REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
04/29/2021	Master of Military Studies Research Paper	September 2020 - April 2021

4. TITLE AND SUBTITLE
Maneuver or Fires in Cyberspace? It Depends

5a. CONTRACT NUMBER
N/A

5b. GRANT NUMBER
N/A

5c. PROGRAM ELEMENT NUMBER
N/A

6. AUTHOR(S)
Conley, Jonathon B. (Major)

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)
N/A

10. SPONSOR/MONITOR'S ACRONYM(S)
N/A

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

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

13. SUPPLEMENTARY NOTES
N/A

14. ABSTRACT
Analogies and metaphors serve the human mind in making sense of what is unknown through association with what is known, but there comes a point where they can be distracting. Such is the case with maneuver in cyberspace when it is moved from the echelons of reality to the tactical ground formation and discussed hand in hand with tactical ground maneuver. When considering the principles such as maneuver and fires in cyberspace the tactical level of warfare is the point of departure at which discussing maneuver in cyberspace should be left in the cyber mission planning room and kept out of the discussion of ground operations.

15. SUBJECT TERMS
Analogies, metaphors; domains, cyberspace; maneuver, fires, effects; multi-domain operations, cross-domain

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Marine Corps Univ/Command and Staff College
Unclass	Unclass	Unclass	UU	32	19b. TELEPHONE NUMBER *(Include area code)* (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

MANEUVER OR FIRES IN CYBERSPACE? IT DEPENDS

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

Major Jonathon "Barron" Conley, USA

AY 2020-21

MMS Mentor and Oral Defense Committee Member:
James H. Joyner, Jr., Ph.D.
Approved: _____
Date: 15 APR 21

MMS Mentor and Oral Defense Committee Member:
J.D. Work
Approved: _____
Date: 15 April 2021

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

MANEUVER OR FIRES IN CYBERSPACE? IT DEPENDS

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

Major Jonathon "Barron" Conley, USA

AY 2020-21

MMS Mentor and Oral Defense Committee Member:
James H. Joyner, Jr., Ph.D.
Approved: _____
Date: _____

MMS Mentor and Oral Defense Committee Member:
J.D. Work
Approved: _____
Date: _____

Executive Summary

Title: Maneuver or Fires in Cyberspace? It Depends

Author: Major Jonathon Barron Conley, United States Army

Thesis: When considering the principles of maneuver and fires in cyberspace the tactical level of warfare is the point of departure at which discussing maneuver in cyberspace should be left in the cyber mission planning room and kept out of the discussion of ground operations.

Abstract: This paper offers a way to look at cyberspace from the perspective of the Army ground tactical level that prevents confusion when applying common principles of warfare such as fires and maneuver in a multi-domain or cross-domain context. With the rollout of Multi-Domain Operations as the Army's future operating concept, and the associated push to integrate cyberspace capabilities previously thought to be at the national and strategic level to the lower tactical level of warfare, came the introduction of new terms into the Army lexicon such as *cross-domain maneuver* and *cross-domain fires*. Confusion has resulted at the tactical level from cross-domain maneuver as it has subsequently forced the discussion of cyber maneuver into the same room as tactical ground maneuver. While analogies and metaphors serve the human mind in making sense of what is unknown through association with what is known, there comes a point where they can be distracting. Such is the case with cyber maneuver when it is moved from the echelons of reality to the tactical ground formation and discussed hand in hand with operations in the physical domains. Cyber maneuver at echelons above reality can be a useful way of understanding the operations within the domain as a standalone, but for any cyberspace operations at these levels that touch the physical domains with noticeable effects, a better analogy already exists in the way that the air domain provides operational and strategic effects in support of the ground units. Likewise, at the tactical level, the best way to think about cyberspace is from a purely fires and effects-based point of view, as is already the case with Army aviation when delivering effects in close proximity to friendly forces.

Conclusion: Analogies and metaphors are useful until they are not. The implementation of maneuver as an analogy to understand cyberspace was useful until the Army decided to integrate cyberspace capabilities into tactical operations. The use of fires analogies and metaphors serve more purpose for cross-domain concepts than maneuver. If multi-domain operations is the way forward, a clear line should be drawn on the matter of cross-domain maneuver at the tactical level to exclude the use of cyber maneuver.

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.

Table of Contents

Page

Acknowledgements

I am grateful to have been afforded the opportunity to interact with so many talented military officers, interagency civilians, and professors over the course of this academic year. Your shared experiences and knowledge have given me a new breath of ideas to share when I return to the operational Army. I would especially like to thank LtCol Zachariah "Butters" Anthony for taking a vested interest in my growth as an officer and human being.

Working with Dr. James Joyner and Mr. J.D. Work on this project has been a truly remarkable experience. I have learned more than I could have ever imagined about my own research and writing abilities through your guidance. More importantly, I have a newfound respect and better understanding for the cyberspace domain, which no longer seems as distant to me as it did prior to beginning this project. Thank you for the patience and constant feedback that you provided throughout this journey as I required ample course corrections to maintain forward progress.

Lastly, I would like to thank my wife Gina for putting up with all of the late nights and long hours of research and writing.

J. Barron Conley
Quantico, Virginia
March 2021

Chapter 1 – Cyberspace as Its Own Domain

Introduction

With the rollout of multi-domain operations as the Army's future operating concept, and the associated push to integrate cyberspace capabilities previously thought to be at the national and strategic level to the lower tactical level of warfare, came the introduction of new terms into the Army lexicon such as *cross-domain maneuver* and *cross-domain fires*. Confusion has resulted at the tactical level from *cross-domain maneuver* as it has subsequently forced the discussion of cyber maneuver into the same room as tactical ground maneuver, raising a valid question. Does the Army maneuver in cyberspace or does it use actions in cyberspace as fires in support of maneuver forces? The answer is not simple, but instead depends largely on the perspective through which is viewed.

While analogies and metaphors serve the human mind in making sense of what is unknown through association with what is known, there comes a point where they can be distracting. Such is the case with the application of maneuver analogies to cyberspace operations when it is moved from the higher levels of warfare to the tactical ground formation and discussed hand in hand with operations in the physical domains.

Cyber maneuver at "echelons above reality" can be a useful way of understanding the operations within the domain as a standalone, but for any cyberspace operations at these levels that touch the physical domains with noticeable effects, a better analogy already exists in the way that the air domain provides operational and strategic effects in support of the ground units. Likewise, at the tactical level, the best way to think about cyberspace is from a purely fires and effects-based point of view, as is already the case with Army aviation when delivering effects in close proximity to friendly forces.

When considering the principles of maneuver and fires in cyberspace the tactical level of warfare is the point of departure at which discussing maneuver in cyberspace should be left in the cyber mission planning room and kept out of the discussion of ground operations.

The first chapter of this paper provides context on how the military arrived at cyberspace as a domain and shares insight on some of the initial resistance to applying external domain analogies. The second chapter covers many of the issues that exist for the tactical Army in viewing cyberspace which is to most still largely at the higher levels of warfare above reality. In doing so, the chapter looks at some of the fundamental issues with conceptualizing maneuver in cyberspace as opposed to fires before offering an air domain fires-based approach through which operational and strategic cyberspace effects are best viewed. The third chapter explains the tactical lens in more detail, showing that the way in which the tactical Army already views the actions in the air domain to view cyberspace actions as fires instead of maneuver.

How did we arrive at cyberspace as a domain? (Literature, Doctrine, Policy, and Confusion)

The U.S. Army published its 2017 rewrite of FM 3-0, *Operations,* which resulted in the subsequent overhaul of service warfighting function doctrines to address both the Army's current role in Unified Land Operations and, "[E]lements of the multi-domain operations future concept that could be implemented within the Army's currently fielded capabilities."[1] Multi-domain operations is the Army's answer to changes in the National Defense Strategy since 2015 and addresses how the Army will conduct operations against near-peer adversaries as a part of the future joint force to counter challenges in all domains including cyberspace.[2] Multi-domain operations also promotes the idea of maneuver in cyberspace as one of its concepts where it requires, "[M]aneuver to operate both in and across all domains."[3]

The Army's current cyberspace doctrine, FM 3-12, *Cyberspace and Electronic Warfare Operations* was released prior to the 2017 rewrite of FM 3-0 or the multi-domain operations rollout and makes no direct mention of maneuver in cyberspace. However, FM 3-12 borrowed heavily from the existing terminology and framework established by the joint doctrine, JP 3-12 [R], *Cyberspace Operations,* which included ample description of maneuver in and across cyberspace.[4] Instead, FM 3-12 shows a proclivity towards actions and effects to describe cyberspace operations, which suggests that prior to multi-domain operations the Army viewed its actions in cyberspace as fires or effects in support of ground maneuver. The fires and effects-oriented nature of current Army cyberspace doctrine contrasted with the cyberspace maneuver-oriented approach of MDO is a source of confusion for the tactical Army.

The first area of literature reviewed covers the establishment of cyberspace as a domain in concert with the evolution of doctrine and policy. Cyberspace is still recognized as part of the overall information environment, but what is now referred to as cyberspace operations was once captured under both the information environment and its associated information operations.

In 2001, then-Army Colonel Glenn Takemoto introduced the concept of cyberspace as a domain in his Army War College Strategy Research Project titled, "Information Warfare in the Cyber Domain." Takemoto argued for the establishment of cyberspace as its own domain and suggested the existing principles of war should be used as an initial doctrinal framework for what he called information warfare in the cyber domain.[5] At the time, information operations encompassed the entire information environment, to include what we now refer to as cyberspace.

For examples of now cyberspace but then information operations doctrinal terms in circulation at the time information warfare in the cyber domain was written, one could look to the 1998 Joint Publication 3-13, *Information Operations*. There they would likely find

information operations (IO) centric terms such as, "Offensive IO, Defensive IO, and Information Warfare."[6] Offensive and Defensive IO are doctrinal derivatives of the Offensive Cyber Operations (OCO) and Defensive Cyber Operations (DCO) found in current doctrine, whereas Information warfare encompassed what is now referred to as cyberconflict in addition to other operations in the information environment. Takemoto's writing holds a seminal value for cyberspace in some ways as his recommendations are nearly identical to many principles found in current cyberspace doctrine such as the 2018 Joint Publication 3-12, *Cyberspace Operations*. Despite the 2001 emergence of Takemoto's recommendation, neither the break from information operations, nor the translation of his cyberspace domain from theory to doctrine were immediate.

Today, cyberspace is referred to among defense and security circles as the fifth domain, but it was the information environment that first achieved status as the fifth domain in doctrine. Joint Publication 3-0, *Operations*, 10 September 2001, introduced information as a fifth domain in addition to the four physical domains.[7] In conjunction with the information domain, the 2001 JP 3-0 described IO as, "actions to affect or defend information and information systems."[8] Using today's terms and understanding of cyberspace doctrine, this prior definition could be interpreted as conducting OCO, DCO or Department of Defense Information Network (DODIN) operations to ensure freedom of action or maneuver in cyberspace. Information's lifespan as a domain was short-lived, having its domain status in doctrine formally removed in the 2006 publication of JP 3-0, which described information as an environment, "aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information."[9]

One key takeaway from the interim period between the 2001 publication and the 2006 update of the JP 3-0 was the advancement of policy language to acknowledge cyberspace as both a domain and a global commons. For instance, the 2004 National Military Strategy was the first

place in policy where senior defense leadership recognized cyberspace as a domain along with the four physical domains; attributed to the growing reliance on information systems and acknowledgment of their vulnerabilities.[10] While groundbreaking in the formal acknowledgement of cyberspace as the fifth domain in place of information, the 2004 National Military Strategy contains an inconsistency that suggests cyberspace and information were still potentially interchangeable words in domain discussions. "[I]nformation domain," was still used on one instance in the document even after declaring cyberspace as the fifth domain in contrast to the four physical domains.[11] The one for one substitution in the policy document was possibly made as an oversight while referencing the 2001 JP 3-0. The first doctrinal publication solely devoted to cyberspace was published in 2012 with Joint Publication 3-12, Cyberspace Operations. JP 3-12 established cyberspace as the fifth domain.

Area of disagreement: Cyberspace is Not a Domain – The Differences

The next area of literature covered focuses on invalidating the existing doctrine concerning cyberspace as a domain by focusing on the differences between the other pre-existing domains. RAND analyst Martin C. Libicki was one of the initial opponents to the establishment of cyberspace as a domain. In his 2012 article transparently titled, "Cyber Is Not a Warfighting Domain," Libicki leads off with a quote from former NSA Director Michael Hayden, in which the senior leader praises the evolution of doctrine and domains to the advent of cyberspace as the fifth, but also acknowledges the significant difference in cyberspace properties proposing the question, "Are these differences important enough for us to rethink our doctrine?"[12] Libicki's central argument is that by likening cyberspace to a warfighting domain, there is a necessity to force the pre-existing problems and principles of cyberspace into broader, traditional warfighting context and away from a creative, engineering mindset.[13] The engineering mindset, as Libicki

suggests, is more in line with the technical education and foundation of the cybersecurity realm.[14] The potential risk of departing from an already established industry mindset can result in unintended effects or the failure to align the correct priorities. Libicki also suggests a reason for importing older domain concepts into cyberspace doctrine occurred because senior military leaders initially in charge of cyber and the writing of its doctrine all came with the pre-existing frameworks from their previous domains of expertise as a necessity for making sense of cyberspace. [15] This article does not expand on the topic, but it is key to highlight a possibility that future military members, specifically leaders could reach a level of understanding that negates the need to force outside principles into cyberspace.

Like Libicki, McGuffin and Mitchell focus their argument against cyberspace as a domain on the differences between domains which they highlight as technical, procedural, and physical.[16] From a technical standpoint key terrain in the cyber domain can be changed because it is manmade; from a procedural standpoint vulnerabilities can be fixed once they are discovered; and from a physical standpoint soldiers cannot jump into cyberspace.[17] While from a physical standpoint a soldier jumping into cyberspace or physical space would hardly constitute a requirement for domain status, it is valuable to note that both joint and Army doctrine fail to define what exactly constitutes a domain. Their conclusion suggests that cyberspace activities or cyber operations should focus on executing a support role of providing effects in the other physical domains rather than existing as a stand-alone domain because of the lack of similarities between the other domains.

The fact that conflict can exist by itself in cyberspace seems enough to justify its existence, but to the authors' standpoint the argument might be better made if there were a doctrinal definition for what constitutes a domain. To address the counterargument that physical

domains share inconsistencies with one another, the authors suggest that cyberspace's lack of permanence is what disqualifies it as a standalone domain.[18] In addition to arguing against cyberspace as a warfighting domain, both works support a suggestion that activities in cyberspace or cyber operations are more fitting to providing effects in the traditional domains.

Chapter 2 – Echelons Above Reality

> *Army organization above corps, with its links to the joint and combined environment, is less easily described and understood than the structure at corps and below.*[19]
> – Lieutenant General John J. Yeosock, commanding general, Third US Army

For most of the Army, which resides in tactical ground units, the operational and especially strategic levels of warfare are generally perceived as 'echelons above reality.'[20] Traditionally echelons above corps have been associated with the strategic and operational levels of warfare. Joint doctrine offers definitions for both the strategic and operational levels of war. The strategic level of warfare is defined as, "The level of warfare at which a nation, often as a member of a group of nations, determines national or multinational (alliance or coalition) strategic security objectives and guidance, then develops and uses national resources to achieve those objectives."[21] One level below strategic, is the operational level of warfare which is defined as, "The level of warfare at which campaigns and major operations are planned, conducted, and sustained to achieve strategic objectives within theaters or other operational areas.[22] The tactical level of warfare, which resides below the operational level, will be addressed in more detail during the next chapter. However, this chapter incorporates elements of the tactical discussion as necessary to establish context for how the Army should view cyberspace, especially at the higher levels of warfare.

The conceptualization of cyberspace, cyber forces, and the operations that occur within the domain are also generally perceived to be at echelons above reality when viewed from the tactical level of warfare looking up. This perception can be attributed to multiple factors, which

include but are not limited to the highly technical nature of cyberspace; a lack of integration of both cyberspace capabilities and cyber units at the tactical level; gaps in current cyberspace doctrine between the echelons above reality and the tactical level; the highly classified nature of offensive cyberspace operations; and limitations in the usefulness of land domain analogies and metaphors.

The Army's current mission is, "To deploy, fight, and win our Nation's wars by providing ready, prompt, and sustained land dominance by Army forces across the full spectrum of conflict as a part of the joint force."[23] At the end of the day, the Army's goal is land dominance, which is achieved by the projection of physical force through ground maneuver, but cyberspace as a warfighting domain is here to stay and must not be overlooked in any current or future multi-domain fight. The continued exponential growth of the internet of things (IoT) will result in what JD Work describes as, "[W]ider attack surface and an ever-greater range of both subtle and immediate effects."[24] From this assumption, cyberspace can be viewed as a parallel dimension to the other conflict domains in which an increased surface area created by the IoT will provide nearly unlimited physical layer points of access to integrate cyber capabilities where forces are on the ground.[25]

The relative recent introduction of the Army's future operating concept of multi-domain operations for the strategic and operational level and cross-domain maneuver for the tactical level have raised some additional challenges for Army leaders looking to understand the where and how cyberspace fits in. The future operating concept has ushered into the tactical ground unit discussion, the concept of cyber maneuver and fires as an integral part of maneuvering across domains in the multi-domain fight. Luckily, from the ground tactical lens looking up, a useful framework already exists in the way that the air domain provides operational and strategic fires

or effects in support of Army land dominance through ground maneuver. To better understand the suitability of using the analogy of air domain effects over land domain maneuver at the strategic and operational levels to describe cyberspace actions, it is first necessary to take a deeper look into the source of confusion for Army tactical units.

Lack of Integration of Cyber Forces

Cyberspace capabilities and forces are not yet organic to Army tactical ground units at the corps and below. The lack of integration adds to the perception that cyberspace is at an echelon above reality, which is exacerbated by the fact that current cyber forces focus on strategic or national level cyber operations.[26] Under the direction of the Joint Staff and ARCYBER, the Army stood up 41 cyber mission teams (CMTs) as part of the United States Cyber Command's (USCYBERCOM) cyber mission force (CMF).[27] Tasked with the missions of conducting offensive and defensive cyberspace operations, as well as DODIN operations, the Army CMTs are made up of, "Cyber Protection Teams (CPTs), Cyber Combat Mission Teams and Combat Support Teams (CSTs), as well as National Mission Teams (NMTs) and their complementary National Support Teams (NSTs)."[28] The Army has made strides in closing the gap between its strategic cyber forces at USCYBERCOM and Army Cyber Command (ARCYBER) and the tactical ground units by activating new units such as the 915th Cyber Warfare Battalion (CWB), which is designed to take organic cyberspace capabilities closer to the fight through deployable expeditionary cyber teams (ECT).[29] The future integration of ECTs into the tactical formations will undoubtedly help in making cyberspace less of a myth for tactical units, as was the case when the Army started integrating organic electronic warfare capabilities at the tactical level.

Cyberspace Doctrine is Too Strategic

An additional factor that contributes to the current perception of cyberspace at echelons above reality and unrelatable to tactical ground units looking up lies with gaps in doctrine especially when addressing the principle of maneuver in cyberspace. Current cyberspace doctrine only covers maneuver at the joint doctrine level, which is limited to addressing the conduct of cyberspace operations within a strategic sense at the, "combatant command, joint force command, or national objective level."[30] At this strategic level, the doctrine covers both the principles of maneuver and fires within cyberspace as specific types of actions in the conduct of offensive cyberspace operations, defensive cyberspace operations, and DODIN operations.[31] In the context of offensive cyberspace operations specifically, fires refers to the specific cyberspace action of cyberspace attack, while maneuver refers to the specific cyberspace action of cyberspace exploitation.[32] A cyberspace attack is defined by Joint Publication 3-12, *Cyberspace Operations,* as action(s) which, "[C]reate noticeable denial effects…"[33] Denial effects can occur in cyberspace alone or through cyberspace to a physical domain and be accomplished by degrading, disrupting, or delaying.[34] Conversely, with respect to cyberspace exploitation, the joint publication highlights that, "Maneuver in cyberspace is complex and generally not observable."[35]

At the service level, Army cyberspace doctrine fails to clarify the concept of maneuver in cyberspace established by joint doctrine.[36] The Army's Field Manual 3-12, *Cyberspace and Electronic Warfare Operations*, uses a fires or effects based approach to addressing planning and coordination of cyberspace activities into tactical operations instead of the independent maneuver and fires distinguishment of the activities as in the joint publication.[37] A significant

issue lies in that the Army makes no mention of maneuver as a warfare principle in cyberspace at all in its own cyberspace doctrine despite use of the cyberspace exploitation concept. If the Army does in fact maneuver in cyberspace, it would be advantageous to clarify the concept in future doctrinal updates.

Over-Classified in Nature

When Army ground tactical units are looking up at echelons above reality in terms of the strategic and operational cyberspace, the offensive cyberspace operations are generally what produce noticeable effects in the physical domains. An additional factor that impacts understanding of cyberspace from the outside looking in is the highly classified nature of offensive cyber operations. A glance at the literature regarding the initial integration of cyberspace attack and cyberspace exploitation capabilities into military operations can provide context for current problems in conceptualization. Cybersecurity experts Williams Owens, Kenneth Dam, and Herb Lin captured the essence of this problem lying in issues of over classification, "Programs to develop cyberattack capabilities are classified and dispersed throughout many program elements within the Department of Defense, with the result that overall capabilities may not be widely known even among those with the necessary clearances."[38] Additional criticism against the classified nature was provided by former Director of the National Security Agency, Michael Hayden, who stated, "It is difficult to develop consensus views on things that are largely unknown or only rarely discussed by a select few."[39] If a capability is so classified that no one is allowed to talk about, then it is unreasonable to expect that they should be able to understand it.

Maneuver Metaphors and Analogies Have Limitations

Metaphors and analogies are useful in assisting humans with understanding complex or new concepts. Domains have served the military with understanding how to fight in new dimensions well before the term domain was added to the military lexicon. Each time throughout military history that technology increased to provide access to a new place to fight, theorists would use some of the existing principles of the military dimension in which they were most comfortable to make sense of the new one. While domain theories have their uses in assisting the military in understanding cyberspace, its uniqueness and complexity also pose limitations when importing one-to-one domain comparisons from the land domain.

One way to look at metaphors and analogies is that they are useful until they are not. When viewing a concept like maneuver in cyberspace at an echelon that is already above reality from one's vantage point, as is the case with cyberspace at the operational and strategic level, the use of domain analogies is relatively transparent, especially when talking about actions occurring independent of other domains. It can be maneuver or fires and matter little to the tactical ground unit. With the case of cyberspace and the land domain, the use of the maneuver analogy was useful until the theories of maneuver in cyberspace and ground maneuver became intermingled into the same discussion, as is becoming the case with multi-domain operations and cross-domain maneuver discussions.

Despite its growing importance, cyberspace remains a complicated domain when compared to the other physical domains, especially the land, sea, and air domains in which warfare has traditionally been conducted across. The highly technical nature of cyberspace, which consists of three separate, but interrelated layers (physical network, logical network, and cyber-persona) is a leading contributor to the complexity of the domain, which often results in confusion among non-technical experts.[40] Confusion among tactical Army circles often arises

over the fact that aside from the 'hardware and infrastructure'[41] of the physical network layer, which includes tangible elements such as computers, routers, switchboards, etc..., the preponderance of cyberspace and the actions that occur within the domain are largely untouchable or invisible to the human eye. While it is capable for cyberspace actions to produce visible effects in the physical domains, this is not always the case, which can be frustrating for those on the outside looking in.

In an attempt to advance an understanding of how military operations fit in cyberspace, joint doctrine suggests that domains in general are beneficial models for conceptualizing the physical space in which military operations occur.[42] Jordan Branch describes the use of domains in the military context through a practice referred to as 'foundational metaphors.'[43] The analogy of similarities in physical operating spaces such as land, sea, or air through this foundational metaphor construct are particularly helpful in providing a framework to understand complex concepts.[44] After all, applying concepts that one already understands to new unfamiliar spaces is a common practice among everyday life.

Existing literature on metaphors provides a way to looking at how the properties of metaphors can either work for or against their use. Metaphor experts Lakeoff and Johnson state that, "The essence of metaphor is understanding and experiencing one kind of thing in terms of another."[45] As many of the initial military cyber leaders came from non-cyberspace, physical domain backgrounds it is understandable why many theorists and doctrine writers have and continue to incorporate existing principles of war into the framework and concepts of cyberspace operations.[46] Since the Army is in the business of fighting land wars, it especially makes since that its own doctrine writers and theorists looked to analogies and metaphors of fires and maneuvers for cyberspace as these two elements are among the most fundamental for conducting

ground combat operations. However, as analogies and metaphors have their usefulness, they also have their limitations and can sometimes be distracting if applied the wrong way or taken too literally.

In the case with cyberspace, the usefulness of the maneuver principle of warfare as a metaphor tends to expire prior to the usefulness of fires or effects. This section will use Lakeoff and Johnson's logic of the interactional properties of metaphors to analyze fires and maneuver as multi-dimensional concepts in comparison from physical domain to cyberspace.[47] In terms of interactional properties of metaphors Lakeoff and Johnson argue, "The kind of conceptual system we have is a product of the kind of beings we are and the way we interact with our physical and cultural environments."[48] When applying modifiers to a concept, such as land, ground, or cyber to maneuver, the interactional properties can be used to determine if the modifier creates a negating or preserving effect to the dimensions of the original concept.[49]

Fires as a Metaphor

To analyze the interactional properties of fires in cyberspace, it is first necessary to look at joint doctrine, which provides the following definition, "To employ fires is to use available weapons and other systems to create a specific effect on a target."[50] In the context of fires, joint doctrine also offers the following definition for effect as, "The physical or behavioral state of a system that results from an action, a set of actions, or another effect."[51] A useful example for framing fires from the tactical ground perspective is a basic call for fire from an infantry platoon in contact with an enemy machine gun position. In this case the forward observer as the sensor representative of a surface-to-surface fires kill chain identifies and derives accurate targeting data on the target, which is the enemy machine gun nest. Utilizing organic communications equipment, the derived target data and a standard call for fire format, the forward observer

requests a desired effect in the form of an immediate suppression mission from platoon's assigned mortar section. The mortar section delivers a volley of rounds within effective range of the enemy position, causing the enemy to stop shooting momentarily, and achieving the desired effect of suppression.

Using the fires concept definition in conjunction with the common land domain example serves as a baseline for comparison when cyberspace or cyber is used as a modifier to the original concept, fires. The properties of the concept to include weapons and systems, effects, and targets are all conceptually preserved when applied to cyberspace. It is generally understood that weapons or systems of weapons can be used to cause some form of damage or intended effect through implementation or action against a specified target. It is also generally understood what effects and targets represent. Without changing the basic understanding of terms, the concept of fires or effects can be applied to actions that create effects both in and out of cyberspace.

Maneuver as a Metaphor

The same analysis can be applied to the concept of maneuver, which joint doctrine defines as, "Employment of forces in the operational area, through movement in combination with fires and information, to achieve a position of advantage in respect to the enemy."[52] An offensive action common to the land domain such as an infantry platoon conducting an assault on an enemy machine gun position within its unit's battlespace with clear fields of fire can be easily applied to the maneuver definition to serve as a baseline for the land domain. The platoon represents the forces in the operational area, which starts at a position of disadvantage to the enemy as soon as it comes into contact. The platoon immediately takes cover to preserve combat power. If the platoon conducts a movement directly towards the enemy position, the result will

most likely be failure. However, if the platoon utilizes a squad in a support by fire position in conjunction with organic fires such as a mortar system to suppress or keep the machine gun nest focused on them, a separate squad may be able to break contact and conduct a coordinated movement against the enemy position from an avenue outside of the enemy's field of fire. Thus, through movement and fires, the platoon has achieved a position of relative advantage over the enemy.

The term cyber or cyberspace, when used as a modifier to the maneuver concept preserves some interactional properties of maneuver, while negating others. Forces is negated conceptually because the perception of a platoon in cyberspace does not exist in the same way as it does in the land domain. To make forces work for cyberspace maneuver, the understanding of force must be modified, which exists as a point of confusion. For the land domain forces are clearly thought of as soldiers and the warfighting equipment that they bring to battle such as weapons and vehicles. While it is generally understood that cyber forces exist in terms of actual uniformed personnel in military formations, the application of forces to cyberspace requires one to think of forces not in terms of formations but capabilities.

The operational area is preserved without further modification given an individual understands the definition of cyberspace, the three-layer model of cyberspace as well as the joint doctrines classification of the different types of cyberspace, which are based off ownership. Movement is also negated because the action requires modification of ground tactical understanding of movement, which conceptually requires some type of physical change in position. Movement in the context of the infantry platoon entails physical change of a forces from one point to another. Actions within cyberspace are virtual and essentially invisible, which can be hard to conceptualize. The required modification of understanding to make this property

work is by thinking of movement in cyberspace as using capabilities in cyberspace to gain access to different layers of cyberspace in different types of networks rather than physical movement of forces in relation to a specific location.

Fires in cyberspace is generally preserved. Although most typically think of fires in the context of kinetic, destructive effects, the concept of non-lethal effects or fires is not new and is often used interchangeably in common military lexicon with effects. In cyberspace, the use of fires as previously established refers to those cyberspace attack actions that produce denial effects such as degrading, disrupting, destroying a target which can occur in cyberspace.[53] While these effects are sometimes noticeable in the physical domain through manipulation of the physical network layer, in the conduct of a cyber maneuver in cyberspace alone, the use of denial producing effects to enable some sort of cyberspace action is understandable. "Positional advantage" is also preserved as an interactional property for maneuver in cyberspace, but only after necessary modification to the understanding of forces and movement.

At echelons of above reality, both fires and maneuver metaphors can be useful for understanding cyberspace operations from the perspective of the cyberspace forces. However, the use of maneuver becomes a distraction when discussing operations in a cross-domain context from the perspective of the tactical Army. Conversely, fires as a concept is easily translatable and can be applied to describe effects in or out of cyberspace without confusion at the operational and strategic levels of warfare from the perspective of both the tactical Army and the cyber forces. Through analysis of the interactional properties of maneuver and fires, the foundational concepts for each principle when modified to fit cyberspace have different degrees of effectiveness. Using the land domain as the baseline perspective for comparison of both principles shows that maneuver requires more adaptation from the original concept than fires.

The properties that negate the conceptual understanding of maneuver are forces and movement, which entail a level of physical permanence not relatable to cyberspace without further modification. The need for modification of terms further highlights gaps in existing doctrine.

Aaron Brantly, an advocate for the maneuver in cyberspace principle, offers a useful way of conceptualizing the various types of cyberspace operations based off where they begin in and end through a framework that can be described by either virtual standalone or a combination of virtual and physical with order of word denoting the origin of action.[54] Under this logic, the term virtual by itself refers to cyberspace actions not intended to produce effects outside of the domain, whereas virtual-physical cyberspace operations would originate in the cyberspace domain but produce noticeable effects in the physical domain. From the physical domain lens looking into cyberspace, if the joint cyberspace doctrine principles of maneuver and fires previously established are applied to this framework, virtual standalone operations could be both cyberspace attack or cyberspace exploitation actions (maneuver or fires), whereas virtual-physical operations would be cyberspace attack actions (fires).

Air Power for Strategic and Operational Cyberspace Effects

From the ground tactical lens looking up at the echelons above reality and higher levels of warfare, a useful framework already exists to view cyberspace operations in the way that the air domain provides operational and strategic fires or effects in support of the joint force to enable Army land dominance through ground maneuver. Air Force doctrine states that with respect to the relation of air power to the various levels of war, "Airmen should not define a given level by the specific weapons used, or on the targets attacked, but on the level of desired effects one wishes to create."[55] This goes in line with the common military saying that all tactical actions can have strategic effects. The Air Force, through air power, is less concerned on

conveying in military principle how it conducts the maneuver of a specific platform to deliver its weapon, and more focused on the effects of the weapon that it is delivering. Essentially, this is how the tactical Army should view both virtual and virtual-physical cyberspace operations for the operation and strategic levels. Simply stated, if the cyberspace action produces noticeable effects such as in a virtual-physical operation, then classify it as operational or strategic effects accordingly. If the cyberspace action produces no visible effects, such as in a virtual standalone operation, then the tactical Army should probably not be concerned with classifying it as anything unless it transitions to a virtual-physical operation.

Chapter 3 – The Tactical Lens

The tactical level of warfare is the point of departure at which discussing maneuver in cyberspace should be left in the cyber mission planning room and kept out of the discussion of ground operations. To understand the context through which the Army views tactical operations it is first necessary to establish what the tactical level is for the Army as well as what units the Army considers tactical. One can refer to the joint doctrinal definition, which describes the tactical level of warfare as the level, "[A]t which battles, and engagements are planned and executed to achieve military objectives assigned to tactical units or task forces.[56] In terms of large-scale combat operations (LSCO), the Army's tactical units reside at the corps level and below with its brigade combat teams (BCT), functional and multi-functional brigades.

As a combined arms maneuver formation, the BCT is generally viewed as the building block under which corps and divisions conduct tactical operations. The corps is primarily focused on driving the operational level of warfare but also serves as a bridge between the operational and tactical level as it is generally viewed as the highest level of echelon with the capability to direct tactical operations. While tactical operations are not the corps primary mission, the capability exists for the corps to assume tactical command and control over an independent brigade or task force, thought the likelihood of this happening would likely be limited to the conduct of a rear area security or quick reaction force mission. Although the corps and its subordinate formations are comprised of a host of functional and multi-functional brigades such air defense artillery (ADA) brigades, field artillery (FA) brigades, and aviation brigades, the BCT is the primary vehicle through which the Army conducts tactical maneuver to achieve its mission. Actions in cyberspace at the tactical level, whether they are offensive or defensive, are better viewed through the function that they support the BCT such as fires or effects. The Army already does

this in many ways with the application of other lethal and non-lethal capabilities which operate across domains.

Air-ground Operations and Ground Maneuver

The air domain is an example of a dimension with cross-domain capabilities that are generally not useful to discuss in terms of maneuver at the Army tactical ground level. One way in which the Army already conceptualizes the tactical actions of the air domain as support to maneuver in the land domain can be seen through the way it employs organic air assets in attacks against enemy forces in close friendly contact.[57] The utilization of rotary wing aviation in this case is viewed as fires or effects rather than independent maneuver. In a close combat situation, the ground commander in contact with the enemy communicates the desired effect for the aviation asset to bring against the enemy through a Joint Forward Observer (JFO) utilizing the standard five-line Army call for fire format. Upon receipt of the call for fire, the aviation asset conducts the attack and transitions to follow on tasks.

On the other hand, one might point out that Army aviation is also capable of operating in the other warfighting functions to support ground force objectives and even conducts maneuver on its own as a part of the ground commander's operation.[58] However, tactical aviation maneuver is only recognized as "maneuver" in the combined arms team where it can conduct the same actions as the ground tactical formation. For example, Army aviation operates in a maneuver role while conducting air-ground operations (AGO) by executing certain offensive and security tasks such as movement to contact, attack, reconnaissance, screen, and guard.[59] In the case of the previously mentioned tasks, it is suitable to discuss aviation maneuver in the same way as ground tactical maneuver as opposed to fires if it is understood that proximity to friendly forces is the limiting factor. Army aviation assets operating beyond the tactical reach of the

ground tactical unit's forward line of own troops (FLOT) or within the confines of its own boundaries set by air or movement control measures are maneuver.

The case of rotary wing aviation maneuver at the tactical level shows how a given capability can produce both fires and maneuver while operating in multiple domains. The classification of whether the capability is maneuver or effects largely depends on the perspective of the stakeholder in the fight. A tactical aviation formation undoubtedly performs maneuver functions in the air domain as it positions relative to both enemy and friendly ground formations to prosecute rotary wing calls for fire. If the stakeholder is the aviation unit, the aspect of maneuver in the air domain matters more than it does to the tactical ground formation from who's perspective the effects produced are fires in the land domain. In the same regards, a cyber force conducting a cyberspace attack with the intent to produce fires in the land domain in support of a tactical ground formation may view its actions in cyberspace as conducting maneuver to achieve a position in which the effect can be delivered but viewing the action as fires matters more to the tactical ground formation. Ultimately, the air domain differs from cyberspace from the perspective of the tactical ground commander only in cases where rotary wing aviation can essentially replicate the same types of maneuver tasks that the ground formation can conduct. In these limited cases, such as the screen or the guard, this perspective of maneuver matters to the tactical ground unit because the task can be directly assumed or transitioned between the ground unit or the air unit. However, there are no cross-domain capabilities originating from cyberspace that have the ability mimic a one for one maneuver task in the land domain for the tactical ground unit, which cements why the discussion of maneuver in cyberspace is distracting from the perspective of the land domain.

Tactical Ground Maneuver Can Support Cyber Operations

While the tactical level Army unit will most likely view cyberspace capabilities in terms of the effects produced to support ground tactical operations, there is the opportunity for the ground tactical unit to support independent operations in the cyberspace domain. Offensive cyber operations commonly consist of cyberspace exploitation and cyberspace attack, both of which require what Herb Linn categorizes as, "[A] vulnerability, access to that vulnerability, and a payload to execute."[60] According to cyberspace doctrine, the exploitation action is maneuver and the attack is fires, with the difference lying in what Linn describes as the intent of the payload.[6162] A tactical ground unit could be involved in this type of cyberspace operation by assisting cyber forces in gaining access to the intended system on which they will carry out the cyber payload.

There are generally two ways to gain access when conducting an offensive cyberspace operation. The first means is referred to as 'remote access' and can be accomplished from anywhere physically if access to the outside networks such as the internet is available to introduce a vulnerability.[63] Cyberspace operations involving remote access occur transparent of ground tactical forces and are typically unnoticed unless the operation provided a specific effect noticeable to the ground commander's operation. The second method is 'close access' and differs from the first in fact that close proximity to the network or system is required to employ the vulnerability or payload.[64] In the even of a close access situation, a tactical ground tactical unit could potentially be utilized to locally assist the cyber forces in gaining access. However, to the tactical ground unit this action would only be viewed as a separate mission task. The maneuver unit would not be involved in the cyber planning room.

Cyberspace Operations Support Ground Tactical Operations as Fires or Effects

There is currently no way for a tactical commander to command-and-control actions in cyberspace in real time at the tactical level, nor does the tactical commander have organic cyberspace capabilities at his or her disposal. Absent of these circumstances, the commander is relegated to utilizing the cyber and electronic warfare request format (CERF) to request effects.[65] This is a reach back tool that occurs during planning of the operation like the joint tactical air support request (JTAR) used to request close air support.[66]

Current Army doctrine employs cyberspace actions as fires or effects at the tactical level. At the level of warfare where U.S. Army forces are engaged in close combat, the analogies of maneuver in cyberspace are confusing and not helpful to the combined arms maneuver fight, no more than the infantry platoon leader should be thinking about how an artillery round is flying through the sky, and thus the air domain once he directs a forward observer to call for fire. The control measures, detailed integration, and control of where the round goes matter but not how it gets to the target. As the Army works to bring organic cyberspace capabilities to the tactical level of war, the importance of the effect provided by the capability will continue to be more important than the technical aspect of how it occurs, unless the use of ground forces is required to assist in gaining access to the intended target network or system through close proximity. For the cyberspace domain in general, the principles of warfare, specifically in the case of maneuver, may serve as useful framework for the conceptualization and planning of missions independent of other domains or at higher levels of warfare.

Chapter 4 – Conclusion

Analogies and metaphors are useful until they are not. The implementation of maneuver as an analogy to understand cyberspace was useful until the Army decided to integrate cyberspace capabilities into tactical operations. The use of fires analogies and metaphors serve more purpose for cross-domain concepts than maneuver. If multi-domain operations is the way forward, a clear line should be drawn on the matter of cross-domain maneuver at the tactical level to exclude the use of cyber maneuver. Whether the Army continues to push maneuver in cyberspace as a principle through the cross-domain maneuver and multi-domain operations concepts or accepts the fires or effects-based analogies remains to be seen. If maneuver analogies for cyberspace do persist, a hard look at current and future doctrine must occur to ensure that definitions are updated to clearly delineate what has changed.

One thing is for certain, the importance of cyberspace in current and future military operations will continue to increase. The Army is making strides to incorporate tactical cyberspace capabilities at the division level and below with through its experimental multi-domain task force and its already operational expeditionary cyber teams. However, a relook at the current organization of the brigade combat team is necessary. For example, by cutting out the third infantry battalion from each BCT, the Army could free up approximately 780 positions per brigade, which would provide the opportunity to add organic cyberspace and other cross-domain capabilities that are currently absent.[67] The multi-domain task force is still in testing while the Army only has one operational unit capable of deploying expeditionary cyber teams in the 915th Cyber Warfare Support Battalion. If tactical cyber units remain experimental, limited in number, and not organic to tactical ground units they will be perceived at echelons above reality.

Notes

[1] US Army, *Doctrine Primer,* ADP 1-01, Washington, DC, July 2019, V.
[2] Foreword, US Army TRADOC, TRADOC Pamphlet 5-25-3-1, *The U.S. Army in Multi-Domain Operations 2028*, Fort Eustis, VA, US Army TRADOC December 2018.
[3] US Army TRADOC, TRADOC Pamphlet 5-25-3-1, *The U.S. Army in Multi-Domain Operations 2028*, Fort Eustis, VA, December 2018, C-1.
[4] Joint Chiefs of Staff, Cyber*space Operations,* JP 3-12 [R], Washington, DC: Joint Chiefs of Staff, February 5, 2013.
[5] Glenn Takemoto, "Information Warfare in the Cyber Domain," USAWC Strategic Research Project, AY 2001, https://apps.dtic.mil/sti/pdfs/ADA389750.pdf WE KNOW THE ACTUAL DATE OF PUBLICATION
[6]Joint Chiefs of Staff, *Information Operations*, JP 3-13, Washington, DC: Joint Chiefs of Staff, October 9, 1998, I-10 – I11.
[7] Joint Chiefs of Staff, *Joint Operations*, JP 3-0, Washington, DC: Joint Chiefs of Staff, September 10, 2001, III-31.
[8] Joint Chiefs of Staff, *Joint Operations*, JP 3-0, Washington, DC: Joint Chiefs of Staff, September 10, 2001, III-31.
[9] Joint Chiefs of Staff, *Joint Operations*, JP 3-0, Washington, DC: Joint Chiefs of Staff, September 17, 2006, xi.
[10] Joint Chiefs of Staff, *2004 National Military Strategy*, Washington, DC: Joint Chiefs of Staff, 2004, 18.
[11] Joint Chiefs of Staff, *2004 National Military Strategy*, Washington, DC: Joint Chiefs of Staff, 2004, 14.
[12] Michael V. Hayden quoted in, Martin C. Libicki, "Cyberspace is Not a Warfighting Domain," *I/S: A Journal of Law and Policy for the Information Society*, vol. 8, no. 2 (2012), 321.
[13] Martin C. Libicki, "Cyberspace is Not a Warfighting Domain," *I/S: A Journal of Law and Policy for the Information Society*, vol. 8, no. 2 (2012), 321-336.
[14] Martin C. Libicki, "Cyberspace is Not a Warfighting Domain," *I/S: A Journal of Law and Policy for the Information Society*, vol. 8, no. 2 (2012), 321-336.
[15] Martin C. Libicki, "Cyberspace is Not a Warfighting Domain," *I/S: A Journal of Law and Policy for the Information Society*, vol. 8, no. 2 (2012), 332.
[16] Chris McGuffin and Paul Mitchell, "On Domains: Cyber and the Practice of Warfare," *International Journal*, vol. 69, no. 3 (2014), 394-412.
[17] Chris McGuffin and Paul Mitchell, "On Domains: Cyber and the Practice of Warfare," *International Journal*, vol. 69, no. 3 (2014), 394-412.
[18] Chris McGuffin and Paul Mitchell, "On Domains: Cyber and the Practice of Warfare," *International Journal*, vol. 69, no. 3 (2014), 394-412.
[19] John J. Yeosock, "Army Operations in the Gulf Theater," *Military Review,* September 1991, 3, quoted in, Kelvin Crow and Joe R. Bailey, ed., *Essential to Success: Historical Cases Studies in the Art of Command at Echelons Above Brigade* (Fort Leavenworth, KS: The Army University Press, 2017), 251, https://www.armyupress.army.mil/Portals/7/combat-studies-institute/csi-books/essential-to-success-historical-case-studies-in-the-art-of-command-at-echelons-above-brigade.pdf
[20] John J. Yeosock, "Army Operations in the Gulf Theater," *Military Review,* September 1991, 3, quoted in, Kelvin Crow and Joe R. Bailey, ed., *Essential to Success: Historical Cases Studies in the Art of Command at Echelons Above Brigade* (Fort Leavenworth, KS: The Army University Press, 2017), 251, https://www.armyupress.army.mil/Portals/7/combat-studies-institute/csi-books/essential-to-success-historical-case-studies-in-the-art-of-command-at-echelons-above-brigade.pdf
[21] Joint Chiefs of Staff, *Joint Operations*, JP 3-0, Washington, DC: Joint Chiefs of Staff, January 17, 2017, I-12.
[22] Joint Chiefs of Staff, *Joint Operations*, JP 3-0, Washington, DC: Joint Chiefs of Staff, January 17, 2017, I-13.
[23] Headquarters US Army, *The Army Vision,* 2018, Washington, DC: Headquarters US Army, 2018, https://www.army.mil/e2/downloads/rv7/vision/the_army_vision.pdf
[24] John Watts, Ben Jenson, JD Work, Nina Kollars, and Chris Whyte, *Alternate Cybersecurity Futures*, The Stowcraft Center for Strategy and Security, September 2019, https://www.atlanticcouncil.org/in-depth-research-reports/report/alternate-cybersecurity-futures/
[25] John Watts, Ben Jenson, JD Work, Nina Kollars, and Chris Whyte, *Alternate Cybersecurity Futures*, The Stowcraft Center for Strategy and Security, September 2019, https://www.atlanticcouncil.org/in-depth-research-reports/report/alternate-cybersecurity-futures/

[26] Mark Palmerleau, "How the Army is taking cyber units to the battlefield," IT And Networks (Blog), C4ISRNET, March 13, 2019, https://www.c4isrnet.com/dod/army/2019/03/13/how-the-army-is-taking-cyber-units-to-the-battlefield/
[27] U.S. Army Cyber Command, *Fact Sheet,* February 7, 2020, https://www.arcyber.army.mil/Portals/34/Fact%20Sheets/Cyber%20Mission%20Force/ARCYBER%20fact%20sheet%20-%20Cyber%20Mission%20Force%20(7Feb2020).pdf?ver=9hogFsBylRoHHLJ0oN2MAQ%3d%3d
[28] U.S. Army Cyber Command, *Fact Sheet,* February 7, 2020, https://www.arcyber.army.mil/Portals/34/Fact%20Sheets/Cyber%20Mission%20Force/ARCYBER%20fact%20sheet%20-%20Cyber%20Mission%20Force%20(7Feb2020).pdf?ver=9hogFsBylRoHHLJ0oN2MAQ%3d%3d
[29] Mark Palmerleau, "Here's how the US Army is planning tactical cyber operations," *AUSA* (Blog), C4ISRNET, October 9, 2020, https://www.c4isrnet.com/cyber/2020/10/09/heres-how-the-us-army-is-planning-tactical-cyber-operations/
[30] Joint Chiefs of Staff, *Cyberspace Operations*, JP 3-12, Washington, DC: Joint Chiefs of Staff, January 8, 2018, II-5.
[31] Joint Chiefs of Staff, *Cyberspace Operations*, JP 3-12, Washington, DC: Joint Chiefs of Staff, January 8, 2018, xii.
[32] Joint Chiefs of Staff, *Cyberspace Operations*, JP 3-12, Washington, DC: Joint Chiefs of Staff, January 8, 2018, II-11-II-12.
[33] Joint Chiefs of Staff, *Cyberspace Operations*, JP 3-12, Washington, DC: Joint Chiefs of Staff, January 8, 2018, II-11-II-13.
[34] Joint Chiefs of Staff, *Cyberspace Operations*, JP 3-12, Washington, DC: Joint Chiefs of Staff, January 8, 2018, II-7.
[35] Joint Chiefs of Staff, *Cyberspace Operations*, JP 3-12, Washington, DC: Joint Chiefs of Staff, January 8, 2018, I-4.
[36] US Army, *Cyberspace and Electronic Warfare Operations*, FM 3-12, Washington, DC, Department of the Army, April 2017.
[37] US Army, *Cyberspace and Electronic Warfare Operations*, FM 3-12, Washington, DC, Department of the Army, April 2017.
[38] National Research Council 2009, *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities* (Washington, DC: The National Academies Press, 2019), 26, https://doi.org/10.17226/12651.
[39] 14. Michael V. Hayden, "The Making of America's Cyberweapons," Christian Science Monitor, February 24, 2016, quoted in, Herbert Lin and Amy Zegart, ed., *Bytes, Bombs, and Spies: The Strategic Dimension of Offensive Cyberoperations* (Washington, DC: Brookings Institute Press, 2018), Kindle edition, 5.
[40] Joint Chiefs of Staff, *Cyberspace Operations*, JP 3-12, Washington, DC: Joint Chiefs of Staff, January 8, 2018, I-2.
[41] Joint Chiefs of Staff, *Cyberspace Operations*, JP 3-12, Washington, DC: Joint Chiefs of Staff, January 8, 2018, I-2.
[42] Joint Chiefs of Staff, *Cyberspace Operations*, JP 3-12, Washington, DC: Joint Chiefs of Staff, January 8, 2018, I-8.
[43] Jordan Branch, "What's in a Name? Metaphors and Cybersecurity," *International Organization,* vol. 75, no. 1, 2021, 39 https://www.cambridge.org/core/journals/international-organization/article/whats-in-a-name-metaphors-and-cybersecurity/563998100A2FAF1E5DFDB5C52EC68569
[44] Jordan Branch, "What's in a Name? Metaphors and Cybersecurity," *International Organization,* vol. 75, no. 1, 2021, 47, https://www.cambridge.org/core/journals/international-organization/article/whats-in-a-name-metaphors-and-cybersecurity/563998100A2FAF1E5DFDB5C52EC68569
[45] George Lakeoff and Mark Johnson, *Metaphors We Live By* (Chicago, IL: Chicago University Press, 1980, Afterword, 2003), Kindle edition, 11.
[46] Jordan Branch, "What's in a Name? Metaphors and Cybersecurity," *International Organization,* vol. 75, no. 1, 2021, 52, https://www.cambridge.org/core/journals/international-organization/article/whats-in-a-name-metaphors-and-cybersecurity/563998100A2FAF1E5DFDB5C52EC68569
[47] George Lakeoff and Mark Johnson, *Metaphors We Live By* (Chicago, IL: Chicago University Press, 1980, Afterword, 2003), Kindle edition, 110-114.
[48] George Lakeoff and Mark Johnson, *Metaphors We Live By* (Chicago, IL: Chicago University Press, 1980, Afterword, 2003), Kindle edition, 110.

[49] George Lakeoff and Mark Johnson, *Metaphors We Live By* (Chicago, IL: Chicago University Press, 1980, Afterword, 2003), Kindle edition, 110-111.
[50] Joint Chiefs of Staff, *Joint Operations*, JP 3-0, Washington, DC: Joint Chiefs of Staff, January 17, 2017, III-30.
[51] Joint Chiefs of Staff, *Joint Operations*, JP 3-0, Washington, DC: Joint Chiefs of Staff, January 17, 2017, GL-9.
[52] Joint Chiefs of Staff, *Joint Operations*, JP 3-0, Washington, DC: Joint Chiefs of Staff, January 17, 2017, III-38.
[53] Joint Chiefs of Staff, *Cyberspace Operations*, JP 3-12, Washington, DC: Joint Chiefs of Staff, January 8, 2018, II-7.
[54] Aaron F. Brantly, "Strategic Cyber Maneuver," *Small Wars Journal,* October 17, 2015, https://smallwarsjournal.com/jrnl/art/strategic-cyber-maneuver
[55] US Air Force, *Levels of War,* Volume 1 Basic Doctrine, Washington, DC: Department of the Air Force, February 27, 2015.
[56] Joint Chiefs of Staff, *Joint Operations*, JP 3-0, Washington, DC: Joint Chiefs of Staff, January 17, 2017, GL-16.
[57] Headquarters US Army, *Aviation Operations,* FM 3-04, Washington, DC, Headquarters US Army, April 2020, 3-4.
[58] Headquarters US Army, *Aviation Operations,* FM 3-04, Washington, DC, Headquarters US Army, April 2020, 1-2.
[59] Headquarters US Army, *Aviation Operations,* FM 3-04, Washington, DC, Headquarters US Army, April 2020, 1-3.
[60] Herb S. Linn, "Offensive Cyber Operations and the Use of Force," *Journal of National Security Law & Policy*, vol., no. 4. 63 (August 2010), 64, https://jnslp.com/wp-content/uploads/2010/08/06_Lin.pdf.
[61] Joint Chiefs of Staff, *Joint Operations*, JP 3-12, Washington, DC: Joint Chiefs of Staff, January 17, 2017, xii, II-6-II-7.
[62] Herb S. Linn, "Offensive Cyber Operations and the Use of Force," *Journal of National Security Law & Policy*, vol., no. 4. 63 (August 2010), 63, https://jnslp.com/wp-content/uploads/2010/08/06_Lin.pdf.
[63] Herb S. Linn, "Offensive Cyber Operations and the Use of Force," *Journal of National Security Law & Policy*, vol., no. 4. 63 (August 2010), 66, https://jnslp.com/wp-content/uploads/2010/08/06_Lin.pdf.
[64] Herb S. Linn, "Offensive Cyber Operations and the Use of Force," *Journal of National Security Law & Policy*, vol., no. 4. 63 (August 2010), 66, https://jnslp.com/wp-content/uploads/2010/08/06_Lin.pdf.
[65] Headquarters US Army, *Cyberspace and Electronic Warfare Operations*, FM 3-12, Washington, DC, Headquarters US Army, April 2017, C-1-C4.
[66] Joint Chiefs of Staff, *Close Air Support*, JP 3-09.3, Washington, DC: Joint Chiefs of Staff, June 10, 2017, A-1.
[67] Daniel Vasquez, "Is the Brigade Combat Team Becoming Obsolete?" *War on the Rocks,* April 17, 2020, https://warontherocks.com/2020/04/is-the-infantry-brigade-combat-team-becoming-obsolete/

Bibliography

Branch, Jordan. "What's in a Name? Metaphors and Cybersecurity." International Organization. vol. 75, no. 1, (2021), 39-70. https://www.cambridge.org/core/journals/international-organization/article/whats-in-a-name-metaphors-and-cybersecurity/563998100A2FAF1E5DFDB5C52EC68569

Brantly, Aaron F. "Strategic Cyber Maneuver." *Small Wars Journal.* October 17, 2015. https://smallwarsjournal.com/jrnl/art/strategic-cyber-maneuver

Crow, Kelvin and Joe R. Bailey, ed. *Essential to Success: Historical Cases Studies in the Art of Command at Echelons Above Brigade.* Fort Leavenworth, KS: The Army University Press, 2017. https://www.armyupress.army.mil/Portals/7/combat-studies-institute/csi-books/essential-to-success-historical-case-studies-in-the-art-of-command-at-echelons-above-brigade.pdf

Headquarters US Army. *Doctrine Primer.* ADP 1-01. Washington, DC, Headquarters US Army, July 2019.

Headquarters US Army. *The Army Vision, 2018*. Washington, DC, Headquarters US Army, 2018. https://www.army.mil/e2/downloads/rv7/vision/the_army_vision.pdf

Headquarters US Army. *Cyberspace and Electronic Warfare Operations*. FM 3-12. Washington, DC, Headquarters US Army, April 2017.

Headquarters US Army. *Aviation Operations.* FM 3-04, Washington, DC, Headquarters US Army, April 2020.

Joint Chiefs of Staff. *Information Operations.* JP 3-13. Washington, DC, Joint Chiefs of Staff, October 9, 1998.

Joint Chiefs of Staff. *Operations.* JP 3-0. Washington, DC, Joint Chiefs of Staff, September 10, 2001.

Joint Chiefs of Staff. *Operations.* JP 3-0. Washington, DC, Joint Chiefs of Staff, September 17, 2006.

Joint Chiefs of Staff. *Operations.* JP 3-0. Washington, DC, Joint Chiefs of Staff, December 17, 2017.

Joint Chiefs of Staff. *Cyberspace Operations.* JP 3-12 [R]. Washington, DC, Joint Chiefs of Staff, February 5, 2013.

Joint Chiefs of Staff. *Cyberspace Operations.* JP 3-12. Washington, DC, Joint Chiefs of Staff, January 8, 2018.

Joint Chiefs of Staff. *2004 National Military Strategy*. Washington, DC, Joint Chiefs of Staff, 2004.

Joint Chiefs of Staff. *Close Air Support*. JP 3-09.3. Washington, DC: Joint Chiefs of Staff, June 10, 2017.

Lakeoff, George and Mark Johnson. *Metaphors We Live.* Chicago, IL: Chicago University Press, 1980. Afterword, 2003. Kindle Edition.

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

Lin, Herbert and Amy Zegart, ed. *Bytes, Bombs, and Spies: The Strategic Dimension of Offensive Cyberoperations.* Washington, DC: Brookings Institute Press, 2018. Kindle edition.

Linn, Herb S. "Offensive Cyber Operations and the Use of Force." *Journal of National Security Law & Policy* vol., no. 4. 63 (August 2010), 63-86, https://jnslp.com/wp-content/uploads/2010/08/06_Lin.pdf

McGuffin, Chris and Paul Mitchell. "On Domains: Cyber and the Practice of Warfare," *International Journal.* vol. 69, no. 3 (2014), 394-412.

National Research Council 2009. *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities.* Washington, DC: The National Academies Press, 2019. https://doi.org/10.17226/12651.

Palmerleau, Mark. "How the Army is taking cyber units to the battlefield." IT And Networks (Blog). C4ISRNET, March 13, 2019. https://www.c4isrnet.com/dod/army/2019/03/13/how-the-army-is-taking-cyber-units-to-the-battlefield/

Palmerleau, Mark. "Here's how the US Army is planning tactical cyber operations." *AUSA* (Blog). C4ISRNET, October 9, 2020. https://www.c4isrnet.com/cyber/2020/10/09/heres-how-the-us-army-is-planning-tactical-cyber-operations/

Takimoto, Glenn. "Information Warfare in the Cyber Domain." USAWC Strategic Research Project, February 26, 2001. Defense Technical Information Center. https://apps.dtic.mil/sti/pdfs/ADA389750.pdf

US Air Force. *Levels of War.* Volume 1 Basic Doctrine. Washington, DC: US Air Force, February 27, 2015.

US Army Cyber Command, *Fact Sheet,* February 7, 2020, https://www.arcyber.army.mil/Portals/34/Fact%20Sheets/Cyber%20Mission%20Force/ARCYBER%20fact%20sheet%20-

%20Cyber%20Mission%20Force%20(7Feb2020).pdf?ver=9hogFsBylRoHHLJ0oN2MAQ%3d%3d

US Army TRADOC. *The Army in Multi-Domain Operations 2028.* TRADOC Pamphlet 525-3-1. Fort Eustis, VA, US ARMY TRADOC, December 2018.

Vasquez, Daniel. "Is the Brigade Combat Team Becoming Obsolete?" *War on the Rocks.* April 17, 2020. https://warontherocks.com/2020/04/is-the-infantry-brigade-combat-team-becoming-obsolete/

Watts, John, Ben Jenson, JD Work, Nina Kollars, and Chris Whyte. *Alternate Cyber Futures.* Washington, DC: The Stowcraft Center for Strategy and Security, September 2019. https://www.atlanticcouncil.org/in-depth-research-reports/report/alternate-cybersecurity-futures/