M., EdD. "Commanding in Multi- Domain Formations." *Military Review,* 98, no. 2 (2018): 90-100.

Commons, Austin G. "Cyber is the New Air: Domain Superiority in the Megacity." *Military Review,* 98, no. 1 (January/February 2018): 120-130.

Dries, William. "Some New, Some Old, all Necessary." *Fires* (May/June 2017): 16-18.

Frank, Richard. *Guadalcanal: The Definitive Account of the Landmark Battle.* New York, NY: Penguin Books, 1992.

Frühling, Stephan. “Uncertainty, Forecasting and the Difficulty of Strategy.” *Comparative Strategy*, 25, no. 1 (2006): 19-31.

Ham, Carter F. “The Great War Echoes Today: Army Faces Similar Challenges a Century Later.” *Army Magazine*, 67, no. 10 (October 2017): 4–8.

Harris, Albert. "Preparing for Multidomain Warfare: Lessons from Space/Cyber Operations." *Air & Space Power Journal,* 32, no. 3 (Fall 2018): 45-61.

Harris, Harry B. Jr., “Role of Land Forces In Ensuring Access to Shared Domains.” Speech, Association of the United States Army Institute of Land Warfare LANPAC Symposium. Honolulu, HI, May 25, 2016.

Headquarters, US Army Training and Doctrine Command. *Multi-Domain Battle: Evolution of Combined Arms for the 21st Century 2025-2040 v. 1.0.* TRADOC White Paper, October 2017.

Headquarters, US Army Training and Doctrine Command. *The US Army in Multi-Domain Operations 2028.* TRADOC PAM 525-3-1, December 6, 2018.

Headquarters, Department of the Army. *Operations.* ADRP 3-0. Washington, DC: Headquarters, Department of the Army, November, 2016.

Headquarters, US Department of Defense. *Department of Defense Dictionary of Military and Associated Terms.* Joint Publication 1-02, February 15, 2016.

Headquarters, US Marine Corps. *Warfighting.* MCDP 1. Washington, DC: Headquarters US Marine Corps, June 20, 1997.

Headquarters, US Marine Corps. *Command and Control.* MCDP 6. Washington, DC: Headquarters US Marine Corps, October 4, 1996.

Headquarters, US Marine Corps. *Marine Corps Planning Process.* MCWP 5-10. Washington, DC: Headquarters US Marine Corps, May 2, 2016.

Hornfischer, James D. *Neptune's inferno: the U.S. Navy at Guadalcanal*. New York, NY: Bantam Books, 2011.

Jontz, Sandra. "Taking Cyber War to the Front Lines." *Signal*, 71, no. 2 (October 2016): 20-23.

Jennings, Nathan A. "Realign the Army for Multi-Domain Battle." *Army Magazine*, 67, no. 4 (2017): 45–48.

Jennings, Nathan A., Amos C. Fox, Adam L. Taliaferro, David W. Griffith, and Kyle T. Trottier. "The Return of Cavalry: A Multi-Domain Battle Study." *Cavalry & Armor Journal*, 8, no. 3 (2017): 23–28.

Johnson, David E. Shared Problems: The Lessons of AirLand Battle and the 31 Initiatives for Multi-Domain Battle: *RAND Corporation*. (August 2018).

Kennedy, Michael R. "MAGTF Area of Operations: Turf War Or Doctrinal Necessity?" *Joint Force Quarterly*, 32 (2002): 93-97.

Klipstein, Michael, and Michael Senft. "Cyber Support to Corps and Below: Digital Panacea or Pandora's Box?" *Small Wars Journal*. http://smallwarsjournal.com/jrnl/art/cyber-support-to-corps-and-below-digital-panacea-or-pandora%E2%80%99s-box.

Libicki, Martin C. "Cyberspace is Not a Warfighting Domain." *I/S: A Journal of Law and Policy*, 8, no. 2 (2012): 321-336.

Macgregor, Douglas. "Strategic Means: Building an Army for an Era of Uncertainty," in *American Grand Strategy and the Future of U.S. Landpower*. Carlisle, PA: U.S. Army War College Press, December 2014.

Mattis, James N. *Summary of the 2018 National Defense of the United States of America: Sharpening the American Military's Competitive Edge*. Arlington, VA: Office of the Secretary of Defense, 2018.

Mazzara, Andrew F. "Integrating MAGTF into Joint Operations." *Marine Corps Gazette*, 78, no. 7 (1994): 64-68.

McCoy, Kelly. "The road to multi-domain battle: An origins story." *Modern War Institute at West Point,* (October 2017). https://mwi.usma.edu/road-multi-domain-battle-origin-story/.

Perkins, David G. “Multi-Domain Battle: The Advent of Twenty-First Century War.” *Military Review*, 97, no. 6 (2017): 8–13.

Perkins, David D., and James M. Holmes. “Multi-domain battle: Converging concepts toward a joint solution.” *Joint Force Quarterly,* 88, (January 2018): 54-57.

Reese, C. T. "Between Buzzwords and Big Ideas." *Army,* 67, no. 1 (2017): 11-13.

Rein, Chris. “Guadalcanal: A case study for multi-domain battle.” *Military Review,* 98, no. 3 (May/June 2018): 93-102.

Skinner, D. W. *Airland Battle Doctrine*. Washington, DC: Center For Naval Analyses, 1988.

Sinnreich, Richard Hart. "Multi-Domain Battle: Old Wine in a New Bottle?" *Army,* 67, no. 2, (2017): 13-14.

Townsend, Stephen J. “Accelerating Multi-Domain Operations: Evolution of an Idea.” *Military Review*, 98, no. 5 (2018): 4–7.

Zanol, James E. and Brian M. Pierce PhD. "Overcoming the Challenges in Implementing Emerging Maneuver Concepts." *Military Review*, 98, no. 3 (2018): 84-92.