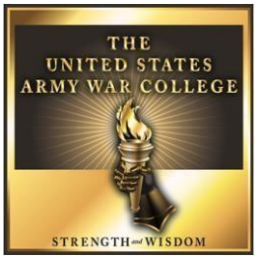
Strategy Research Project

On Cyber: Evolving Theory for Cyberspace

by

Mr. Jeffrey R. Jones
Department of the Army



United States Army War College
Class of 2015

REPORT DOCUMENTATION PAGE

Form Approved--OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
01-04-2015	STRATEGY RESEARCH PROJECT	

4. TITLE AND SUBTITLE
On Cyber: Evolving Theory for Cyberspace

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Mr. Jeffrey R. Jones
Department of the Army

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Professor Brian Gouker
Department of Military Strategy, Planning and Operations

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
U.S. Army War College, 122 Forbes Avenue, Carlisle, PA 17013

10. SPONSOR/MONITOR'S ACRONYM(S)

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

12. DISTRIBUTION / AVAILABILITY STATEMENT
Distribution A: Approved for Public Release. Distribution is Unlimited.

13. SUPPLEMENTARY NOTES
Word Count: 5065

14. ABSTRACT

Cyberspace is a man-made environment created through the evolution of technology. People, institutions, organizations, and governments across the globe use cyberspace as the primary enabler for global communications, shipping, commerce, and finance. Cyberspace is also the newest warfighting domain that supports, yet challenges, traditional modes of warfare and its practitioners. Countless theorists through the centuries, such as Clausewitz, Corbett, and Sun-Tzu, have offered military theories for waging war. However, a theory for fighting from and in cyberspace has yet to be developed. Cyberspace theory would guide and enhance the DoD's use of cyberspace in support of enterprise and military operations. For cyberspace to be truly used as a warfighting domain, it must be underpinned by theory in order to understand how to fight and win in the virtual space. Without a theoretic baseline, one will never know when to deviate from the norm and why. Evolving theories from classical theorists to create cyberspace theory will enable the DoD to effectively project cyberpower and gain the competitive advantage in cyberspace.

15. SUBJECT TERMS
Cyberspace Operations, Clausewitz, Corbett, Sun-Tzu

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			**19b. TELEPHONE NUMBER** *(w/ area code)*
UU	UU	UU	UU	31	

USAWC STRATEGY RESEARCH PROJECT

On Cyber: Evolving Theory for Cyberspace

by

Mr. Jeffrey R. Jones
Department of the Army

Professor Brian Gouker
Department of Military Strategy, Planning and Operations
Project Adviser

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

Abstract

Title:	On Cyber: Evolving Theory for Cyberspace
Report Date:	01 April 2015
Page Count:	31
Word Count:	5065
Key Terms:	Cyberspace Operations, Clausewitz, Corbett, Sun-Tzu
Classification:	Unclassified

Cyberspace is a man-made environment created through the evolution of technology. People, institutions, organizations, and governments across the globe use cyberspace as the primary enabler for global communications, shipping, commerce, and finance. Cyberspace is also the newest warfighting domain that supports, yet challenges, traditional modes of warfare and its practitioners. Countless theorists through the centuries, such as Clausewitz, Corbett, and Sun-Tzu, have offered military theories for waging war. However, a theory for fighting from and in cyberspace has yet to be developed. Cyberspace theory would guide and enhance the DoD's use of cyberspace in support of enterprise and military operations. For cyberspace to be truly used as a warfighting domain, it must be underpinned by theory in order to understand how to fight and win in the virtual space. Without a theoretic baseline, one will never know when to deviate from the norm and why. Evolving theories from classical theorists to create cyberspace theory will enable the DoD to effectively project cyberpower and gain the competitive advantage in cyberspace.

On Cyber: Evolving Theory for Cyberspace

> Theory offers the opportunity to roam freely back and forth between the general and the particular. In doing so, it can help one frame issues more broadly, ask questions more concisely, evaluate responses more discriminately, propose alternatives more imaginatively, investigate options more systematically, and arrive at accurate conclusions more rapidly.
>
> — Harold R. Winton[1]

Military theory has been around for centuries. Sun-Tzu's theory of war, captured in *The Art of War*, is widely read by military and non-military personnel, was written, by some accounts, in the sixth century BC.[2] Thucydides' description of the Peloponnesian War (431 – 405 BC) captured the Athenian view that war is waged because of fear, honor and interest, a theory that still holds true to this day.[3] Countless theorists through the ages, such as Clausewitz, Corbett, and Sun-Tzu, have offered theories for waging war. While some of these theories were discounted in the time in which they were written, some gain more value as time passes. The usefulness of centuries old theories is still debated, however, as Sir Julian Corbett so eloquently stated, "[t]heory will warn us the moment we begin to leave the beaten track, and enable us to decide with open eyes whether the divergence is necessary or justifiable."[4]

Cyberspace is the newest warfighting domain, and represents a technological revolution that supports, yet challenges, traditional modes of warfare and its practitioners. Succinctly, cyberspace is defined as, "[t]he notional environment in which communication over computer networks occurs."[5] Its modern implementation can be traced back to creation of the U.S. Advanced Research Projects Agency Network (ARPANET) in 1969. The ARPANET was originally designed to facilitate computer resource sharing by geographically dispersed researchers. However, the technologies

created to enable this functionality served as the starting point for what is now known as the Internet. The ARPANET started a revolution that changed the way the Department of Defense (DoD) and the world used computers.[6] However, over the past four decades, criminals and states alike have become very adept at exploiting the benefits provided by these technological advancements. The ease at which cyberspace capabilities can be created and wielded allows even individuals to threaten great harm on powerful nation-states. In essence, cyberspace is our strength and our Achilles heel. A theory for cyberspace would guide and enhance the DoD's use of cyberspace in support of enterprise and military operations. The lack of theory prevents the DoD from answering two critical questions: how do you operate in and fight from cyberspace, but more importantly, how do you win?

Fundamentals

Cyberspace is a man-made environment created through the evolution of technology. Even though the majority of people in the world still do not have Internet access, cyberspace is responsible for driving some of the most critical aspects of globalization and military modernization.[7] People, institutions, organizations, and governments across the globe use cyberspace as the primary enabler for global communications, shipping, commerce, and finance. These are made possible by the widespread technological advances attained since the first message passed through the ARPANET over forty years ago.

To better organize itself to support national security objectives, the DoD officially designated cyberspace as a warfighting domain in 2008.[8] It currently defines cyberspace as a "global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data,

including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."[9] In today's increasingly technological world, just about anything can be included in this definition. Since the 1960s, the DoD has become increasingly reliant on cyberspace for the effective employment of advanced weapon systems, global logistics and sustainment, as well as command and control. For instance, the F-4 Phantom jet fighter, originally introduced at the end of 1960, had only 8% of its internal operational enabled by software.[10] In contrast, the F-22 Raptor, introduced in 2005, is at least 80% reliant upon advanced computer technologies.[11] Further highlighting the DoD's reliance on cyberspace is the fact that it currently operates "over 15,000 networks and seven million computing devices" at installations across the globe "to enable its military, intelligence, and business operations, including the movement of personnel and material and the command and control of the full spectrum of military operations."[12] In essence, the DoD's ability to operate and project power around the globe is completely intertwined with cyberspace.

Cyberspace has a tremendous influence on all the warfighting domains, while being a domain itself. It serves as an enabler for people, systems and operations in the land, sea, air and space domains. Cyberspace is used to conduct stand-alone missions and actions, but its real power lies in the synergistic integration of cyberspace operations with activities in other warfighting domains to achieve national, strategic, operational or tactical objectives.[13] For instance, offensive cyberspace operations can be employed to disrupt enemy communications preceding a land-force attack. In addition, robust cyber defenses are employed to secure the DoD's extremely complex logistics system, thereby ensuring forces and materiel arrive at the right time. Military

cyberspace operations can be used for a myriad of options, which are composed of missions and enabling actions.

The U.S. Cyber Command and its Service Components conduct missions within cyberspace. These missions are composed of DoD Information Network (DoDIN) Operations (DoDIN Ops), Defensive Cyberspace Operations (DCO) and Offensive Cyberspace Operations (OCO). Each of these missions is categorized by intent, should not be considered separate and distinct from each other, and must be integrated and synchronized to be effective.[14]

The intent of DoDIN Ops is to design, build, configure, secure, operate, maintain and sustain the DoD's networks, creating a protected operating environment, which preserves the confidentiality, integrity and availability of its data.[15] DoDIN Ops are performed on a daily basis by a variety of personnel in the Services and Joint communities. A recent, ongoing example of DoDIN Ops is the design, configuration, installation, and operation of the Joint Information Environment (JIE). The JIE is a DoD effort to consolidate and standardize many of the disparate networks used by the Services today.[16] In essence, the DoDIN Ops mission provides assured access to the DoD's portion of cyberspace, as defined and desired in the DoD's Joint Operational Access Concept (JOAC).[17]

DCO is intended to defend the DoDIN or other supported networks through passive and active defensive measures.[18] DCO's goal is to create and maintain an environment conducive to friendly maneuver, while denying freedom of action to the adversaries.[19] DCO also encompasses two sub-mission areas. The first is internal defensive measures (DCO-IDM) conducted on friendly networks to secure them from

intentional attacks, as well as actively hunting for threat actors who have bypassed the network's perimeter security.[20] The second is response actions (DCO-RA), which is conducted outside of the DoDIN boundaries and involve deliberate actions, such as the implementation of countermeasures, to directly counter specific threats to the network.[21] The DCO mission set is analogous to performing anti-access and area-denial as defined in the JOAC, but within cyberspace.[22]

DoDIN Ops and DCO share similar aspects with respect to creating and maintaining a secure operating environment. DoDIN Ops' responsibility to *secure* is often confused with DCO's *defend* mission, but can be easily explained using the concept of defensive information warfare espoused by Dorothy Denning in 1999. One purpose of DoDIN Ops is to secure the network, which is done in response to unintentional threats, such as software vulnerabilities or human error.[23] DCO's primary purpose is to defend networks, which is done in response to intentional attacks by third parties or insider threats.[24]

The final mission set within cyberspace operations is OCO, which is "… intended to project power by the application of force in and through cyberspace,"[25] to deliver lethal or non-lethal effects. For instance, the destruction of data (non-lethal effect) on a single computer system may only affect the normal operation of that system. However, an attack such as Stuxnet, which exploited vulnerabilities in Iran's industrial control systems (ICS) and supervisory control and data acquisition (SCADA), modified different computer systems (non-lethal effects) resulting in the physical destruction (lethal effects) of Iran's nuclear centrifuges.[26]

Cyberspace actions executed in support of the DoDIN Ops, DCO and OCO mission areas are focused on the application of capabilities to deliver specific effects.[27] These actions include: cyberspace defense; cyberspace intelligence, surveillance and reconnaissance (ISR); cyberspace operational preparation of the environment (OPE); and cyberspace attack. Defensive actions are primarily used to support DoDIN Ops and DCO, focusing on protecting against, detecting, characterizing, countering and mitigating the threat.[28] ISR and OPE primarily support offensive and defensive cyberspace operations. ISR is focused on intelligence activities to gather information from a target network, while OPE are those non-traditional intelligence activities to gather information about a network or systems.[29] Finally, cyberspace attacks support OCO and DCO-RA, and are those executed to deny, disrupt, degrade, destroy or manipulate targets.[30]

The missions and actions composing cyberspace operations enable the DoD and the U.S. to project cyberpower. Cyberpower is "the ability to use cyberspace to create advantages and influence events in all the operational environments and across the instruments of power."[31] To effectively and efficiently project cyberpower, these missions and actions must be integrated and synchronized with each other and with efforts in other domains. Cyberspace operations are executed during all six phases of military operations. Intelligence (ISR) and information gathering operations (OPE) are conducted throughout the six phases to ensure operators are prepared for all planned and contingency operations. DoDIN operations and the passive portions of DCO efforts are primarily focused on shaping (phase 0), deterring (phase 1), stabilization (phase 4) and enabling civil authority (phase 5). Actively defending networks via DCO mainly

occurs during deterrence, seizing the initiative (phase 2), dominating the environment (phase 3), but are also utilized during stability operations. Similarly, OCO is mainly focused on deterrence, seizing the initiative and domination. In essence, the DoD leverages the virtual domain to conduct cyberspace operations throughout the continuum of military operations to wield cyberpower in support of the commander's objectives. Theory will help establish a baseline for the precise use of these operations and this power.

The Need for Theory and the Applicability of Theorists

Technology has changed the way the world interacts and the way wars are fought. Incorporating various technologies into the DoD's operational and enterprise environments facilitates gathering, storing, analyzing, sharing and acting on information in a way only imagined in science fiction novels of yore. Information is power. It is an instrument of national power and a catalyst for transformation in the physical and virtual domains. Information also enhances the destructive and disruptive capabilities of the armed forces.[32] Cyberspace leverages technology to exchange information. Learning to use cyberspace to enable the projection of power, or information, makes theory definition a requirement sooner rather than later. Cyberspace is its own warfighting domain in which, arguably, different variations of war are fought today. It also enables information exchange and technology incorporation in all other domains. Due to these facts, it would be irresponsible not to apply the intellectual constructs of war from classical theorists addressing other warfighting domains to cyberspace and the projection of cyberpower.

Given that the U.S. and its military are increasingly reliant upon the benefits of cyberspace, the first question to address is why there should be a theory in the first

place. In fact, this question was addressed recently by Martin Libicki, PhD., visiting professor at the U.S. Naval War College, who opined that speed of operations and change in this domain prevent theory from making more than a modest impact.[33] In fact, it could be said that professionals conducting operations within this domain would hold a similar opinion, simply based on the speed at which they must make decisions. However, these opinions are extremely shortsighted.

The argument regarding the need for theory in a domain is not unique to cyberspace. Every domain has had a period of time during which there was no guiding theory to drive how to strategically leverage the domain during war and peace. Theory is defined as a "set of principles on which the practice of an activity is based."[34] This leads to the hypothesis that a domain should have theory to adequately define what can and should be done to operate effectively and efficiently. Exploring the validity of this hypothesis through the lens of classical military theorists leads to Carl von Clausewitz. Clausewitz eloquently stated in his seminal work *On War*:

> Theory cannot equip the mind with formulas for solving problems, nor can it mark the narrow path on which the sole solution is supposed to lit by planting a hedge of principles on either side. But it can give the mind insight into the great mass of phenomena and of their relationships, then leave it free to rise into the higher realms of action.[35]

Succinctly, while theory does not provide answers to all imaginable questions, it provides strategists, operators and decision makers a common, general baseline of understanding. It also permits the individual engaged in thought on the subject an opportunity to expand on the theory to determine how it applies to the situation at hand, hence enhancing his or her military judgment.[36] Even more importantly, in the age of dwindling resources within the DoD, a theory for cyberspace should help ensure that the nation's resources and military power are effectively and efficiently applied.[37] Finally,

having theory that is applied and well understood allows an individual to comprehend the political and human dimensions of warfare within cyberspace, which is extremely critical given its pervasiveness.[38] While traditional theory does not apply in total, it equips one with the insight into the relationship between cyberspace and the other warfighting domains, possibly leading to multiple evolutions of theory.

Although it is debatable whether the day-to-day operations conducted within cyberspace alone constitute war, theoretical constructs penned by Carl von Clausewitz can be practically applied. Clausewitz is one of the preeminent land warfare theorists, by which many aspects of war are still measured. Concisely, he viewed war as a continuation of policy, involving violence, chance and reason, waged with force to compel the enemy to do our will.[39] A brief examination of war's components will demonstrate that it is reasonable to apply existing military theory to cyberspace.

As it relates policy and reason for war, one needs look no further than the U.S. National Security Strategy, which designates the nation's critical, digital infrastructure a strategic national asset and a national security priority to protect.[40] The DoD further directs that it will defend itself and its networks against enemy actions in cyberspace, conduct cyberspace operations outside of the U.S., as well as defend government and critical networks as required.[41] Therefore, all cyberspace operations conducted by the DoD or U.S. Government, whether building secure networks, defending those same networks, or conducting offensive cyberspace operations (OCO), are firmly rooted as an extension of policies and politics.

The use of force and violence to compel an enemy requires a more liberal interpretation of Clausewitz. Given the character of war in Clausewitz's era, his theory,

as written, dealt with physical force and primordial violence during the conduct of war.[42] Today, force is "strength or power exerted upon an object …"[43] Furthermore, violence is "[t]he intentional use of physical force or power, threatened or actual, that either results in or has a high likelihood of resulting in injury, death, psychological harm, maldevelopment or deprivation."[44] Given these definitions, it is not difficult to conclude that force and violence are just as applicable in the virtual realm as it is in the physical.

Cyber attacks, or OCO in the DoD's parlance, are the easiest mission area to demonstrate the application of force through cyberspace. As stated previously, OCO in the DoD is the "…project[ion of] power by the application of force in or through cyberspace."[45] Leveraging this virtual domain, force is applied through technical capabilities to disrupt, degrade, deny, destroy or manipulate target networks or systems. Attack effects can be non-lethal and constrained solely to the virtual domain, or have lethal effects in the physical domains.

Stuxnet is a prime example of physical force and violence applied virtually. Stuxnet is malicious software created and employed by unknown actors against Iran's Natanz nuclear facility. Once installed on computers residing in the facility, the software modified the machines controlling Iran's nuclear centrifuges. Assessments estimate that Stuxnet, software deployed through cyberspace, caused the physical destruction of approximately one-fifth of Iran's nuclear centrifuges.[46] In essence, the attackers deployed software (*forcefully exerting power*) against an object (*computers and centrifuges*) to deprive Iran of their nuclear capability. Therefore, while different than Clausewitz's vision, force and violence from and within the cyberspace domain meet the intent Clausewitz laid out in the 1800s.

Chance and friction are other key components of Clausewitz's theory and are very applicable to cyberspace. Clausewitz stated, "[c]hance makes everything more uncertain and interferes with the whole course of events."[47] He also loosely defines friction as, "… the force that makes the apparently easy so difficult."[48] One of cyberspace's strength, the speed at which actions can occur, allows *chance* and *friction* to have a tremendous impact. For instance, operations can theoretically occur in cyberspace 20,000 times faster than in space, 200,000 times faster than in air, and 10 million times faster than on land or sea.[49] As discussed previously, this can be a tremendous benefit for delivering effects against an enemy. Likewise, it can also make the job of a network defender very difficult. For all its benefits, this speed has its drawbacks, one of which is the information deluge it enables.

Operations in cyberspace are conducted at amazing speeds. Information travels at the speed of light, constantly inundating operators and decision makers with information from and about the operating environment. This increases the likelihood that key items will be missed at any given moment. Cyberspace is also a domain in which the operating environment constantly changes. Every software patch, configuration change, or hardware installation modifies the cyber terrain in which offensive and defensive forces operate. Slight modifications could inadvertently introduce security flaws that must be protected by a defender. As it relates to attackers, a minor modification could, in the blink of an eye, remove a well-researched avenue of approach. Dynamic changes, information deluge, and speed in the environment demonstrate the *friction* inherent in this warfighting domain, opening the door for *chance* to have an even greater impact.

Evolving Theory

While the debate rages on regarding the need for a cyberspace theory, its requirement is evident and has a strong supporting basis from Carl von Clausewitz, one of the most well-known military theorist. Fighting in cyberspace may be the newest form of warfare, but any theory to provide a baseline need not start from scratch. While many of the classical theorists share similarities in their ideas[50], one cannot expect theories from other domains to blindly apply to cyberspace. Cyberspace is a warfighting domain to which theories from Clausewitz, Corbett, and Sun-Tzu can be evolved and applied. Deferring the creation of cyberspace theory inhibits operators and their commanders from having an analytical tool that can make sense of deviations from the norm.[51]

The Use of Cyberpower is an Extension of Politics

As stated previously, it is U.S. policy to defend its critical digital infrastructure against enemy attack.[52] The corollary to this is all of the DoD's operations to build, operate and defend its networks are in support of the nation's policies and political system. In addition, the U.S. is prepared to use force to "… defend [itself] and allies or to preserve broader peace and security,"[53] thereby justifying the preparation for and use of offensive cyberspace operations when directed.

Cyberspace Operations are Interdependent with Operations in other Domains

Sir Julian Corbett, a distinguished naval warfare theorist, was a firm believer that naval warfare's purpose was to support land operations.[54] He believed that naval strategy and subsequent operations were most effective when there is clear understanding of how it supports the nation's army.[55] In a similar vein, cyberspace operations are most effective when used as a part of the larger military apparatus, simultaneously employed in conjunction with land, sea, air, and space operations.. .

This is the only way to ensure the missions and actions of cyberspace operations effectively and efficiently operate cohesively within the continuum of military operations.

Cyberspace Operations is a System

Cyberspace operations and its supporting missions and actions are "more than the sum of its parts."[56] Execution of the whole requires constant information flows and feedback loops amongst all of its parts. Built-in security for systems and networks to support enterprise and military operations must be driven by information and intelligence obtained about the threat and ongoing defensive operations. Likewise, defensive operations are also informed not only by the threat, but also the layout of friendly networks. Offensive operations are dependent on operating from a secure environment. In addition, enemy vulnerabilities discovered during intelligence or information gathering operations can be provided to friendly defenders and engineers to enhance the security of blue networks. These information flows and feedback loops are necessary throughout the all phases of military operations.[57]

Cyberpower is Useless Without the People to Project It

Clausewitz stated, "[w]arfare comprises everything related to the fighting forces—everything to do with their creation, maintenance, and use."[58] General Merrill A. McPeak, a former U.S. Air Force Chief of Staff, also stated, "… the effective employment of air and space power has to do not so much with airplanes and missiles and engineering as with thinking and attitude and imagination."[59] Effectively and efficiently manning, training and equipping cyberspace forces with the agility and flexibility to operate in a constantly evolving cyberspace environment is directly related to the ability to project cyberpower. Likewise, leader education must be sufficient to instill knowledge of the technical complexities inherent in this domain and

comprehension of how to use cyberspace operations in support of strategic, operational and tactical objectives. Concentrating on people is the only way to grow a cadre of operators and leaders who are equipped with the intellect, temperament and courage to manage the expected and unexpected.[60]

Defense is the Stronger Form of Warfare[61]

The ability to defend ones' systems and networks against enemy exploitation and attack is of the highest importance. If an agent of war cannot preserve (defend) what he has, his conquests (attacks) are for naught in the end, as he cannot maintain and consolidate gains. The systems and networks upon which the DoD depends for virtually all of its military and enterprise operations must be protected and adapted to counter-evolving, technologically advanced threats. The goal is mission assurance, which requires strong, persistent, and agile defenses for day-to-day, contingency and deliberate operations. If these defensive requirements are not met, mission assurance will not be obtained.

Understand Yourself and Your Enemy

Sun-Tzu said, "Know the enemy and know yourself … when you are ignorant of the enemy, but know yourself, your chances of winning or losing are equal … If ignorant of your enemy and of yourself, you are certain in every battle to fail."[62] Cyberspace is geographically unbounded, which makes it extremely difficult to defend. Sun-Tzu concentrated on *knowing* yourself and the enemy. However, it is of greater importance to *understand* each. Rather than just having knowledge, it is more important to understand the implications and impacts of various circumstances.[63] Every device connected to the network is a possible enemy avenue of approach. Inadequate understanding of your operating environment leads to increased risks of security

breaches. Deliberate, dogged intelligence and information gathering actions must be employed against the enemy to understand his intentions and capabilities. Understanding the enemy's intentions will provide insight into his attack and response option predictors. Enemy capabilities include those technical tools, which can be used to exploit or attack, as well as the system and network infrastructures that enable its operations. This knowledge proactively informs building, securing and defending your networks, as well as enabling the DoD to react appropriately to unforeseen enemy capabilities and activities.

Identify and Concentrate Defenses at Friendly Cyber Centers of Gravity (CoG)

Clausewitz's CoG concept is firmly embedded in U.S. Doctrine, particularly the joint publications for operations[64] and planning[65]. Its usefulness, however, is still a highly debated topic.[66] Clausewitz's considered CoGs the "… hub of all power and movement, on which everything depends," which necessitates the concentration of energy on that one point.[67] It is virtually impossible to protect everything in cyberspace, so it is necessary to mass defenses at key locations. Given the ubiquitous nature of cyberspace, unlike traditional military doctrine, there may be numerous critical nodes, or cyber CoGs. Once an understanding of friendly networks is obtained, it is crucial to identify cyber CoGs, which are key to enterprise and military operations. Once identified, advanced defensive measures should be massed and employed at these locations to reduce possible impact of enemy exploitation and attack. For other points on the network, the goal should be to enhance defenses sufficiently to increase the risk and cost for the attacker.

Command of Cyberspace

Corbett believed that complete control, or command, of the sea was unobtainable.[68] Therefore, one must seek to control lines of maritime communications, preserving them for friendly forces while denying that same control to the enemy.[69] Likewise, total command of cyberspace is not achievable. However, after actions are taken to gain friendly situational awareness, identify friendly cyber CoGs and understand the threat, key lines of communication can be identified. These lines of communication are the cyberspace operator's maneuver space. Therefore, one must protect these lines of communication to ensure friendly freedom of maneuver and prevent the enemy from obtaining the same. Defenses should be intensely focused on these lines of communication, which will further enable offensive actions against the enemy.

Use Force with Caution

An inventory of offensive capabilities serves as a valuable deterrent for adversaries and enemies alike[70]. The ability to project force via offensive capabilities or defensive response actions can be an effective method to achieve the commander's objectives and possibly prevent the commander from having to send a person in harm's way. However, restraint and unity of effort must be used when considering this option. Cyberspace is an information conduit. While cyberspace enables rapid information exchange between friendly forces, it also creates opportunities for an adversary or enemy to capture that information. The tools used to attack opponents in cyberspace are, in its basic form, information. Should an adversary capture these tools, they could employ those same tools against friendly forces. Therefore, one must always be

cognizant that friendly forces may have to defend against the same type of weapons used against the enemy.

Cyberpower is Based on Deception and Surprise

Sun-Tzu believed that “[a]ll warfare is based on deception,”[71] and that one must surprise the enemy by appearing where ”he does not expect you.”[72] This is the essence of cyberspace operations. Offensive operations are successful because they contain both of these elements. Due to the inherent anonymity afforded in cyberspace, attribution of attacks is extremely difficult. If the adversary is not completely stealthy in his operations, he is likely to mask himself as someone else coming from an entirely different location than his true origination point. Friendly forces must rely on timely and usable intelligence and forensic analysis to determine the true enemy. However, friendly forces must take advantage of this anonymity when appropriate during the conduct of offensive operations. One can obtain the element of surprise by exploiting unknown vulnerabilities, attacking where the enemy least expects, or operating at increased speeds to counter human intervention. The use of zero-day attacks[73], indirect approaches, and automated attacks can keep the element of surprise. However, the adversary can employ the same tactics, therefore more automated defenses should be employed to counter the adversary’s ability to surprise.

Conquest may be Obtained through Unlikely Means

Sun-Tzu stated, “[h]e who knows the art of the direct and indirect approach will be victorious.”[74] The operating environment in cyberspace is always in flux, which may limit the options of attack against a target to only indirect means. For instance, the risk may be too great to completely disable the enemy’s logistics operations, but the same objective could be accomplished by modifying his logistics database so that the wrong

materiel is delivered at the wrong time. One must view the target from a systems thinking perspective. The target is part of the enemy's system, which is composed of agents, information flows and feedback loops. It is not wise to focus solely on only one agent in the system, as modifying other components could yield the same results. The goal is to understand the enemy's environment, the relationship between its system's components, and obtain the desired effects with minimal friendly risk and cost.

Conclusion

Cyberspace, an innovation that took root over forty years ago, changed the landscape of how businesses, institutions, organizations, governments, and militaries operate. Cyberspace changes the character of war, even more so now that cyberspace is its own warfighting domain, through which militaries will project cyberpower. The general purpose of military theory is to reach a general understanding of the character of war.[75] Libicki argues that cyberspace is not ready for theory due to its constant evolution, and the infancy of operations conducted therein.[76] However, this line of reasoning is precisely what will prevent the DoD from making significant advances in effectively and efficiently fighting from and in cyberspace

The evolution of cyberspace will continue. Operations conducted within this domain are maturing, but will also evolve, which will always leave some aspect of cyberspace its infancy. Science is rife with theories proven wrong or superseded. Winton stated, "theory is never complete and is always bound to be at least partially invalid."[77] It is precisely this reason why cyber theory is required sooner rather than later. Evolving theory from those penned by classical military theorists is a logical and advantageous starting point. For cyberspace to be truly used as a warfighting domain, it must be underpinned by theory in order to understand how to fight and win in the virtual

space. Without a theoretic baseline, one will never know when to deviate from the norm and why. The theories proposed here are meant to be the beginning of that theoretic baseline to be expanded and improved upon as the cyberspace domain and the operations conducted therein progress through various stages of maturity. Evolving theories from classical theorists to create cyberspace theory will enable the DoD to effectively project cyberpower and gain the competitive advantage in cyberspace.

Endnotes

[1] Harold R. Winton, "An Imperfect Jewel: Military Theory and the Military Profession," *Journal of Strategic Studies* 34, no. 6 (December 2011): 874.

[2] Sun-Tzu, *The Art of War*, Samuel B. Griffith, trans. (New York: Oxford University Press, 1963,).

[3] Thucydides, *The Landmark Thucydides: A Comprehensive Guide to the Peloponnesian War*, trans. Robert Strassler (New York: Free Press, 1996), 1.75, 43.

[4] Sir Julian S. Corbett, *Some Principles of Maritime Strategy* (Online eBook: Project Gutenberg, 2005), published originally in 1911, 10, http://www.gutenberg.org/files/15076/15076-h/15076-h.htm (accessed November 17, 2014).

[5] Oxforddictionaries.com, "Cyberspace," http://www.oxforddictionaries.com/us/definition/american_english/cyberspace (accessed January 4, 2015).

[6] Bolt Beranek and Newman Inc., "A History of the ARPANET: The First Decade," April 1, 1981, http://www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA115440 (accessed January 20, 2015).

[7] International Telecommunication Union, "ITU releases 2014 ICT Figures," http://www.itu.int/net/pressoffice/press_releases/2014/23.aspx#.VPeZt1PF_pC (accessed March 4, 2015).

[8] U.S. Department of Defense, *Department of Defense Strategy for Operating in Cyberspace* (Washington, DC: U.S. Department of Defense, July 2011), 5.

[9] U.S. Joint Chiefs of Staff, *Department of Defense Dictionary of Military and Associated Terms*, Joint Publication (JP) 1-02 (Washington, DC: U.S. Joint Chiefs of Staff, November 8, 2010 as amended through July 16, 2014), 63.

[10] Clorinda Trujillo, “The Limits of Cyberspace Deterrence,” *Joint Force Quarterly*, no. 75 (4th Quarter, 2014): 44.

[11] Ibid.

[12] U.S. Department of Defense, *Department of Defense Strategy for Operating in Cyberspace*, 1.

[13] U.S. Joint Chiefs of Staff, *Department of Defense Dictionary of Military and Associated Terms*, 63.

[14] U.S. Joint Chiefs of Staff, *Cyberspace Operations*, JP 3-12 (R) (Washington, DC: U.S. Joint Chiefs of Staff, February 5, 2013), II-2.

[15] Ibid., II-3.

[16] *U.S. Department of Defense Chief Information Officer Joint Information Environment Initiative Homepage*, http://dodcio.defense.gov/Initiatives/JointInformationEnvironment/JIE.aspx (accessed January 20, 2015).

[17] U.S. Department of Defense, *Joint Operational Access Concept (JOAC)* (Washington, DC: U.S. Department of Defense, January 17, 2012), 1.

[18] U.S. Joint Chiefs of Staff, *Cyberspace Operations*, II-2.

[19] Ibid.

[20] Ibid.

[21] Ibid.

[22] U.S. Department of Defense, *Joint Operational Access Concept (JOAC),* 6.

[23] Dorothy Denning, *Information Warfare and Security* (Boston, MA: Addison-Wesley, 1999), 40.

[24] Ibid.

[25] U.S. Joint Chiefs of Staff, *Cyberspace Operations*, II-2.

[26] Michael B. Kelley, “The Stuxnet Attack on Iran's Nuclear Plant Was 'Far More Dangerous' Than Previously Thought,” *Business Insider*, November 20, 2013, http://www.businessinsider.com/stuxnet-was-far-more-dangerous-than-previous-thought-2013-11 (accessed September 9, 2014).

[27] U.S. Joint Chiefs of Staff, *Cyberspace Operations*, II-4.

[28] Ibid.

[29] Ibid., II-5.

[30] Ibid.

[31] Daniel T. Kuehl, “From Cyberspace to Cyberpower,” in *Cyberpower and National Security*, ed. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Washington, DC: National Defense University Press, 2009), 38.

[32] John Arquilla and David Ronfeldt, “A New Epoch—and Spectrum—of Conflict,” in *In Athena’s Camp* ed. John Arquilla and David Ronfeldt (Santa Monica, CA: RAND, 1997), 2.

[33] Martin C. Libicki, "Why Cyber War Will Not and should not have its Grand Strategist," *Strategic Studies Quarterly* 8, no. 1 (Spring, 2014): 23-39, http://www.au.af.mil/au/ssq/digital/pdf/spring_2014/Libicki.pdf (accessed December 22, 2014).

[34] Oxforddictionaries.com, “Theory,” http://www.oxforddictionaries.com/us/definition/american_english/theory (accessed December 22, 2014).

[35] Carl von Clausewitz, *On War*, ed. and trans. Michael Howard and Peter Paret (Princeton, NJ: Princeton University Press, 1976), 578.

[36] Winton, “An Imperfect Jewel: Military Theory and the Military Profession,” 859.

[37] John J. Klein, “Corbett in Orbit: A Maritime Model for Strategic Space Theory,” *Naval War College Review* 57, no. 1 (Winter 2011): 59.

[38] Michael I. Handel, *Masters of War: Sun Tzu, Clausewitz and Jomini* (Portland, OR: Frank Cass, 1992), 20.

[39] Clausewitz, *On War*, 85, 89, 75.

[40] Barack H. Obama II, *National Security Strategy* (Washington, DC: The White House, May 2010), 27.

[41] Charles T. Hagel, *Quadrennial Defense Review* (Washington, DC: U.S. Department of Defense, February 2010), 14.

[42] Clausewitz, *On War*, 75, 89.

[43] Dictionary.com, “Force,” http://dictionary.reference.com/browse/force (accessed September 8, 2014)

[44] World Health Organization, *World Report on Violence and Health* (Geneva: World Health Organization, 2002), 5.

[45] U.S. Joint Chiefs of Staff, *Department of Defense Dictionary of Military and Associated Terms*, 188.

[46] Kelley, “The Stuxnet Attack on Iran's Nuclear Plant Was 'Far More Dangerous' Than Previously Thought.”

[47] Clausewitz, *On War*, 101.

[48] Ibid., 121.

[49] Jeffrey L. Caton, *Distinguishing Acts of War in Cyberspace: Assessment Criteria, Policy Considerations, and Response Implications* (Carlisle Barracks, PA: U.S. Army War College, October 2014), 12.

[50] Handel, *Masters of War: Sun Tzu, Clausewitz and Jomini*.

[51] J.J. Widen, "Sir Julian Corbett and the Theoretical Study of War," *Journal of Strategic Studies* 30, no. 1 (March 2007): 116.

[52] Obama, *National Security Strategy*, 27.

[53] Ibid., 22.

[54] Sir Julian S. Corbett, *Some Principles of Maritime Strategy* (Online eBook: Project Gutenberg, 2005), published originally in 1911, 16, http://www.gutenberg.org/files/15076/15076-h/15076-h.htm (accessed November 17, 2014).

[55] Corbett, *Some Principles of Maritime Strategy*, 16.

[56] Donella H. Meadows, *Thinking in Systems* (White River Junction, VT: Chelsea Green Publishing, 2008), 11.

[57] U.S. Joint Chiefs of Staff, *Joint Operations*, JP 3-0 (Washington, DC: U.S. Joint Chiefs of Staff, August 11, 2011), V-6 – V-9.

[58] Clausewitz, *On War*, 95.

[59] Richard Szafranski, "Neocortical Warfare? The Acme of Skill," in *In Athena's Camp*, 395.

[60] Clausewitz, *On War*, 100-102.

[61] Clausewitz, *On War*, 84.

[62] Sun-Tzu, *The Art of War*, 84.

[63] John Rothrock, "Information Warfare: Time for Some Constructive Skepticism," in *In Athena's Camp*, 227.

[64] U.S. Joint Chiefs of Staff, *Joint Operations*.

[65] U.S. Joint Chiefs of Staff, *Joint Operation Planning*, JP 5-0 (Washington, DC: U.S. Joint Chiefs of Staff, August 11, 2011).

[66] One recent example is: Lawrence Freedman, "Stop Looking for the Center of Gravity," *War on the Rocks*, entry posted June 24, 2014, http://warontherocks.com/2014/06/stop-looking-for-the-center-of-gravity/ (accessed December 31, 2014).

[67] Clausewitz, *On War*, 595-6.

[68] Corbett, *Some Principles of Maritime Strategy*, 92.

[69] Ibid., 93-94.

[70] U.S. Joint Chiefs of Staff, *Department of Defense Dictionary of Military and Associated Terms*, B-2, differentiates adversaries and enemies, labeling adversaries as potentially hostile whereas enemies are demonstrably hostile.

[71] Sun-Tzu, *The Art of War*, Samuel B. Griffith, trans. (New York: Oxford University Press, 1963,), 66.

[72] Sun-Tzu, *The Art of War*, 96.

[73] Zero-day attacks are "software or hardware vulnerabilities that have been exploited by an attacker where there is no prior knowledge of the flaw in the general information security community, and, therefore, no vendor fix or software patch available for it." (Definition obtained from: Zheng Bu, "Zero-Day Attacks are not the same as Zero-Day Vulnerabilities," *Fireeye*, entry posted on April 24, 2014, https://www.fireeye.com/blog/executive-perspective/2014/04/zero-day-attacks-are-not-the-same-as-zero-day-vulnerabilities.html (accessed March 5, 2015))

[74] Sun-Tzu, *The Art of War*, 106.

[75] Alan D. Beyerchen, "Clausewitz, Nonlinearity and the Unpredictability of War," *International Security* 17, no. 3 (Winter, 1992): 59-90, http://www.clausewitz.com/readings/Beyerchen/CWZandNonlinearity.htm (accessed January 22, 2015).

[76] Libicki, "Why Cyber War Will Not and should Not have its Grand Strategist," 23-39.

[77] Winton, "An Imperfect Jewel: Military Theory and the Military Profession," 857.