REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. **PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.**

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
04-06-2015	Future Warfare Research Paper	July 2014 - April 2015

4. TITLE AND SUBTITLE
Winning the Digital War: Understanding Maneuver Warfare in Cyberspace

5a. CONTRACT NUMBER
N/A

5b. GRANT NUMBER
N/A

5c. PROGRAM ELEMENT NUMBER
N/A

6. AUTHOR(S)
Walker Jr., Earlie H., Major, USMC

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 School Of Advanced Warfighting
Marine Corps University
3070 Moreel Avenue
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

In our modern world, there currently exist five defined domains where maneuver warfare tenets apply. These domains are land, air, maritime, space, and cyberspace. With the lethality and effects of today's weapons systems and budget constraints requiring smaller and more effective militaries, success in warfare requires the ability to conduct maneuver warfare. Conducting maneuver warfare successfully requires not only an understanding of the tenets of maneuver warfare, but the ability to maintain freedom of maneuver in all five domains. Maneuver warfare concepts permeate existing doctrine and recommendations exist for its application in the land, air, maritime, and space domains. Where then does cyberspace and maneuver warfare intertwine with respect to future war? More importantly, how does a commander achieve success in future war and maintain freedom of maneuver in cyberspace? This paper will study tenets of maneuver warfare and what the cyberspace domain looks like. Armed with those two foundations and using the tenets of maneuver warfare as a lens, this paper will then merge the layers of cyberspace, the three basic lines of operation in cyberspace, and ultimately discuss how the tenets of maneuver warfare apply in cyberspace.

15. SUBJECT TERMS
Maneuver Warfare, Cyberspace, Cyberspace operations, Maneuver Warfare in Cyberspace, Winning the Digital War

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE	UU	23	Marine Corps University/School of A
Unclass	Unclass	Unclass			19b. TELEPHONE NUMBER *(include area code)* (703) 432-5318 (Admin Office)

School of Advanced Warfighting

United States Marine Corps
School of Advanced Warfighting
Marine Corps University
3070 Moreell Avenue
Marine Corps Combat Development Command
Quantico, Virginia 22134

FUTURE WAR PAPER

TITLE:
Winning the Digital War: Understanding Maneuver Warfare in Cyberspace

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

AUTHOR:
Earlie H. Walker Jr.

AY 2014-15

Mentor: Dr. Brad Meyer
Approved: Bradley J. Meyer
Date: 20 April 2015

Executive Summary

Title: Winning the Digital War: Understanding Maneuver Warfare in Cyberspace

Author: Major Earlie H. Walker Jr., United States Marine Corps

Thesis: Success in future war requires planners and commanders to understand not only the nature of warfare and the tenets of maneuver warfare, but more importantly how the tenets of maneuver warfare apply when conducting operations in cyberspace.

Discussion: In our modern world, there currently exist five defined domains where maneuver warfare tenets apply. These domains are land, air, maritime, space, and cyberspace. With the lethality and effects of today's weapons systems and budget constraints requiring smaller and more effective militaries, success in warfare requires the ability to conduct maneuver warfare. Conducting maneuver warfare successfully requires not only an understanding of the tenets of maneuver warfare, but the ability to maintain freedom of maneuver in all five domains. Maneuver warfare concepts permeate existing doctrine and recommendations exist for its application in the land, air, maritime, and space domains. Where then does cyberspace and maneuver warfare intertwine with respect to future war? Since cyberspace arguably cuts across every warfighting function, the statement that we do not operate without cyberspace makes sense, but how do current and future commanders put that into perspective? More importantly, how does a commander achieve success in future war and maintain freedom of maneuver in cyberspace? This paper will study tenets of maneuver warfare and what the cyberspace domain looks like. Armed with those two foundations and using the tenets of maneuver warfare as a lens, this paper will then merge the layers of cyberspace, the three basic lines of operation in cyberspace, and ultimately discuss how the tenets of maneuver warfare apply in cyberspace.

Conclusion: Maneuver warfare concepts are still valid in cyberspace. Although, some of the traditional thought processes with maneuver warfare require slight adjustment, and the speed of most actions are greatly increased, there is no need to disregard maneuver warfare tenets. Speed, focus, surprise, center of gravity and critical vulnerabilities, combined arms, and decentralized command and control all still apply; however, the important part is learning what these tenets look like in the domain of cyberspace. Armed with this understanding and the knowledge that these concepts are valid should allow future planners and commanders quick adaptation when the unique nature of cyberspace requires adjustment.

DISCLAIMER

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

QUOTATION FROM, ABSTRACTION FROM, OR REPRODUCTION OF ALL OR ANY PART OF THIS DOCUMENT IS PERMITTED PROVIDED PROPER ACKNOWLEDGEMENT IS MADE.

Table of Contents Page

In defining war Clausewitz wrote, "War is nothing but a duel on a larger scale."[1], and "War is thus an act of force to compel our enemy to do our will."[2] Additionally, he wrote, "War is merely a continuation of policy by other means."[3] Such was the nature of war in Clausewitz's day, even though war during that period was fought predominately in two domains, land and maritime. The same premises remain true for the nature of war today, even though more domains exist.

In our modern world, there currently exist five defined domains where maneuver warfare tenets apply. These domains are land, air, maritime, space, and cyberspace. With the lethality and effects of today's weapons systems and budget constraints requiring smaller and more effective militaries, success in warfare requires the ability to conduct maneuver warfare. Conducting maneuver warfare successfully requires not only an understanding of the tenets of maneuver warfare, but the ability to maintain freedom of maneuver in all five domains.[4]

Maneuver warfare concepts permeate existing doctrine and recommendations exist for its application in the land, air, maritime, and space domains. Where then does cyberspace and maneuver warfare intertwine with respect to future war? Since cyberspace arguably cuts across every warfighting function, the statement that we do not operate without cyberspace makes sense, but how do current and future commanders put that into perspective? More importantly, how does a commander achieve success in future war and maintain freedom of maneuver in cyberspace? **Success in future war requires planners and commanders to understand not only the nature of warfare and the tenets of maneuver warfare, but more importantly how the tenets of maneuver warfare apply when conducting operations in cyberspace.**

To understand why the above statement is so requires that we will briefly review the tenets of maneuver warfare to ensure a shared understanding. Next, we will develop a shared understanding of what the cyberspace domain looks like. Armed with those two foundations and using the tenets of maneuver warfare as a lens, we will then merge the layers of cyberspace and the three basic lines of operation in cyberspace, and ultimately discuss how the tenets of maneuver warfare apply in cyberspace. Before digging into supporting this argument, there is one point that needs explanation. This author maintains that the nature of warfare remains unchanged, since defined by Clausewitz almost two centuries ago; therefore, when the reader sees the term warfare, the Clausewitzian definition applies. With this understanding in mind, we will now review the tenets of maneuver warfare.

MANEUVER WARFARE CONCEPTS

The overall goal of maneuver warfare is generating combat power at a decisive time and place to gain a position of advantage.[5] We are essentially attempting to create an asymmetry against the enemy system we are facing to achieve our objective. Therefore, to achieve this goal the major concepts considered in planning and executing maneuver warfare become offensive and defensive action. In the end, through either offensive action, defensive action, or a combination of the two, maneuver warfare seeks to tear apart the enemy system and if necessary destroy it to get to our desired endstate.

In considering the generation of combat power through maneuver there are several maneuver warfare tenets that require our understanding. Although terminology is very similar depending on which source you reference, this author will use as a source the tenets of maneuver warfare listed in Marine Corps Doctrinal Publication One (MCDP-1), Warfighting. The relevant supporting tenets for generating combat power, as referenced in MCDP-1, Warfighting, are

speed, focus, surprise, center of gravity and critical vulnerabilities, combined arms, and decentralized command and control.[6] Below is a brief description of each tenet to ensure a shared understanding.

Speed in maneuver warfare, sometimes called tempo, revolves around the decision making cycle of the enemy and the ability to dictate the terms of battle. Whether in space or time speed in maneuver warfare requires cycling through the decision making process faster than ones opponent. As this happens, the opponent progressively loses coherence in his actions and becomes overwhelmed.[7] This effort seeks to create or maintain an asymmetrical advantage over the enemy system. Therefore, using maneuver warfare in cyberspace to create an asymmetrical advantage requires the ability to conduct actions in cyberspace faster than an adversary does. Although, this may seem a straightforward premise, as we will explore later it is not that easy.

The next tenet, focus, refers to the focusing of efforts to achieve maximum effects. At all times efforts should focus on the enemy system to disrupt it and maintain any advantage already achieved by our actions. When an opportunity arises, focus should allow all supporting elements to generate maximum combat power at a prescribed time and place against a decisive point. Maintaining focus on the enemy system or more importantly vulnerable parts of it, allows decisive actions to occur. Done correctly, several focused actions can achieve cascading effects.

Another tenet of maneuver warfare is surprise. The purpose of surprise becomes to throw off an opponent to your real intentions in order to catch your opponent unprepared. This tenet, which seems simple, is sometimes hard to achieve. Most often achieving surprise requires some type of deception. According to Van Creveld, "Surprise can only be based on deception."[8]

Another tenet in maneuver warfare refers to a focused effort at the center of gravity, by identifying and exploiting critical vulnerabilities that allow the destruction or at a minimum the

neutralization of that center of gravity. The general thought process behind this tenet is that an enemy possesses a center of gravity that gives strength to his ability to resist our will. By identifying this center of gravity and then finding a fault line or critical vulnerability that will eliminate the center of gravity we can create an imbalance in the enemy's system and systematically unravel the enemy's ability to react.[9] Sometimes referred to as surfaces and gaps, the goal in maneuver warfare is to avoid surfaces and exploit gaps. Focusing combat power against a critical vulnerability or gap at the right time can have decisive effects.

Another important tenet in maneuver warfare is combined arms. The goal of this tenet is to create the greatest effect possible by combining the capabilities of multiple weapons systems against the enemy. The focus of this effort is to achieve the greatest effect or creation of a tactical asymmetry rather than focus on using the maximum firepower. The effect desired remains the unravelling of the enemy system and preventing his ability to react.[10] The goal is to create a "no win" situation for the enemy.

Finally, the last tenet of maneuver warfare we will discuss is decentralized command and control. Maneuver warfare seeks to create organizations capable of rapidly adapting to fleeting situations by using mission type orders, establishing purpose through well-understood commander's intent, and developing flexible units capable of creating and exploiting opportunities in any domain.[11] Although this type of command and control environment requires a shared thought process, developed through continuous training, when achieved it creates and organization very capable of executing maneuver warfare.[12]

This list of maneuver warfare tenets is not meant to be prescriptive, nor create the appearance that a formulistic process exists for maneuver warfare or warfare in cyberspace. With the above understanding, we have created a shared lens related to maneuver warfare that we can

now apply against elements of the cyberspace domain. Additionally, with that shared understanding, we should see that combining some of these tenets, such as "focus" and "surprise" could help facilitate others such as "speed". However, before we can apply the tenets of maneuver warfare against the elements of the cyberspace domain, we need to develop a shared understanding of what the cyberspace domain looks like.

THE CYBERSPACE DOMAIN AND THE LAYERS OF CYBERSPACE

Next, we will look at the domain of cyberspace. In the man-made domain of cyberspace, three layers exist. These layers are the physical network layer, the logical network layer, and the cyber-persona network layer. In this section, we will define the layers in cyberspace.

"Cyberspace is a global domain within the information environment consisting of multiple and interdependent networks of information technology infrastructures and resident data, including the internet, telecommunications networks, computer systems, and embedded processors and controllers. Cyberspace operations are the exercise of cyberspace capabilities to achieve objectives in or through cyberspace."[13] Cyberspace consists of three distinct but conceptually integrated layers physical, logical, and cyber-persona.

The physical network layer is the area in which data travels. It includes all transmission sources. "It is the focal point when determining jurisdiction and application of authorities."[14] The physical layer includes the geographic component and the physical network component. The geographic component is the physical location of the network components. While it remains easy to hurdle geopolitical boundaries in cyberspace at lightning speed, there is still a physical aspect tied to the other domains. The physical network component includes all the hardware and infrastructure that supports the network and the physical connectors (wires, cables, radio

frequency, routers, servers, and computers). The physical network layer is that part of the cyberspace domain that we can touch.

The logical network layer establishes how we view the physical network layer, depicting how nodes in the physical dimension of the information environment logically relate to one another to form entities in cyberspace. "The logical network layer is the first point where the connection to the physical dimension of the information environment is lost."[15] The logical layer contains the logical network component, which is technical in nature and consists of the logical connections that exist between network nodes. Nodes are any devices connected to a computer network. Nodes can be computers, cell phones, or various other network machines. On an Internet protocol (IP) network, a node is any device with an IP address.

The cyber-persona layer is the digital representation of individual or group online identities. The cyber persona component includes a person's identification or persona on the network (e-mail address, computer IP address, cell phone number, etc...). An individual can have multiple cyber personas (for example, different e-mail accounts on different computers) and a single cyber persona can have multiple users. Cyber-personas can be complex, with elements in many virtual locations and not necessarily linked to a single physical location or form.[16]

MERGING MANEUVER WARFARE AND CYBERSPACE

Now that we have a shared understanding of the tenets of maneuver warfare and what the cyberspace domain looks like we will merge the layers of cyberspace along three basic lines of operation in cyberspace. These three basic lines of operations are (DOD information network operations (DODIN ops), defensive cyberspace operations (DCO), and offensive cyber operations (OCO).[17] Ultimately, we will discuss how the tenets of maneuver warfare apply in cyberspace.

To begin let us define these three basic lines of operations (LOOs) directly from the J3 of U.S. Cyber Command.

> "DODIN operations are actions taken to design, build, configure, secure, operate, maintain, and sustain Department of Defense (DOD) communications systems and networks in a way that creates and preserves data availability, integrity, confidentiality, as well as user authentication and nonrepudiation. Defensive cyberspace operations are passive and active actions intended to preserve freedom of maneuver in cyberspace and apply cyberspace capabilities to protect data, networks, net-centric capabilities, and other designated systems. Offensive cyberspace operations use cyberspace capabilities in intentionally projecting power by the application of force in or through cyberspace. These form essentially two major objectives for cyberspace operations: Defensive maneuver in cyberspace (providing and maintaining freedom of maneuver in cyberspace, includes DODIN, DCO and Offensive maneuver in cyberspace (projecting power in and through cyberspace to achieve campaign objectives))."[18]

We will view each of these LOOs within the cyberspace domain through the lens of maneuver warfare.

Maneuver Warfare in Cyberspace (Speed, Focus, Surprise, COG, Combined Arms, C2)

The most obvious characteristic of maneuver is cyberspace is the speed at which actions occur. Actions in cyberspace are virtually instantaneous, happening at extremely fast computer speeds. The speed at which actions take place in cyberspace make it exceptionally hard to counter an effective attack. By the time detection of a successful attack occurs, most likely the adversary has already achieved their goal. Although, if detection and counteraction occurs in the midst of an attack, it is unlikely the attacker will be able to continue the attack successfully. In cyber operations, speed can allow one side to create and maintain an asymmetrical advantage, and successful maneuver allows both attacker and defender to penetrate their adversaries' decision loop rapidly.[19] In this case, any action that requires human decision or action will always occur at a slower speed. Speed is also relative to enemy actions and the actions of a system. Therefore, to defeat an enemy action one must act faster in relative terms. Then, using

the maneuver warfare tenant of speed in cyberspace, to create an asymmetrical advantage, requires the ability to conduct actions in cyberspace faster than an adversary does. Consequently, the two most obvious ways to win the speed race are operate faster than the adversary operates or impede adversary operations to a point where their actions are slower than your actions.

Maneuvering in cyberspace requires maintaining focus and connection to friendly, third party, and adversary systems identified as key terrain, and when required gain access to these systems in order to facilitate follow-on operations such as exploitation of data, system disruption or to create an asymmetrical advantage for follow-on cyberspace operations of operations in other domains.[20] Gaining control of systems is synonymous with shaping in a conventional operation. Essentially, it gives the attacker an advantage of being in the forward position close to the target network and ready to strike in order to set conditions for follow on operations.

Covertness and deception have become the symbols of most attacks in cyberspace. Every act that takes place in cyberspace is noticeable, although, most actions go undetected during occurrence. These attacks, normally detected after the fact, make reaction and the ability to counter surprise difficult. In cyberspace, attacks can rapidly build from a single system to thousands of systems with little or no warning to the target system. In cyberspace, attackers using botnets can quickly generate large-scale effects with surprise attacks such as distributed denial of service attacks (DDoS). This type of surprise attack occurred against Estonia in May of 2007, and although no additional military actions occurred, this event brought the most wired country in Europe down for over a week.[21]

Determining enemy and friendly strengths and weaknesses is and will remain a never-ending process. A strength today may be a weakness tomorrow based on changing technology. Continuous monitoring of key cyber terrain and capabilities can help mitigate this. Cyberspace

technology constantly evolves. This ongoing progression leads to continuous changes in the methods used by both attackers and defenders in cyberspace. Methods that work today may not work tomorrow due to new and unforeseen technological advances. In any case, when the time comes to maneuver in cyberspace, knowing the strengths and weaknesses of both friendly and enemy systems will be a requirement.

Knowing how cyberspace capabilities integrate with other weapons systems will be key to future operations in all domains. Since cyberspace touches every warfighting function, this integration will be key in achieving maximum effects against future adversaries. The dynamic effects of cyberspace capabilities coupled with other weapons systems may very well help achieve decisive effects.

"The preeminent Joint Force Commander requirement for freedom of maneuver in cyberspace is command and control. It is impossible to employ today's joint force without leveraging cyberspace."[22] Since the enemy's systems require command, control, and freedom of maneuver in cyberspace also, the ability to exploit the enemy system and limit his freedom of maneuver will have definite effects. Using cyberspace as maneuver space allows attackers and defenders to conduct actions simultaneously across multiple systems at multiple levels of warfare. These indirect effects, against an adversaries plan, can create serious dilemmas when attackers focus their attacks at multiple levels, generating tactical, operational, and strategic effects simultaneously.[23] Simply put, without command and control a force cannot maneuver and without operating effectively in cyberspace a force cannot command and control. Therefore, a force must first maneuver to defend (this includes counterattack) their network in cyberspace and once this is accomplished they can begin to maneuver offensively in cyberspace against their

adversary. Next, we will explore what offensive and defensive maneuver in cyberspace might look like.

Defensive Maneuver in Cyberspace (Defense in Depth, Moving Target Defense, Counter Attack)

To date, defensive maneuver in cyberspace generally resembles defensive operations in the other domains, with a few minor exceptions. Intrusion detection and defense-in-depth are almost conceptually identical in cyberspace to the other domains.[24] Many regard defensive operations in cyberspace as much more difficult than offensive cyberspace operations due to the perception that the attacker automatically has an asymmetric advantage.[25] This author disagrees with this argument. Using the tenets of maneuver warfare effectively to defend in cyberspace can create the conditions necessary to win the overall cyberspace fight. This does not mean that the defense has no offensive arm. To accomplish this one must create an effective defense in depth where encounters throughout the layers of the network are mutually supported by actions within the network.

Defense in Depth is a conventional term applied in cyberspace. Most organizations spend resources protecting their network with firewalls, intrusion detection systems and other defensive measures on the exterior and complete their defense in depth by hardening the interior of the network and individual systems. While defense in depth is a somewhat effective strategy just as in other domains, an enemy who spends the time and resources probing for vulnerabilities can exploit fixed targets with relatively static defenses.[26] Consequently, if there are seams, which inevitably there always are, the networks are vulnerable. However, using tenets of maneuver warfare organizations can design a network that possesses a mutually supporting defense in depth. Just as in conventional warfare, the defense can be designed where as an adversary moves

through the defense he must expose himself to other attributes of the defense. An example of this is gaining information from penetrations of the outer layers of the defense to help with the attribution fight. Once an anomaly is discovered, monitoring rather than immediately counterattacking can yield larger results. Therefore, once the who (adversary) is discovered, what if the attacker (focus) could be isolated in a box without knowing (surprise) and when ready the defender could counter-attack using a variety of exploitation, and, if necessary, destruction assets (combined arms) to defeat the adversary. Essentially, using the age-old adage of defense to wrest the initiative from the adversary and create the conditions necessary for offensive actions to win.

Moving Target Defense (MTD) is the concept of controlling change across multiple system dimensions in order to increase uncertainty and apparent complexity for attackers, reduce undetected exposure time, and increase the costs of probing and attack efforts. In conventional warfare, this concept is similar to the concept of mobile defense. During the 2008 cyber-attacks against Georgia, the Georgian government demonstrated a rudimentary form of the Moving Target Defense by relocating its primary sites on servers in several other allied countries.[27]

The Georgian government took an unconventional and unprecedented step of seeking refuge for its cyber capabilities in the U.S., Poland and Estonia. Within the U.S., Georgia located its cyber capabilities on servers with civilian companies in Atlanta, Ga., and California.[28] When Estonia underwent its cyberattack, it essentially conducted a static defense; Georgia, on the other hand, maneuvered. By employing defensive maneuver, unlike Estonia, Georgia was able to maintain key government services in the face of a massive denial of service attack, which was largely successful against its original Defense-in-Depth strategy.[29] The other unique point of the Georgia attack was that Russia maneuvered forces in conjunction with this cyberattack and

although never attributed directly to the Russian government, it is amazing how the Russian hacktivists conducted their cyberattack in synchronization with the Russian military maneuvers. Believing the coordination was just a coincidence requires a leap of faith; although, proving that is essentially impossible.

The counter attack is another form of defensive maneuver that resembles the conventional concept in the other domains. While the concept of a counter attack is relatively straight forward, the execution of a counter attack in cyberspace remains complicated due to the difficulty of attribution and the fact that many attacks originate from compromised, third party systems. To put it another way, in cyberspace counteraction may require shooting the hostage. Sometimes it may prove necessary to restore critical operations even at the cost of disabling or damaging a compromised third party system. However, by combining the tenets of maneuver warfare with the concepts of defense in depth and moving target defense, network defenders can create conditions to gain local superiority in cyberspace and in doing so set the conditions where their forces have the initiative. Consequently, once the initiative is seized offensive maneuver inside and outside of cyberspace can achieve the ultimate objectives.

Offensive Maneuver in Cyberspace

Offensive maneuver in cyberspace differs significantly from offensive operations in the other domains. While the goal of maneuver warfare, to secure asymmetrical advantages in respect to an adversary, remains consistent with maneuver warfare in the other domains, the speed at which maneuver actions occur vastly differs in cyberspace. This speed can give the offense a significant asymmetrical advantage in cyberspace.

Exploitation as a form of offensive maneuver in cyberspace attempts capturing information resources in order to gain a strategic, operational or tactical asymmetrical advantage.

Some refer to this form of operation as cyber espionage, but the use of this information in subsequent operations makes it an effective and potentially deadly form of offensive cyberspace maneuver.[30] In the cyberspace domain, the capture of key terrain (information) can lead to decisive results across all warfighting domains.

Once critical information resources are exposed, the originating entity often loses a significant competitive advantage and the gaining entity utilizes these resources for its own purposes. Over the course of the last decade, various nation-states have recognized the competitive advantage they can gain by harvesting the intellectual property and state secrets of competitor nations.[31] While this concept is not new, cyberspace has enabled the seizure and exploitation of information on an unmatched scale. Given that, information in cyberspace is critical key terrain, it makes sense that the processes involved in attacking and defending it must represent key forms of maneuver in cyber operations.

Additionally, offensive cyberspace maneuver attempts the process of gaining access to key physical network assets or logical network assets in cyberspace. Controlling these assets, which are most likely centers of gravity in the information and command and control environments, allow the attacker significant asymmetrical advantage during conflict, especially where combat operations in other domains are concerned.[32]

A prime example of this kind of maneuvering is the 2007 Israeli attack on a suspected nuclear reactor in Syria. Israeli attack aircraft managed to fly into Syria without alerting Syrian air defense systems to carry out this raid. Allegedly, this was accomplished through a combination of both electronic and cyber-attacks, which caused all of Syria's air defense radar systems to go offline for the duration of the raid.[33] The use of offensive cyberspace operations prior to the initiation of actual kinetic combat operations appears to have allowed Israel's success

and illustrates the potential decisive nature of this form of offensive operation in cyberspace, especially at the tactical and operational levels of war. Another example is Russia's attack on Georgia during the same year. Although, denied by the Russian Government, hacktivists acted in concert with Russian military actions, creating an asymmetrical advantage and paralyzing Georgian military responses. Although Georgia effectively maneuvered in cyberspace to maintain network services, the reduction of command and control and information flow decisively affected Georgia's overall ability to respond to the Russian threat.

CONCLUSION

In conclusion, success in future war requires planners and commanders to understand not only the nature of warfare and the tenets of maneuver warfare, but more importantly how the tenets of maneuver warfare apply when conducting operations in cyberspace. Maneuver warfare in cyberspace is set to challenge our traditional understanding of what a battlespace looks like. This in itself requires that commanders and planners at all levels understand where maneuver warfare and cyberspace intertwine.

The physical and non-physical characteristics of cyberspace make maneuver warfare theory an appropriate model for planning and operating in cyberspace. Consequently, understanding the weaponry and techniques used to conduct maneuver warfare in cyberspace remains essential. Commanders and planners must develop an expertise in cyberspace weaponry the same that exists for weapon systems employed in the four other domains.

One of the most dominant characteristics of maneuver in cyberspace is the fact that blatantly hostile acts occur with little or no recrimination against the initiator due to the difficulty of attribution. In many cases, similar acts in the other domains would elicit kinetic responses. As states around the world are building and developing cyberspace programs, understanding how

the principles of maneuver warfare apply to this new warfighting domain becomes increasingly important since it is these principles that planners and commanders use to develop strategy.

Maneuver warfare in cyberspace has a critical role, since cyberspace is an integral domain that supports and enables all warfighting functions. Maneuver warfare seeks to gain and maintain the initiative and exploit gained asymmetries to achieve tactical, operational and strategic objectives. While maneuver warfare in cyberspace has some unique differences from the other domains, its objective remains the same, to gain a position of advantage over an adversary and to leverage that position for decisive success. It is therefore important to continue to study and define the evolving principle of maneuver warfare in cyberspace to ensure the successful operations in this new warfighting domain.

Notes

[1]Carl Von Clausewitz. Edited by Michael Howard and Peter Paret. On War. Princeton University Press, Princeton, New Jersey, 1989. Pg. 75.
[2] Clausewitz. Pg. 75.
[3] Clausewitz Pg. 87.
[4] Brett T. Williams. "The Joint Force Commander's Guide to Cyberspace Operations." Joint Force Quarterly, Issue 73, 2nd Quarter 2014: Pg. 12.
[5] Martin Van Creveld with Steven L. Canby and Kenneth S. Bower. Air Power and Maneuver Warfare. Air War College, Air University, 1994. The following information from Van Creveld's book helps shed light on the subject of maneuver warfare for those who are not intimately familiar. "Before the fight, maneuver warfare seeks ways to place the enemy at a disadvantage by taking up favorable positions, or else by first taking on part of the enemy's forces within a limited area to obtain a subsequent advantage over the force as a whole. Once the fight is over, it seeks to take maximum advantage of the outcome by pursuing the enemy, keeping him off balance, and striking into his vitals." Pg. 1
[6] Headquarters U.S. Marine Corps. Warfighting. MCDP-1. Washington, DC.: Headquarters U.S. Marne Corps, June 20, 1997. Pgs. 72 – 96.
[7] Van Creveld "For maneuver warfare to be put into practice, the first vital element is tempo. Tempo is not the same as speed; Colonel John Boyd, perhaps best defined it, as the observation-orientation, decision, action cycle, sometimes called the OODA Loop. The idea is to get "inside the loop by transitioning from one mode of action to another before the other party can react. As this happens, the opponent progressively loses coherence in his actions. In ground combat; too, the idea is to move faster than the other can react and to react faster than the other can move. All this is done while aiming at fault lines in the opposing array." pg. 3
[8] Van Creveld "This is also a direct reference to Sun Tzu. "One must pretend to be at point A doing B while actually being at point C doing D; being at point C, one must pretend to be at point A doing B. pg. 4. "The purpose of all this maneuvering – which can be very complicated, time-consuming, and expensive—is to confuse the opponent, throw him of balance, and introduce an element of uncertainty into his plans. Once surprise is achieved, the dilemma becomes a question of attacking him with all the force one can muster." pg. 5
[9] Van Creveld "it is sometimes known as hitting the enemy at the right place and time with the most force. Discerning this fault line is not always easy, and much of this discernment is intuitive. A good analogy is a diamond cutter shattering a diamond by tapping it at exactly the right place in exactly the right direction with exactly the right amount of force. The artistic touch therefore consists of finding a spot that is both vital and weakly defended – a spot that, as the campaigns of the Great Captain show, can be found in almost any situation and under almost any circumstances. Next, that spot should be developed to systematically unravel the enemy's ability to react. pg. 3-4
[10] Van Creveld The modern combined arms team requires diversity. The value of combined arms is obtained from the coordination of the team's diversity, not in the sum of its firepower sources. pg. 6
[11] Van Creveld Because tempo, surprise, and combined arms all mean the rapid adaptation of available resources to a fleeting situation, the fifth cardinal element of maneuver warfare is flexibility. To be flexible, a military organization must be well rounded, self-contained and not too specialized. It must discourage excessive standardization of component parts and allow redundancy (which permits the organization to absorb hits without impairing its ability to function) and even allow some waste. Even when all of these structural elements are in place, the only factor that can guarantee flexibility is training and still more training. pg. 6
[12] Van Creveld "To those who are unfamiliar with its basic concepts, maneuver warfare often looks like some kind of secret magic whose objective is to obtain something for nothing. In fact, it is nothing of the kind; rather, it is based on the way we perceive the enemy and, by implication, the nature of our duel with

him. Its starting premise is that the enemy resembles us. Therefore, he needs to be approached not as an assembly of "targets" to be destroyed one by one, but as a living, intelligent entity capable of acting and reacting." Pg. 19.

[13] Headquarters U.S. Marine Corps. Marine Corps Cyberspace Operations. MCIP 3-40.2. Washington, DC.: Headquarters U.S. Marne Corps, October 06, 2014.pg. 1-2.

[14] MCIP 3-40.2 pg. 1-2.

[15] MCIP 3-40.2 pg. 1-2.

[16] MCIP 3-40.2 pg. 1-2.

[17] MCIP 3-40.2 pg. 1-3.

[18] Williams Pg. 14

[19] Jeppe Teglskov Jacobsen, "The cyberwar mirage and the utility of cyberattacks in war; How to make real use of Clausewitz in the age of cyberspace." DIIS Working Paper, Danish Institute for International Studies, June 2014. Pg. 11.

[20] Jacobsen Pg. 14

[21] Joshua Davis "Hackers Take Down the Most Wired Country In Europe" Wired Magazine Issue 15.09 August 21, 2007.

[22] Williams Pg. 12

[23] Williams Pg. 15

[24] Dawn Dunkerley and T.J. Samuele *Mike Meyers Certification Passport: Comp TIA Security +.* McGraw Hill Education, New York, New York, 2014 Chapter 8

[25]Huba Wass de Czege. "Warfare by Internet: the Logic of Strategic Deterrence, Defense, and Attack." Military Review (July-August 2010): pg 85.

[26] Dunkerley and Samuele Chapter 8

[27] Stephen W. Korns and Joshua E. Kastenberg. "Georgia's Cyber Left Hook." Parameters (Winter 2008-2009): Pg. 60.

[28] Korns Kastenberg Pg. 60.

[29] Korns and Kastenberg. Pg. 65.

[30] Jeffery Carr *Inside Cyber Warfare.* O'Reilly Media Inc., Sebastopol, CA 2012. Pg. 2

[31] Carr Pg. 4.

[32] Carr 8 – 11.

[33] Carr 251.

Bibliography

Barcomb, Chris E. "From Sea Power to Cyber Power: Learning from the Past to Craft a Strategy for the Future." Joint Force Quarterly, Issue 69 2nd Quarter 2013: 79-83.

Bowden, Mark. Worm: The First Digital World War. New York: Atlantic Monthly Press, 2011.

Brown, Gary D. "Why Iran Didn't Admit Stuxnet Was an Attack." Joint Force Quarterly, Issue 63, 4th Quarter 2011: 70-73.

Carr, Jeffery, Inside Cyber Warfare. O'Reilly Media Inc., Sebastopol, CA 2012.

Clausewitz, Carl Von. Edited by Michael Howard and Peter Paret. On War. Princeton University Press, Princeton, New Jersey, 1989.

Czege, Huba Wass de. "Warfare by Internet: the Logic of Strategic Deterrence, Defense, and Attack." Military Review (July-August 2010): 85-96.

Davis, Joshua "Hackers Take Down the Most Wired Country In Europe" Wired Magazine Issue 15.09 August 21, 2007.

Dunkerley, Dawn and T.J. Samuele "Mike Meyers Certification Passport: Comp TIA Security + McGraw Hill Education, New York, New York, 2014

"Hacktivisim: Cyberspace has Become the New Medium for Political Voices," White Paper, McAfee, May 2012. Pp. 18.

Headquarters U.S. Marine Corps. Warfighting. MCDP-1. Washington, DC.: Headquarters U.S. Marne Corps, June 20, 1997.

Headquarters U.S. Marine Corps. Marine Corps Cyberspace Operations. MCIP 3-40.2. Washington, DC.: Headquarters U.S. Marne Corps, October 06, 2014.

Hollis, David M. "Cyber War Case Study, Georgia 2008." Small Wars Journal. January 6, 2011.

Jacobsen, Jeppe Teglskov, "The cyberwar mirage and the utility of cyberattacks in war; How to make real use of Clausewitz in the age of cyberspace." DIIS Working Paper, Danish Institute for International Studies, June 2014.

Kallberg, Jan and Bhavani Thuraisingham, "Cyber Operations: Bridging from Concept to Cyber Superiority." Joint Force Quarterly, Issue 68, 1st Quarter 2013: 53-58.

Korns, Stephen W. and Joshua E. Kastenberg. "Georgia's Cyber Left Hook." Parameters (Winter 2008-2009): 60-76.

Libicki, Martin C. Conquest in Cyberspace. RAND Corp, Cambridge University Press, New York, New York, 2007.

Libicki, Martin C. "Cyberdeterrence and Cyberwar." RAND Corp, Prepared for the Air Force, 2009.

Lonsdale, David J. The Nature of War in the Information Age: Clausewitzian Future. Frank Cass Publishing, New York, New York. 2004.

Mayfield, Thomas D. III. "A Commander's Strategy for Social Media." Joint Force Quarterly, Issue 60, 1st Quarter 2011: 79-83.

Metz, Steven. "The Internet, New Media, and the Evolution of Insurgency." Parameters, Vol. XLII, No. 3 (Autumn 2012): 80-90.

Milevski, Lucas. "Stuxnet and Strategy: a Special Operation in Cyber Space?." Joint Force Quarterly, Issue 63, 4th Quarter 2011: 64-69.

Murphy, Matt. "War in the Fifth Domain: Are the Mouse and Keyboard the New Weapons of Conflict?" The Economist, July 1, 2010.

Shanahan, John, N.T. "Achieving Accountability in Cyberspace: Revolution or Evolution?" Joint Force Quarterly, Issue 73, 2nd Quarter 2014: 20-25.

Van Creveld, Martin with Steven L. Canby and Kenneth S. Bower. Air Power and Maneuver Warfare. Air War College, Air University, 1994.

Williams, Brett T. "The Joint Force Commander's Guide to Cyberspace Operations." Joint Force Quarterly, Issue 73, 2nd Quarter 2014: 12-19.